Study to support the impact assessment for the revision of the eIDAS regulation

Final Report

Written by PwC and DLA Piper

t

Internal identification

Contract number: SMART 2019/0024
VIGIE number: 2020/666

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology
Directorate H — Digital Society, Trust & Cybersecurity
Unit H.4 — eGovernment & Trust

Contact: CNECT-H4@ec.europa.eu

European Commission
B-1049 Brussels

Study to support the impact assessment for the revision of the eIDAS regulation

Final Report

EUROPE DIRECT is a service to help you find answers to your questions about the European Union

Freephone number (*):
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you)

Authors: Giovanna Galasso (*Project manager,* PwC), Giorgio Garbasso (PwC), Danilo Bianchini (PwC), Martina Tortis (PwC), Matteo Gori (PwC), Patrick Van Eecke (DLA Piper), Florian De Roucke (DLA Piper), Riccardo Genghini (external expert), Viky Manaila (external expert), Marc Sel (external expert), Massimiliano Tancioni (external expert).

LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the European Commission is not liable for any consequence stemming from the reuse of this publication. The Commission does not guarantee the accuracy of the data included in this study. More information on the European Union is available on the

PDF KK-09-21-162-EN-N ISBN 978-92-76-37859-4 DOI:10.2759/671740

Internet (http://www.europa.eu)

Manuscript completed in April 2021
2021 edition

The European Commission is not liable for any consequence stemming from the reuse of this publication.

Luxembourg: Publications Office of the European Union, 2021

© European Union, 2021

The reuse policy of European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under a Creative Commons Attribution 4.0 International (CC-BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightholders.

ABSTRACT

This study supports the European Commission in assessing the impact of different policy options to review the eIDAS Regulation, with the aim of establishing a legislative framework for a convenient, widely usable, secure and interoperable Digital Identity for the Digital Single Market.

The study contributes to the definition of the problem and the justification behind the need for an EU legislative intervention in this field, and provides a comparative analysis of costs and benefits expected for relevant groups of stakeholders affected by the different policy options, namely: public authorities, online service providers, conformity assessment bodies, trust service providers, eID providers and wallet app providers.

Data and evidence have been collected through different methods: an open public consultation, targeted surveys and in-depth interviews involving key stakeholders of the eIDAS ecosystem in the public and private sector. Based on the collected evidence, the study draws conclusions and provides a preferred option for the legislative intervention, which should be considered as a substantial input for the introduction of a EU framework for digital identity.

EXECUTIVE SUMMARY

The **eIDAS Regulation** introduced a cross-border framework for electronic identification (eID) and trust services in 2014. The aim of the eIDAS regulation was to enable EU citizens, companies and public administrations to safely access services and carry out transactions online and across borders[1].

Article 49 of eIDAS requires the Commission to review the application of the regulation no later than July 2020, particularly to evaluate whether it is appropriate to modify its scope or its specific provisions taking into account technological, market and legal developments.

While the Regulation delivered on many of its goals and it became a recognised and globally respected approach to electronic identity, number of challenges are still unaddressed. Since 2014, fast paced changes in technology availability, market structure, user behaviour and the increasing role of online platforms acting as identity providers call for a revision of the eIDAS regulation. There is a recognised need for an updated framework for a competitive, convenient, trustworthy and versatile Digital Identity to exploit the opportunities of the Digital Single Market.

The findings of this study will contribute to supporting the Impact Assessment of the **revision of the Regulation.** The **three specific objectives of the study** are to:

1. assess the expected costs and benefits and impacts of different options for policy intervention in the area of digital identity and their components;
2. compare different policy options available based on the assessment of costs, benefits and impacts;
3. produce a conclusion on the most effective, efficient and coherent policy intervention in the area of digital identity.

In order to pursue the study objectives, several data collection activities (desk research, interviews, sectoral case studies, surveys, workshops) to gather stakeholder views and quantitative data have been launched and implemented in between July and December 2020, in line with the seven Key Questions included in the Better Regulation Guidelines[2].

Political and legal context

The Commission has committed in its Strategy on Shaping Europe's Digital Future to **revise the eIDAS Regulation** to improve its effectiveness, extend its application to the private sector and promote trusted digital identities for all Europeans. In providing political momentum for the need for a revision the conclusions adopted by the European Council on 9 June 2020 on Shaping Europe's digital future[3] call upon the European Commission to:

"consider proposals for further development of the current framework for cross-border identification and authentication based on the eIDAS Regulation towards a framework for a European digital identity, which would drive the Member States to make widely usable, secure and interoperable digital identities available for all Europeans for secure government and private online transactions."

[1] European Commission. (2020). *Inception impact assessment*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-

[2] European Commission (2017) *Better Regulation guidelines: Chapter III Guidelines on impact assessment*

[3] The Council of the European Union. (2020). *Shaping Europe's Digital Future - Council Conclusions (9 June 2020)* https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf

In her State of the Union Speech, the European Commission President Ursula Von Der Leyen, while setting out the EU's technology policy priorities, also announced the Commission's commitment to delivering a secure European Digital Identity:

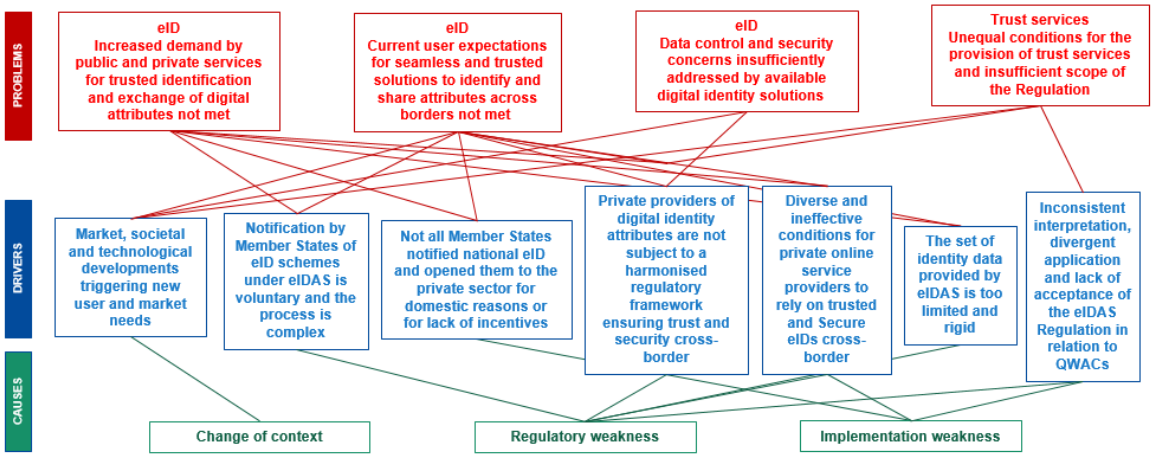
"We want a set of rules that puts people at the centre. (...) This includes control over our personal data which still have far too rarely today. Every time an App or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will soon propose a secure European e-identity. One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data and how data is used."

In the same vein, the Council Conclusions of 1-2 October 2020 invite the European Commission to come forward with a proposal for a European digital identity framework initiative by mid-2020, calling for[4] :

"the development of an EU-wide framework for secure public electronic identification (e-ID), including interoperable digital signatures, to provide people with control over their online identity and data as well as to enable access to public, private and cross-border digital services".

The revision of eIDAS is driven by the above-mentioned political mandate conferred on the European Commission, as well as the obligations pursuant to Article 49 of the Regulation and the necessity to address the significant challenges identified with respect to the current eIDAS framework.

Problem definition



The core problems addressed by the revision of eIDAS with respect to eID means are as follows:

Increased demand by public and private services for trusted identification and exchange of digital attributes not met (eID)

The eIDAS Regulation focuses on access to cross-border public sector services, and has been able to offer this access only for a limited number of them. However, given its inherent

[4] The Council of the European Union. (2020). *Special meeting of the European Council - Council Conclusions (1-2 October 2020)* https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf

limitation to the public sector, it cannot address growing demands for secure and trusted identification and exchange of attributes for access to ***private services***. In particular, the complexity for online private providers to connect to the system, its insufficient availability in all Member States and its lack of flexibility to support a variety of use cases (see section on drivers) are significant limiting factors. Furthermore, identity solutions provided outside eIDAS by social media providers and other private service providers (such as banks) cannot seamlessly respond to these new market needs as they may not be available to external customers, lack a direct link to trusted and secure eID and/or they do not benefit from cross-border recognition, preventing such solutions from being scalable.

As regards the ***public services***, demand for cross-border access has also grown and evolved due to digitisation and increased mobility (about 30% of EU population travel yearly to another Member State). However, eIDAS focuses mainly in the needs of those EU citizens of working age residing in another EU Member State, which represents in number only around 3% of EU population[5]. Crucially, today many citizens do not even have access to trusted and secure government eID means allowing them to access services across border. Six years after the adoption of eIDAS, the eIDAS framework covers only about half of the EU population , leaving 41% of EU citizens without the possibility to use any trusted and secure eID scheme across borders.Even in those Member States which notified a national eID under eIDAS, substantial barriers to access public online services persist and the number of services connected to the national nodes is considerably smaller than the number of services declared as being accessible via the domestic eID scheme.

In relation to the ***market demand for credentials digitally proving attributes,*** such as medical certificates or professional qualifications, they are currently not covered by eIDAS and as a result, Member States and service providers have been forced to develop proprietary trust and interoperability frameworks to ensure the security of these services and/or their recognition across borders.

Current user expectations for seamless and trusted solutions to identify and share attributes across borders not met (eID)

Users today expect seamless online journeys, mobile applications and single-sign-on solutions that can be used for online services in the public and private sector, covering all use cases for identification ranging from pseudonymous log-on to an online platform to secure identification for e-health or e-banking. Secure online identification and the exchange of attribute credentials is becoming more important as the number of identity-sensitive and personalised services increases. The ability to identify digitally will become an important factor of social inclusion and the provision of digital identity a strategic asset.

New technological solutions are adopted by the public and private sectors that aim to address the evolving needs of citizens and businesses, wuch as digital wallets which allow the user to manage and exchange their own identity-related information, attributes and credentials. Some Member States are moving into this direction, which, unless regulated at EU level, will further increase the disparity between national systems.

Alternative ***digital identification solutions by private providers*****,** not recognised by governments, do exist. However, as mentioned above they only address some private use cases not requiring high level of security. Other more secure solutions offered by private providers lack common frameworks or standards as regards for example, the levels of assurance that they provide. They can therefore not scale up and be recognised across borders for access to public or private services which require a certain level of trust.

[5]https://ec.europa.eu/eurostat/statistics-explained/index.php/EU_citizens_living_in_another_Member_State_-_statistical_overview

Without access to seamless and trusted identity solutions recognised cross border, citizens and businesses will have to rely on solutions that are not linked to their legal identities issued by Member States and are therefore less secure. This contradicts the increasing user demand for a secure digital identity to access all online services in the EU that gives users control over the use of their personal data and allows for the exchange of personal data attributes and credentials.

Data control and security concerns insufficiently addressed by available digital identity solutions (eID)

The **security risks** involved in providing personal data online or in information systems for authentication purposes are significant and increasingly important as more citiens conduct transactions online on a frequent basis. However, neither public nor private offers fully respond to this demand. Existing eIDs under eIDAS are not sufficiently widely usable for identification in the private sector to represent a viable alternative and has inherent limitations to discretional data disclosure for the user. Despite offering a high level of security, they show limitations as regards the principle of **data minimisation**; For example, eIDAS does not support so called ***"zero-knowledge claims".*** In addition, identification provided by large online platforms often does not allow for the effective protection of personal data, as evidenced by major data breaches and enforcement actions over the last decade, but is used by service providers given the large market power and customer base of platforms. The general shift towards a more comprehensive identity ecosystem that integrates attributes and credentials, some of them carrying sensitive data such as in the health sector, makes it necessary to develop eID ecosystems that are able to effectively protect personal data and offer full user control.

Unequal Conditions for the Provision of Trust Services and insufficient Scope of the Regulation (Trust services)

Although the evaluation of the eIDAS Regulation concludes that the regulatory framework has successfully established legal certainty on liability, burden of proof, legal effect and international aspects of trust services, it also shows that there is room for improvement regarding a harmonised application of ***supervisory procedures*** and ***processes for identity proofing***, in particular when these processes are carried out remotely.

In addition, there are national differences in the way the conformity assessment of qualified trust services providers is carried out, which requirements apply and which standards are used. As the eIDAS Regulation does not regulate these aspects, differences in the application of the rules for national supervision between Member States raise challenges regarding a comparable level of trust and security of the services provided and of a common level playing field.

The problems described for the provision of trust services are also linked to the absence of a common governance structure at EU level similar to that of the Cooperation Network for eIDs allowing Member States to jointly address them. In the evaluation, some supervisory authorities noted that the role of FESA[6] should be formalised to address the need of consistent application of eIDAS chapter on trust services in all Member States.

Risks of market barriers have also been identified for ***eArchiving services***. The eIDAS Regulation requires archiving the signatures of electronic documents but does not specify

[6] The Forum of European Supervisory Authorities (FESA) for trust service providers, is a forum open to national bodies responsible for supervision and/or trusted lists in accordance with the eIDAS Regulation. The scope of FESA is to support the cooperation, information and assistance among the members and to facilitate the exchange of views and agreement on good practices: http://www.fesa.eu/

requirements and which standards to use, leading several Member States to develop competing national rules

There is also need for improvement concerning the efficiency of a particular trust service, the provision of ***Qualified Website Authentication Certificates (QWACs)***. Despite the introduction of these certificates by the eIDAS Regulation, web browsers refuse to include them in their root stores and to display them clearly, which makes these certificates unusable for traders and consumers. For websites run by intermediaries or trading companies[7] only QWACs can guarantee identity of the entity behind a website with a high level of assurance. The lack of recognition of QWACs by web-browsers may also conflict with the protection of fundamental rights of consumers as enshrined in articles 12, 101, 102, 114 and 169 of the Treaty on the Functioning of the European Union and with EU Consumer protection legislation, in particular Directive 2005/29/EC[8].

A range of drivers underpins these problems, namely:

- Market, societal and technological developments triggering new user and market needs
- Notification by Member States of eID schemes under eIDAS is voluntary and the process is long and complex
- Not all Member States notified national eID and opened them to the private sector for domestic reasons or for lack of incentives
- Private providers of digital identity attributes are not subject to a harmonised regulatory framework ensuring trust and security cross-border
- Diverse and ineffective conditions for private online service providers cannot rely on trusted and secure eIDs cross-border
- The set of identity data provided by eIDAS is too limited and rigid
- Inconsistent Interpretation, divergent application and lack of acceptance of the eIDAS Regulation in relation to QWACs

Evolution of the problem

Globally, an increase in demand for digital identity solutions is expected, with a predicted annual market growth ranging from 13% to 20% . Users' expectations with regard to control of personal identity data and effective technologies for fraud and identity theft prevention will increase. Continued growth in mobile penetration strengthens the demand for convenient and secure mobile-first platforms and solutions . In the light of these expected trends, a no change scenario for the eIDAS Regulation may have the following impacts on the problems and drivers.

- Not all EU citizens and businesses will have access to a trusted and secure eID that can be conveniently used to authenticate to cross-border and cross-sector online services.

[7] Following the definition of article 1 of the 2011/83/EU Directive on consumers rights.

[8] Directive 2005/29/EC concerning unfair business-to-consumer commercial practices, protecting the right of consumers to know the legal entities they are interacting with, their geographical location to the point that providing misleading/inaccurate information or no information at all on the true identity of the business/trader, amounts to misleading or aggressive commercial practice (and fall just short of consumer fraud).

- In the absence of a common solution for identity matching, cross-border usability of eIDs will remain limited and this would also pose a risk to the functioning of other EU legislation, such as the Single Digital Gateway Regulation, and in particular the functioning of the Once-Only Principle.
- The market fragmentation for private eID solutions is likely to grow in the absence of a unitary regulatory framework at EU level. It is likely that a few powerful players (e.g. online platforms) will increase their dominance. This is likely to create dependencies for online service providers, user lock-in and a decrease in value creation as well as presenting a challenge to the EU's digital autonomy.
- User will not be able to control the use of their identity data in the absence of clear, uniform data protection and privacy safeguards for identity providers including online platforms.
- The risk of IoT devices being used as intermediaries to fraudulently reach citizens' and businesses' data is also expected to increase as more and more connected devices will be in circulation.

Justification for EU action

The EU has competence to act in order to address the current hurdles of the eIDAS regulation. The proposal to establish European Digital Identity finds its legal basis in:

- The 1992 Maastricht Treaty, as regards EU citizenship. Being able to effectively deploy electronic identification means in online services throughout Europe is supports this fundamental concept
- Article 21 TFEU, as regards the exercise of the freedom of movement of EU citizens, which would be facilitated by the measure

The proposal is also in line with the principles of subsidiarity and EU added value, as domestic action alone would not suffice for the fulfilment of the conclusions adopted by the Council on 9 June 2020 on the shaping Europe's digital future.

Definition of objectives

The objectives for the revision of the eIDAS Regulation are set at three levels, which then feed into the policy options:

General objectives
ensure the proper functioning of the internal market, particularly in relation to the provision of cross-border and cross-sector digital public and private services.
Specific objectives
Digital Identity • Provide access to trusted and secure digital identity solutions for all EU citizens and businesses cross borders • Make accessible a wide range of public and private online services relying on trusted and secure digital identity solutions cross border • Provide citizens full control of their personal data and assure their security when using digital identity solutions **Trust services** • Ensure equal access to the trust services market

Operational objectives		
A) Reinforce the scope and improve the current eIDAS framework by introducing further requirements to member states and the private sector, procedural simplification, harmonisation and standardisation measures;	B) Extend the scope of eIDAS regulation to create a market for the secure exchange of Data linked to identity, credentials and attestations and introducing new requirements to the private sector	C) create a legal and technical framework for the deployment of the European digital identity as a user-controlled digital Wallet App which could be deployed by private qualified service providers and governments.

Policy options

The research has considered four main options, which are not mutually exclusive.

Under the baseline scenario (**Option 0**), the Commission would not propose any changes to the current legislation, and the eIDAS Regulation and its framework would therefore remain in force. In order to allow a consistent assessment and comparison of the options, the baseline also integrates the measures envisaged under secondary legislation that could be enforced without any changes brought to the Regulation (e.g. non-adopted implementing acts) or positive spill-overs stemming from other pieces of legislation (e.g. Digital Markets Act).

Option 1 involves creating a European Digital Identity in the form of a strengthened legislative framework for national eIDs notified under eIDAS. It would require Member States to make eIDs available to all citizens and companies for cross-border use and improve the effectiveness and efficiency of mutual recognition. The use of national eIDs by private online service providers would be triggered and facilitated through harmonised cost and liability rules, extended data sets and access obligations. All these measures would be taken without extending the scope of the eIDAS Regulation nor affecting its underlying principles (e.g. applicable to eID solutions notified by Member States, mutual recognition and technological neutrality).

Under **Option 2,** the private sector would support the delivery of a European digital identity ecosystem in the form of a new qualified trust service for the exchange of digital identity attributes across borders, such as proof of age (e.g. for accessing age restricted social media), professional qualifications (e.g. lawyer, student, doctor), digital driving licences, medical test certificates etc. The scope of eIDAS would be expanded to cover this new trust service where identity data and attributes would be securely linked to the legal eID of the user, making the data trustworthy and legally enforceable across borders. National eIDs notified under eIDAS would continue to be the sole means to provide legal identity when this is required (e.g. for public services, such as submitting a tax declaration online). This option sets-up a framework that allows citizens to exercise their citizenship (Article 20 TFEU) under common rules across the EU.

Option 3 would define a legal and technical framework for the deployment of the European digital identity as a user-controlled digital Wallet App. The Wallet App would empower users to securely share data related to their identity to public and private online service providers through their mobile device and allow them to control their own personal data in a user-centric way. Further to legal requirements, common standards and/or technical references for the Wallet App would be developed in close dialogue with Member States and private sector stakeholders. Two sub-options are considered for the deployment of the wallet: (1) deployment by private qualified trust service providers under eIDAS and (2) deployment by governments, under their mandate or recognised by them, as an extension to notified eID solutions. Policy option 3 sets-up a framework that allows citizens to exercise their citizenship (Article 20 TFEU) under common rules across the EU.

Impacts of the policy options

A cost-benefit analysis was carried out to assess the impacts of the four policy options described above. This section summarises the key costs and benefits identified.

Policy option 0 – Baseline scenario

Benefits

- The baseline scenario would mainly create benefits for **citizens and end users** via the secondary legislation measures envisaged by this option. Requiring gatekeepers to offer access and interoperability with notified eIDs and requiring Member States to limit identification data transmission to only the data necessary for a particular transaction would positively impact on citizens' security online and increase user control and trust in notified eIDs, enabling them to use these more widely and to provide only the minimum required data related to attributes in any transaction. Full control of identity data would however not be reached as the measure supporting data minimisation in the baseline scenario would not enable full integration of zero-knoweldge claims into the notified eIDs. Additionally, continuing refusal by web-browser vendors to display qualified website certificates in their browsers would preclude users and website owners from benefitting from the trust and assurance these independent certificates offer and continue to pose security threats in the form of phishing attacks for citizens and businesses.
- **Public authorities and trust service providers** are also amongst the beneficiaries of this option. Under this scenario, learning effects are likely to make the implementation of the Regulation marginally more efficient and effective over time, as stakeholders gain better awareness of opportunities and learn to manage risks. Additionally, secondary legislation measures will create some modest benefits for these stakeholder groups as well. Generally, however, the most significant weaknesses in the current legal framework that have been identified in the context of the evaluation are expected to persist.
- The main benefits that would likely be achieved by public authorities and trust service providers under this option relate to, respectively, a reduced need for for supervisory bodies to carry out additional audits and reduced national divergences in conformity assessment procedures for qualification of trust service providers. Again, while such harmonisation of Supervisory Procedures for Trust Services would facilitate greater consistency of implementation and facilitate compliance, inconsistencies in interpretation and application of rules for trust services in the baseline scenario would likely continue to exist, and to limit the confidence in trust services.

Costs

- Under this option, limited costs would mainly be incurred by **public authorities** and by **gatekeepers** to comply with the secondary legislative changes envisaged. Specifically, the scenario will create limited compliance costs for gatekeepers to enable offer access and interoperability with notified eIDs (as per Digital Markets Act) and require public authorities to implement technical adaptations that allow identity data transmission via the notified eIDs to be restricted to the minimum required for a specific transaction. Some efforts from the public authorities would also be required to achieve coordination with their peers in other Member States as a result of the greater harmonisation of supervisory procedures for the trust services.

Policy option 1 – Improve the current legal framework for cross-border recognition of national eIDs and trust services

Benefits

Overall, the biggest beneficiary groups of the different measures contained in the reinforcement of the Regulation are expected to be citizens and end users, online service providers, and Public authorities (particularly Supervisory bodies - SBs)..

- **Citizens and end users** would see their digital freedoms expand considerably, by being able to authenticate to public e-services provided in other EU Member States as well as to an increasing range of private services; having more transparent and comparable information on eID and trust services (including remote signing and website authentication); and benefitting from stronger security protection.
- **Online service providers** would benefit from: removing uncertainties and national differences over the terms and conditions applying to usage of a notified scheme, therefore reducing transaction costs and the risk of inadequate compensation for damages; opportunities to achieve efficiency savings for those that decide to adopt these schemes in their workflows; an ability to rely on an extended eIDAS person identification dataset that makes the eIDs usable across a wider range of use cases.
- For **public authorities**, reforms to the peer reviews will likely reduce the administrative burden linked to notification of eIDs under eIDAS and speed up the process. Further, EU-wide certification for security requirements will likely make it easier for the Member States' to prove the compliance of the notified eID schemes, and greater reliance by private online service providers on notified eIDs is expected to increase the transaction volumes within the eIDAS network and therefore help raise additional revenues.

Costs

The main costs stakeholders affected by additional costs under this option are the **public authorities** in the Member States and the Commission. The key costs they will have to bear to implement the different measures in the reinforcement of the regulation Policy options are the following:

- Familiarisation costs linked to the legislative changes for public authorities in the Member States, comprising all the additional resources required for familiarisation with procedural and legislative changes such as extending the list of attributes; requirements for Member States to allow private online service providers to rely on notified eIDs; strengthening security requirements for mutual recognition; introducing of e-archiving as a trust service; harmonising the certification for remote electronic signing.
- Costs of around €1.2 million in the next two years deriving from the increased workload of the peer reviews to be completed by the Cooperation Network
- Costs of upgrading the interoperability infrastructure to handle increased levels of traffic, estimated at around €6.1 million across the EU 27 (an average €225,000 per Member State).
- There will be further additional costs for notification of a scheme under eIDAS for the 13 Member States that have not yet done so, for a cumulative total of between €520,000 and €1.3 million
- The Commission would also incur costs from amending the legislation, updating guidance documents and facilitating dialogue within the Cooperation Network on the streamlining of the notification process. Under option 1, promotion of the use of QWACs amongst public authorities may also create marketing and awareness-raising costs in the region of €200,000-€400,000 on a one-off basis.
- Costs for the significant standardisation work required to implement the extension of the eIDAS person identification Based on stakeholder views, this is likely to create one-off costs of around €300,000.

Other stakeholder groups affected by costs include:

- **eID government providers**. compliance costs for eID providers would be generated from the need to obtain certification of eID means under the newly created EU-wide scheme (which is however voluntary), estimated at an average €60,000-€120,000 plus any required ex-post adjustment of the products and its documentation to a certification scheme. In addition, a requirement to allow private online service providers to rely on eIDAS-notified eID schemes may require them to adapt their scheme to fit the use-cases in the private sector (e.g. provide the required attributes)
- **Online service providers**. These may incur one-off costs from connecting to an eIDAS node estimated at €42,000 per provider.
- **Trust Service Providers.** TSPs wanting to enter the market for qualified preservation services would incur compliance costs similar to those applicable to qualification for other trust services currently covered by eIDAS (an average €545,000 for initial qualification and €255,000 per year on a recurrent basis). Harmonisation of certification for remote electronic signing would also imply some adaptation costs.
- **Browsers.** recognition of QWACs may entail some cost impacts, although these additional costs are likely to be limited as the procedures required are already carried out or are part of standing standard procedures.

Policy option 2 – Creating a market for the secure exchange of Data linked to Identity

Benefits

Overall, the most relevant beneficiary groups of an extension of the Regulation to the private sector are expected to be online service providers, end users/citizens and providers of data exchange services.

- Efficiency gains and other types of benefits for the **online service providers** would be generated as a result of: reduced costs of internal processes involving customer identity verification; reduced fraud costs; reduced costs of storage of attributes and attestations (e.g. because of substitution of paper attestations by their digital equivalents).
- **End users and citizens** will benefit from a strengthened legal basis for the protection of personal data; reduced administrative burden from digitalisation of services; increased access to secure and convenient digital identity authentication services for citizens; more possibilities to actively manage attributes, credentials and attestations (e.g. gender, age, professional qualifications etc.), increasing user control of data related to his/her digital identity and enabling personalised online services in a trusted environment where online privacy can be ensured, and data is protected[9]; improved trust in how attributes, credential ad attestations are handled by service providers; enhanced user control through more transparent terms and conditions of use; a diminished potential for online platforms to engage in unfair competition, which would help preserve user choice.
- Overall, the creation of a new trust service for the secure exchange of data linked to identity is likely to result in a significant expansion of market opportunities for **providers of data exchange services.**

Costs

[9] European Commission. (2020). Inception impact assessment.

The costs added to the system by policy option 2 would mainly fall on **ID providers, online service providers (including "gatekeeper" platforms acting as ID providers)** and **public authorities**. For the **public authorities**, the key additional costs are:

- Technical costs for developing API thus enabling the access to the authentic sources to trust service providers, estimated at around €30,000.
- Integration costs to the API of around €18,000 to €27,000 individually, for a cumulative integration cost estimated at around €625 million while the recurrent costs are expected to be overall €162 million per year. Awareness raising activities are assumed to be cost €8.4 million targeting an audience of 23.120 administrations and all EU citizens at large.
- Some communication and awareness raising costs would need to be incurred for the onboarding of public authorities in enabling to access their authentic sources.
- An increase in resources would also needed for supervisory duties, i.e. enforcement costs, at the national level; for familiarisation with the new regulatory framework; for international cooperation activities
- Defining security requirements and technical standards, estimated at around €1-2 million. EU grants for standard definition – which rely on the voluntary work of experts – are quoted on average at around €200,000 for the definition of one standard.

The other groups affected will need to incur the following costs:

- **Digital credential providers** seeking to offer the new trust services - particularly in their qualified form – would face compliance costs (one-off costs for the initial qualified status and for the technical changes to provide eID compliant solutions, recurrent compliance costs)
- **Online service providers** acting as ID providers (including "gatekeeper" platforms) would need to implement logical segregation of data, which for a medium size infrastructure is estimated to cost around € 25,000 to €30,000[10]. Also non-qualified providers would be subject to this data protection measure and will have to bear the same costs to functionally separate identity data from other data. Online service providers would also incur costs incurred related to IT integration to the API, expected to be from €18,000 to €27,000

Policy option 3 – Personal digital identity wallet (EUeID)

Benefits

Overall, the biggest beneficiary group of the creation of an EU Digital ID scheme is expected to be end users/citizens. **Citizens/end users** will benefit from:

- the convenience and user-friendliness of the authenticating interface. This "mobile first", user-centric design and the development of common standards are likely to help create a consistent user experience and support accessibility
- a more explicit privacy-by-design approach that could yield additional benefits in terms of data protection and privacy. The model proposed under this measure would reduce the need for intermediaries in the process, enabling the citizen to communicate directly with the service and credential providers.

[10] Based on estimates from internal confidential PwC professional activities in cybersecurity field.

- simplification of identity management, as the European Digital Identity Wallet would enable citizens to manage their own different identities and all associated credentials that they receive from various sources from anywhere in the EU.
- increased data security and reduced likelihood of identity theft, thanks to the design of the app as well as clear security requirements and the possibility to use it to access services offered by "gatekeeper" platforms.

The option is also expected to generate benefits for other stakeholder groups, particularly **online service providers** and **Wallet App providers**. For these groups, the following benefits have been identified:

- The introduction of the EU eID Wallet App is expected to reduce operating costs for **online service providers** that integrate it in their workflows, likely resulting in costs savings related to credentials issuance/verification, better customer experience and reduced costs due to fraud.
- an EUeID Wallet will increase the economic feasibility of market opportunities for Wallet App**providers**, as they will have a platform giving them access to an increased number of users on both sides of the market (citizens and online service providers). Further market opportunities may stem for providers of identity credentials from the incentive to design new services connected to the Wallet App. European Digital Identity Wallet App providers may have an advantage compared to existing digital identity means providers, although they can also act as platforms for the provision of their services. The size and type of opportunities will also depend on the business model chosen, which will not be prescribed by the Regulation. Finally, the development of standards would also benefit providers by facilitating a harmonised level playing field.
- Similar to option 2, **CABs** would have opportunities to generate additional revenue under this option.

Costs

Finally, the main costs of an EU Digital ID scheme (**Policy Option 3**) are expected to fall on **public authorities** and **Wallet App providers**.

Cost of enforcement by **public authorities** would be represented by:

- The development of standards would generate some costs related to increased international cooperation activities for Member States and around €1-2 million for standard-setting committee work.
- additional costs from familiarisation with standards and any required alignment between the new system and national legislation;
- **Cost of additional supervision activities**. If the first deployment option was chosen, the development of the legal framework would require resources to cover additional supervision activities for public/private Wallet App providers, with costs estimated at around €1.1 million per year across the EU (an average €44,000 a year per Supervisory Body).

The key costs for Wallet App providers would be as follows:

- the costs of first-time development and rollout of the Wallet App could be assumed at about €10 million for the two years 2021/23.
- To make the Wallet app usable the provider would need to incur costs to look after the onboarding of both credential providers and service providers to the ecosystem

- Even though the wallet will be used by end-users, its success depends on the uptake of service providers, which can imply investment in marketing and customer support

- WalletApp providers would need to demonstrate they comply with requirements. These compliance costs are expected to be similar to currently incurred by trust service providers under eIDAS. Providers would also need to obtain security certification, which will also generate a cost.

- In the case of embedded SE, the provider would have to engage in negotiations to request mobile device manufacturers/all relevant mobile network operators to provide access to the SE or eSIM

Preferred option(s)

Our comparative analysis assessed the policy options against one another based on criteria of effectiveness, efficiency, coherence and proportionality. This analysis supports the conclusion that that a combination of options 1, 2 and 3 would best achieve the objectives set for the revision of eIDAS. The combined implementation of these options is considered appropriate in view of the various objectives for the revision of eIDAS and the need to address the existing challenges of the Regulation in terms of legal certainty, coherence and lack of standardisation, which must be fulfilled for the creation of an effective framework for a European digital identity.The preferred combination of options and measures is in line with the subsidiarity principle, as barriers in the EU Digital Single Market cannot be effectively removed through Member State intervention at national level alone.

An important additional factor in the assessment of this preferred option is its impact on the current eIDAS ecosystem and the overall eID market. In particular, the preferred option must demonstrate that it can, through the combination of measures chosen, create synergies and bring significant added-value at EU level while minimising the negative impact on the current market. In the case of the preferred option emerging from this impact assessment — a combination of options 1, 2 and 3— this condition applies in particular to the measures envisaged for eID (which are covered by option 2 and option 3), as they are expected to have the most far-reaching impact on the current eID market.

TABLE OF CONTENTS

LIST OF ACRONYMS

Acronym	Meaning
CAR(s) / CA report(s)	Conformity Assessment Report(s)
CAB(s)	Conformity Assessment Body(/ies)
CN	eIDAS Cooperation Network
EC	European Commission
eID	Electronic identification
ETSI	European Telecommunications Standards Institute
FESA	Forum of European Supervisory Authorities for trust service providers
ID	Identity
MS(s)	Member State(s)
NAB(s)	National Accreditation Body(/ies)
NCA(s)	National Competent Authority(/ies)
OPC	Open Public Consultation
PO	Policy Option
QTS(s)	Qualified Trust Service(s)
QTSP(s)	Qualified Trust Service Provider(s)
SB(s)	Supervisory Body(/ies)
TSP(s)	Trust Service Provider(s)

CATEGORIES OF STAKEHOLDERS

Category in the Study	Description
eID Providers	Entities responsible for verifying that a user is who they claim to be and assert verified data that identifies them to the relying party.
Online Service Providers	Public and private entities offering online services that rely on eID for authentication.
Public authorities	A wide range of Public Sector Bodies having a role in the eIDAS ecosystem: the European Commission, Member States and their representatives in the eIDAS Cooperation network, Supervisory Bodies and Accreditation Bodies.
Conformity Assessment Bodies	A Conformity Assessment Body (CAB) is the legal entity in charge of performing conformity assessments of the TSPs against eIDAS regulation and relevant standards, in order to decide whether they can be given the status of “qualified” or not. A CAB should audit TSPs and submit conformity assessment reports to a Supervisory Body (SB).
Trust Service Providers	According to the eIDAS Regulation, a Trust Service Provider (TSP) is defined as “a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider." For what concerns the impacts analysed in this Study, the Team has included in this category both qualified and non-qualified TSPs, unless otherwise specified.
Citizens and (end) users	Any subject which makes a regular or occasional use of one, or more, online service(s).

1 INTRODUCTION

This document serves as the Final Report for the "Study to support the impact assessment for the Digital ID Act", under specific Service Order N° 2020/666 of the Framework Contract SMART 2019/0024 Lot 1 for the provision for Evaluation and Impact Assessment Services to DG CNECT. The Study was conducted by PwC EU Services and DLA Piper, together with a team of experts composed by: Marc Sel, Riccardo Genghini, Viky Manaila and Massimiliano Tancioni.

1.1 Purpose of the report

The report outlines the final findings and conclusions from the study activities, undertaken between June and March 2021. The activities completed over this period focused on:

- Project set-up activities (Task 0)
- Refining the analysis of the problem through policy interviews and desk research (Task 1)
- Detailing the policy options through policy interviews and desk research (Task 2)
- Filling data gaps on costs and benefits of policy options through sectoral interviews (covering eCommerce, eHealth, Financial Services and Aviation), targeted surveys[11] and in-depth interviews (Task 3)
- Analysing and comparing the options (Task 4)
- Developing policy recommendations (Task 5)

To increase the efficiency of the project, the largest part of data collection activities included under Tasks 1, 2 and 3 was conducted in parallel throughout July and the beginning of August, while some in-depth interviews were conducted in December. It was agreed with DG CONNECT to reallocate resources from the organisation of two workshops to additional data collection activities (interviews and surveys). Based on the results from these activities, the report provides:

- A description of the background of the digital identity initiative, including a definition of the problem to be addressed and the justification for EU action (section 2)
- The definition of the objectives of the revision of the eIDAS Regulation (Section 3)
- A discussion of the policy options under consideration for improving the eIDAS legal framework, and the extent to which they address the problem earlier defined (Section 4)
- An analysis of the potential costs and benefits of the policy options (section 5)
- A summary of the overall impacts identified (section 6)
- A comparison of the policy options against key criteria (section 7)
- The conclusions from our analysis (section 8)

The report is complemented by annexes providing more details on the activities underpinning the research.

[11] One survey was developed and conducted in the realm of this Study, while some relevant questions on Policy Options were added to questionnaires developed in the realm of the *Evaluation study of the Regulation no.910/2014 (eIDAS Regulation) SMART 2019/0046* (Deloitte, VVA, Spark Legal Network, Ecorys. (2020). *Study to support the evaluation of eIDAS - Final Report.* Unpublished.) and in the Open Public Consultation.

1.2 Subject and content of the study

The eIDAS Regulation was adopted in 2014 in order to address the observed market fragmentation in the European Union due to different transposition of Directive 1999/93 on electronic signatures, and to regulate the electronic identification (eID) and trust services, addressing the lack of trust and confidence in electronic transactions. Despite to the fact that an increasing number of transactions take place online, the potential of electronic identification and authentication under eIDAS remains largely underexploited. The Commission seeks to understand these issues better and gather evidence to undertake an impact assessment to thoroughly examine various policy options in the context of the ongoing revision of the eIDAS Regulation's revision (as stipulated by article 49 of the Regulation).

The findings of this study contribute to support the impact assessment of the revision of the Regulation in order to establish a convenient, widely usable, secure and interoperable Digital Identity for the Digital Single Market.

The three specific objectives of the study are:

i. Assess the expected costs and benefits and impacts of different options for policy intervention in the area of digital identity and their components
ii. Compare different policy options available based on the assessment of costs, benefits and impacts
iii. Produce recommendations on the most effective, efficient and coherent policy intervention in the area of digital identity.

2 BACKGROUND OF THE DIGITAL IDENTITY INITIATIVE

2.1 Political and legal context

The eIDAS Regulation introduced a first cross-border framework for electronic identification (eID) and trust services in 2014. The aim of the eIDAS regulation is to enable EU citizens, companies and public administrations to safely access services and carry out transactions online and across borders. [12]

Creating trust in transactions conducted over a network such as the Internet has been identified as one of the main needs for the proper functioning of the Information Society and, from the perspective of the European Union, of the Digital Single Market. Due to the design of the Internet architecture, which considered security as an optional service to achieve an environment in which people feel safe and confident, it is necessary to actively promote the adoption of such security services. In order to increase the level of confidence in the validity and effectiveness of internet activities, a regulation of legal institutions establishing the basis for legal certainty in relation to security services is deemed appropriate.

In this context, the political and legislative agenda, especially in the European Union, has incorporated specific lines of action to recognise the legal effects of electronic equivalents of the main formal elements of the written document; the guarantee of the identity of the parties and the delivery of the consent; the moment of the delivery of said consent; and the

[12] European Commission. (2020). *Inception impact assessment*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-

moments of issuance and reception of the previous elements, when the parties are at a distance.

The eIDAS regulation was designed to address the lack of a common framework for electronic interaction. Specifically, while such framework was already set up for the electronic signature (regulated by Directive 1999/93/EC[13]), there were no frameworks for mutual recognition of eID/e-authentication or for related trust services. This resulted in two key challenges:

- **Fragmentation of the market for e-signatures, electronic identification and related trust services (such as the time stamping, long-term preservation of e-signatures or registered document delivery services).** Despite the presence of an EU-level framework for e-signatures, outdated standards and significant differences in the interpretation of the directive were identified across Member States, leading to a highly segmented landscape and distortion of the internal market. By contrast, identification remained regulated exclusively at the national level, as the Commission had focused on measures to support interoperability, rather than on provision of eID solutions. As a consequence, the adopted eID solutions were diverse across Member States. This also resulted into discrimination of non-nationals and their exclusion to the access to online services, as eID issued in one MS could not be used to access digital services in other Member States. The stakeholders mostly affected by these issues were the providers of eID services/solutions, who faced significant barriers to entry to the markets of other EU countries and in the deployment of cross-border services.
- **Lack of trust and confidence in electronic systems, the tool provided and the legal framework**, which did not enable citizens, businesses and administrations to feel secure in using eIDs when interacting online in cross-border services. Indeed, both public and private sector and end users were affected by this lack of trust, which limited the market, the confidence and ease of use of digital services, and finally the leverage to innovate for public organizations.

The drivers behind these problems were thus mainly related to the uncertainty and lack of an adequate legal framework, the lack of coordination between eSignature and eID developments, the lack of understanding of security guarantees, and the lack of awareness and user adoption. These drivers were extensively analysed in the 2012 impact assessment accompanying the proposal of the eIDAS regulation.

Aware of this context, on 23 July 2014 the Council passed Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), an important and transformative milestone in the legal regulation of the assurances of juridical traffic performed electronically.

As of July 2016, the regulatory framework for trust services applies directly in Member States and in September 2018 the principle of mutual recognition for electronic identities came into effect. Five years from its introduction, the Commission has committed in its Strategy on Shaping Europe's Digital Future[14] to revise the eIDAS Regulation to improve its effectiveness, extend its application to the private sector and promote trusted digital identities for all Europeans. The initiative is linked with the ongoing revision of the eIDAS

[13] Council of the European Union and European Parliament. (1999) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[14] European Commission. (2020). Strategy on Shaping Europe's Digital Future Strategy on Shaping Europe's Digital Future

Regulation[15], which results from the regulatory obligation included in article 49 of the Regulation.[16] The policy direction of this exercise has been further shaped by a strong commitment by the EU institutions to use the revision as an opportunity to not just improve the current framework, but also further the crucial political goal of providing all European citizens with simple, trustworthy and secure public system with which they can use widely to identify themselves in the digital space. The conclusions adopted by the Council on 9 June 2020 on Shaping Europe's digital future[17] also called upon the European Commission to:

"consider proposals for further development of the current framework for cross-border identification and authentication based on the eIDAS Regulation towards a framework for a European digital identity, which would drive the Member States to make widely usable, secure and interoperable digital identities available for all Europeans for secure government and private online transactions."

In her State of the Union Speech, the President of the European Commission Ursula Von Der Leyen, while setting out the EU's technology policy priorities, also announced the Commission's commitment to delivering a secure European Digital Identity:

"We want a set of rules that puts people at the centre. (...) This includes control over our personal data which still have far too rarely today. Every time an App or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will soon propose a secure European e-identity. One that we trust, and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data and how data is used."

In the same vein, the Council Conclusions of 1-2 October 2020 invite the European Commission to come forward with a proposal for a European digital identity framework initiative by mid-2020, calling for[18] :

"the development of an EU-wide framework for secure public electronic identification (e-ID), including interoperable digital signatures, to provide people with control over their online identity and data as well as to enable access to public, private and cross-border digital services".

Article 49 of eIDAS requires the Commission to review the application of the regulation no later than July 2020, particularly to evaluate whether it is appropriate to modify its scope or its specific provisions taking into account technological, market and legal developments.

The revision of eIDAS is driven by the above-mentioned political mandate conferred on the European Commission, as well as the necessity to address the significant challenges

---

[15] European Commission (2019). *Secure electronic transactions – application of EU rules (report)* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/11973-Report-on-the-Application-of-the-eIDAS-Regulation

[16] European Commission. (2020). *Inception impact assessment*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-

[17] Council of the European Union. (2020). *Shaping Europe's Digital Future - Council Conclusions (9 June 2020)* https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf

[18] The Council of the European Union. (2020). *Special meeting of the European Council - Council Conclusions (1-2 October 2020)* https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf

identified with respect to the current eIDAS framework. The latter are further discussed in the section below.

2.2 The digital identity market context

Organisations including Grand View Research, Fortune Business Insights and Global Market Insights predict that the Identity and Access Management market will grow globally to at least 20 billion US dollars[19] by 2026. Meanwhile, Gartner predicts that by 2023, identity solutions will be a multi-billion-dollar industry[20].

2.2.1 The Demand for eID solutions

Demand for eID solutions can be divided into the following categories:

- **Cost efficiency:** One of the main benefits of using digital identity solutions is the potential for efficiency gains, both in private and public sectors. For example, banking sector's digital champions' cost/income rate is 4 percentage points better and return on equity 1,9 percentage points higher than their incumbent peers[21]. The value of strong user authentication, in particular, is to allow service providers to communicate with their customers online with confidence and cut costs of bricks and mortar. The difference in cost of the online and physical channels can be threefold[22].
- **Customer experience**: Managing multiple digital identities has become a considerable burden for users, who are often asked to create a digital identity for each service they want to access. This situation exposes them to various risks and, since most of these identities are not interoperable and their number will constantly increase due to the digitalisation of organisations. This has led to the emergence of new digital ID solutions that are self-managed, or managed by a third party external to the service provider[23]. According to research conducted by the Ponemon Institute, nearly 50% of consumers have been unable to execute an online transaction due to forgetting their password[24]. Today, with an increasing demand for mobile-based solutions[25] along with rapidly increasing mobile penetration[26], European citizens expect their eID to function on their mobile phone[27], with the result that mobile-based eID solutions and digital wallets (where users can store passwords or other identity data) are increasingly popular on the market.
- **Authentication solutions to private online services, using third-party authentication services** (e.g. using a Facebook or Google account to log in to different services), are becoming more common in eCommerce. This way of

19 https://www.fortunebusinessinsights.com/industry-reports/identity-and-access-management-market-100373

20 Gartner: Innovation Insight for Bring Your Own Identity (2019)

21 https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/financial-services/ce-digital-banking-maturity-2020.pdf

22 https://www.fintechfutures.com/files/2018/10/Backbase_The-ROI-of-Omni-channel_Whitepaper-2.pdf

23 Gartner: Innovation Insight for Bring Your Own Identity (2019)

24 Gigya: Social Login 101: Everything You Need to Know About Social Login and the Future of Customer Identity (2015)

25 Since 2016, mobile has overtaken desktop as the main means of accessing websites, with a market share of 53% in 2018: StatsCounter. (2020). Desktop vs Mobile Market Share Worldwide

26 Estimated to reach 88% in 2025: ENISA. (2019). eIDAS compliant eID Solutions

27 This is supported by the results of the Open Public Consultation in which 90% of respondents consider the ability to use their eID on their mobile phone as very important or somewhat important.

authenticating offers convenience, improves conversion rates (due to not forgetting passwords) and helps save costs on password resets[28].

- **Security and trustworthiness**: While convenient solutions such as those offered by platforms are most popular, they lack the level of assurance of identity required by certain sectors (public sector, health, financial etc) and increasingly expected by users concerned about their data protection. According to a Gigya survey, more than 80% of consumers admit to having quit an online registration form because they were uncomfortable with the amount or type of information requested[29]. A recent Eurobarometer survey shows that 88% of consumers wish for more control over their data[30].
- **Secure authentication** will open up service possibilities at a scale that would otherwise not be possible. E.g. the very high uptake of BankID on LOA high (95% usage to access public services) has made it possible to provide digital e-Health services for almost all citizens, offering services such as: patient journal, vaccinations, doctor appointments, e-prescriptions, secure messages, test results (including COVID tests), travel expenses, change of regular doctor.High-profile data security breaches has highlighted the need to counter evolving cyber risks and is driving innovation in digital identity solutions[31]. Technologies such as artificial intelligence, internet of things, data analytics, biometrics, blockchain and mobile technology intersect to establish and verify a claimed identity. Juniper Research reports regulatory technology spending exceed $127 billion by 202432. These technological developments have also resulted in an increasing role and demand for solutions enabling the identification of non-human entities.
- **Regulatory compliance**: Financial services have an increasing amount of requirements on customer authentication such as stringent “Know Your Customer” (KYC), Anti- Money Laundering (AML) and secure authentication requirements for payment services. Telecoms operators are increasingly required to identify their customers and knowing the identity of the customer is needed in some instances in the transport sector as well. A digital identity approach that works securely and seamlessly across borders is needed for the successful implementation and functioning of the Once-only principle that will come into effect in 2023[33]. Secure identification means can support the GDPR[34], allow reliable age verification to protect minors online, and enable emerging use cases such as the digital driving

28 According to Forrester, one password reset may cost up to $70: https://www.onelogin.com/blog/is-password-reset-the-pebble-in-your-businesses-shoe

29 Gigya 2014 Privacy & Personalization Survey (2014)

30 Eurobarometer 503, Attitudes towards the impact of digitalisation on daily lives, December 2019, see : https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2228

31 The European Union Blockchain Observatory and Forum Blockchain And Digital Identity Blockchain For Government and Public Services. (2019) Blockchain and Digital Identity. https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

32 Juniper Research whitepaper ”Opportunities for AI in regtech”

33 The Once Only Principle will, from 2023, allow public administrations to reuse and share data and documents that people have already supplied in a transparent and secure way. (Article 14 of Regulation (EU) 2018/1724 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services. OJ L 295 of 21.11.2018).

34 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88

licence, the IATA travel pass initiative[35], a digital vaccination certificate[36] and the Digital Euro[37]. The importance of these emerging use cases in the context of the COVID-19 pandemic call for a firm link between trusted and secure digital identification and personal digital certificates and attributes that can be managed and shared by the user.

2.2.2 The digital identity solution providers

The main digital identity solution providers on the market are social media, governments, banks, mobile networks, digital identity companies and digital identity networks[38].

A quick and easy way to create a digital identity is through a **social media** account, since this is self-asserted and does not require further authentication processes. This approach is called "social login" and is a form of single sign-on (SSO) which serves to authenticate to a third party platform through existing information stored by a social networking service. Service providers rely on social media login to simplify authentication for the user, and to gain access to data, if permission is given by the user.

The social media login market is dominated by Facebook, Google Sign-In, Instagram, LinkedIn, Twitter and Amazon. These six cover a market share of 87% of social logins in Europe[39]. One of the main reasons for their dominance is the amount of data that these identity providers store and can share about their users to service providers (e.g. name, email address, birthday, gender, city, education)[40]. Amazon is emerging as the main identity provider across eCommerce websites thanks to its capacity to streamline the checkout process[41]. Another reason for social media login leadership may be the sheer number of websites where these solutions can be used to log in; Facebook Login, Google Sign-in, Twitter Sign-in, Instagram Login and LinkedIn Login are used by over 50.000 service providers as solutions to allow users signing in into their websites[42].

The drawback is that being self-asserted, these identity solutions cannot be used for services that require a higher level of assurance in the identity of the person, such as public services or banking, nor satisfy the increasing demand for higher data protection standards. Most recently, platforms and social media also seek to provide ID with higher levels of assurance, in particular in connection with payment services, e.g. Apple Pay, Google-Pay or Libra Facebook.

Government eIDs are backed up by identity proofing according to strict governmental issued and controlled guidelines, and therefore provide a higher level of assurance in the identity of a person compared to social media identities, but at the same time require a longer process to be issued. The fact that these types of identities have a higher level of

35 https://www.iata.org/en/programs/passenger/travel-pass/

36 See e.g. reference to a WHO pilot project with Estonia: https://www.euro.who.int/en/health-topics/Health-systems/digital-health/news/news/2020/10/estonia-and-who-to-work-together-on-digital-health-and-innovation

37 https://www.ecb.europa.eu/euro/html/digitaleuro.en.html

38 Gartner: Innovation Insight for Bring Your Own Identity (2019)

39 LoginRadius: Digital Identity Trends (2019)

40 From a service provider's perspective, it is likely to be more convenient to implement already existing solutions such as the Facebook Login and Google+ Sign In, covering more than a third of the of the world's population (2.8 billion monthly active users combined), unless other solutions offer significant competitive advantages (such as level of trust and assurance, convenience, user experience, frequency of credential use, and link to a physical credential). Gartner (2019), Innovation insight for Bring Your Own Identity

41 Gigya: Social Login 101: Everything You Need to Know About Social Login and the Future of Customer Identity (2015)

42 https://stack.g2.com/

assurance makes them more relevant for use cases that require a higher level of trust. The usage of Government eID's tends to be much more limited[43]. One of the main reasons is that, despite increase demand for secure and reliable eID means, these types of identities are currently mostly offered for accessing public services. While the majority of EU citizens use public services online (67% in 2019[44]), this represents around 7% of all online transactions[45]. Cross-border access to public services is on the rise[46] although the number of use cases requiring cross-border access remains limited if compared with private use[47].

Several government eID schemes are based on a federation of private sector identity (ID) providers, either under the direction of or independent from the government, with examples including notified schemes under eIDAS such as SPID in Italy and ITSME in Belgium as well as schemes outside the scope of eIDAS like BankID in Sweden. Derived identities (i.e. identities derived from official ID documents) such as Verimi are also being introduced[48]. Based on patent surveys there are clear indications that the platforms are considering this approach.

As mentioned above, in the EU, only those national eIDs that have been notified under eIDAS produce legal effects across borders but those effects are limited to public services.

Banks are acting as service providers for eID proofing. The competitive advantage of eIDs provided by banks/financial institutions is that consumers use them regularly to perform financial transactions, and that financial institutions and banks are usually regarded as trustworthy organisations, providing secure online services. However, use cases for such identities are still limited, as many bank digital identity remain closed off to external service providers and digital services in the private sector[49]. Bank digital identity solutions have gained popularity especially in the Nordic countries, where they can be used not only for bank transactions but also for public digital services and an increasing number of enterprises in a wide range of sectors[50].

Mobile network operators provide users with a SIM card that allows them to be identified within their specific mobile network. Here the level of security depends on the identity verification processes imposed in the countries considered. Some countries require a minimal identity verification, while others require a government ID in order to issue the SIM card. GSMA Mobile Connect, enables people to identify and authenticate using their mobile phone[51] without a username and password, providing a globally interoperable solution made available from mobile network operators worldwide. As of August 2020, 23 mobile

43 Gartner (2019), Innovation insight for Bring Your Own Identity.

44 Digital Economy and Society Index Report 2020 - Digital Public Services

45 the Swedish eID is provided by the banking sector and used in private sector transactions mainly, while less than 7% of the total 4.1 billion requests performed in 2019 are related to public sector services which makes it comparable to the number of public sector transactions in Denmark and the Netherlands in that same year.

46 More than 62.000 cross-border transactions in 2020 based on cumulative cross-border authentication for a selection of countries: Austria, Czechia, Estonia, Netherlands, Luxembourg, and Sweden

47 Eurostat, EU citizens living in another Member State - statistical overview, see : https://ec.europa.eu/eurostat/statistics-explained/index.php/EU_citizens_living_in_another_Member_State_-_statistical_overview

48 Deloitte, VVA, Spark Legal Network, Ecorys. (2020). Study to support the evaluation of eIDAS - First Interim Report. Unpublished.

49 Gartner: Innovation Insight for Bring Your Own Identity (2019)

50 https://www.bankid.no/en/company/

51 https://www.gsma.com/identity/developer-portal

network operators[52] have made the Mobile Connect authentication service available for their users, while a further 11 are piloting it. Major EU telecommunications providers already providing the Mobile Connect solution include Telefonica, Orange, Deutsche Telekom, Vodafone Germany, Telia, T-mobile, and KPN. A secure element (e.g. a tamper-proof chip ensuring safe storage of data) embedded in the mobile device allows for using applications on the phone that requires data security, such as a mobile eID.

Dedicated digital identity companies offer users the opportunity of creating a digital identity by following a registration process backed up by already existing ID documents (e.g. driving license, passport), social media identity, or other certificates, and at the same time increasing the security of these identities with biometric tools such as facial recognition. These solutions offer portability and employ advanced technologies such as biometrics to better protect the identity. Some of the solutions available include: Yoti (UK)[53], SisuID (FI)[54], GlobalID (CH), Onfido (UK), Chekk (HK), Janrain (US), Gigya (IL)

Digital Identity networks are not identity providers, but are instead a sort of facilitator between identity providers and service providers[55]. These solutions are considered a trusted, safe and secure way to verify users' identity online, as their business model consists in providing the network participants (identity and service providers) with an infrastructure where they can exchange identity information of users. Included within this category are "**derived identity" providers**, which draw on existing digital identities to create a new, more user-friendly one. Examples of this type of solution are provided by MasterCard (US), Verimi (DE) and Yes (CH).

Identity-as-a-service (IDaaS) are cloud-based authentication or identity management systems. Such solutions free organisations from the development and monitoring costs associated with managing their own internal access management solutions. Solutions available on the market are provided by operators including Atos (Evidian) (FR), Auth0 (US), Broadcom (CA Technologies)(US), ForgeRock (US), IBM (US), Idaptive (US), Micro Focus (UK), Microsoft (US), Okta (US), OneLogin (US), Optimal IdM (US), Oracle (US), Ping Identity (US), SecureAuth (US)[56]

2.2.3 Key market developments

Since the introduction of eIDAS, the global eID ecosystem has undergone fundamental changes, with digital services becoming the preferred choice for EU citizens and new digital identity business models and players emerging in response to this[57]. More and more banks, telecommunications operators and post offices are now acting as service providers for eID proofing. Several eID schemes are now based on a federation of private sector identity (ID) providers, either under the direction of or independent from the government, with examples including notified schemes under eIDAS such as SPID in Italy and ITSME in Belgium as well as schemes outside the scope of eIDAS like BankID in Sweden. Derived identities (i.e.

52 See https://developer.mobileconnect.io/operators?title=&name_list=All&field_mobile_connect_status_value=2

53 https://www.yoti.com/

54 https://www.biometricupdate.com/201912/finnish-ministry-tests-sisuid-biometrics-nixu-restructures-amsterdam-team

55 Gartner: Innovation Insight for Bring Your Own Identity (2019)

56These services are delivered to a service provider through a remote connection from a third-party provider, as opposed to the feature being managed on site and by in-house personnel alone. Solutions provided by such cloud service providers may be more reliable and robust than in-house security and authentication systems. Solutions available on the market are provided by operators including https://www.gartner.com/en/documents/3956209/magic-quadrant-for-access-management

57 Domingo, A. I. and Enríquez, A. M. (2018). *Digital Identity: the current state of affairs.* BBVA. https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf

identities derived from official ID documents) such as Verimi are also being introduced.[58] As a result, governments are no longer the only dominant identity providers for their citizens, as they were at the time of the adoption of the eIDAS Regulation (2014).

This has created a fragmented landscape of private sector eID solutions that are operated in the absence of clear rules and obligations and with insufficient transparency over security levels and data protection[59], especially compared with the notified schemes. In particular, the fact that the large majority of these eID solutions are currently not covered by the eIDAS Regulation means that these identities often lack a systematic link with a verified legal identity; consequently, citizens and businesses cannot compare the security and level of assurance that these different digital identity solutions provide, creating more opportunities for fraud and increased cybersecurity threats[60].

One the most significant trends associated with the growing provision of identity solutions in the private sector is the rising role of major online platforms as identity gatekeepers. Online platforms share some important and specific characteristics, which the European Commission[61] defines as follows:

- the ability to create and shape new markets, to challenge traditional ones, and to organise new forms of participation or conducting business based on collecting, processing, and editing large amounts of data
- the fact that they operate in multisided markets but with varying degrees of control over direct interactions between groups of users
- the benefit they derive from 'network effects', a dynamic whereby the value of an online service or platform increases with the number of its users, who consequently attract new users, and hence exponentially increase the market success of the service or platform[62]
- their reliance on information and communications technologies to reach their users, instantly and effortlessly
- their key role in digital value creation, notably by capturing significant value (including through data accumulation), facilitating new business ventures, and creating new strategic dependencies

These features of online platforms have brought a range of important benefits to the digital economy and society, for instance in terms of efficiency, consumer choice and data-driven innovation. At the same time, they create concerns about market power, as well as user control over their personal data and the transparency of data processing. This issue particularly applies to their growing role in digital identity. Large online platforms are increasingly moving into digital identity provision, promoting the integration of several platforms by allowing users to log in third-party applications using their social network profile[63] through the so-called social login solutions. This creates concerns over user data privacy and control, market power and its impact on the level playing field where a

[58] Deloitte, VVA, Spark Legal Network, Ecorys. (2020). *Study to support the evaluation of eIDAS - Final Report.* Unpublished.

[59] PwC. (2019). *Digital identity: Your key to unlock the digital transformation*

[60] Deloitte, VVA, Spark Legal Network, Ecorys. (2020). *Study to support the evaluation of eIDAS - Final Report.* Unpublished.

[61] European Commission. (2016) *Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe*

[62] D-CENT project. (2013). *Research on Identity Ecosystem*

[63] D-CENT project. (2013). *Research on Identity Ecosystem*

competitive European digital identity user-empowering services market could develop, if left unregulated. [64]

Social logins

Social logins allow users to access apps or websites using their existing accounts on large platforms such as Amazon, Google, Facebook, Twitter, and LinkedIn. There are three main players involved in a social login process: firstly, the user requesting access to an app or site; secondly, the app or website providing the service that the user wants to access; thirdly, the authoriser i.e. the platform providing the social login, which is responsible for confirming the user's identity and controls access to her data[65].

A typical social login entails the following steps[66]:

- The User chooses how to log-in into an app or website. If a social log-in option is available, the "Log in with ____" button will be displayed.
- When selecting the social log-in option, the user is re-directed to the Authoriser's site and asked to login (if not already logged in). During this process, the Authoriser will receive information on which third party app or website is making the login request and give the user information on the type and extent of the data that will be shared with that third party.
- By pressing the "continue" button, the user is redirected to the third party website with a one-time authentication code. This is done by the authoriser in order to confirm to the third party website that the user holds a valid account with them.
- The authoriser verifies the identity of the third party website by validating the unique code acquired by the third party generated for the when it first registered itself with the authoriser. At this point, it will issue an access token to the website that allows it to request certain account information about the user from the authoriser.

To complete this process, most third-party login services use some combination of the OpenID and OAuth protocols. The OpenID Connect Protocol deals with authorising users i.e. the authoriser confirming to the third party the user's identity (via user log-in into their account on the authoriser's website), while the OAuth protocol governs how the third parties can access the user's data from the platform (e.g. name, age, gender, interests, friends)[67].

Beside convenience, an advantage of these methods is that the user's username and password are not passed on to the third party, meaning that they cannot be hacked from the third party's website. Further, this can benefit security by minimising re-use of passwords. Nevertheless, social logins may create significant issues from a privacy and data protection perspective:

- In case of security attacks on the authoriser, hackers may still that account and use it to impersonate the users in all third-party services. Past experience shows that such attacks are rare, but do happen with potentially significant consequences for millions of users. In 2018, a security breach giving hackers the possibility to completely take over Facebook user accounts compromised nearly 50 million accounts[68].

---

[64] European Commission. (2020). *Inception impact assessment*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-

[65] A. Braun. (2019). *Are Third-party social logins Secure and Private ?* https://www.maketecheasier.com/are-social-logins-secure-private/

[66] A. Golman. (2018). *Social Login & 3rd-Party App Authorization.* https://medium.com/@golman.alan/social-login-3rd-party-app-authorization-f228a3f8ae23

[67] A. Braun. (2019). *Are Third-Party Social Logins Secure and Private?*. https://www.maketecheasier.com/are-social-logins-secure-private/

[68] J. C. Wong (2018) *Facebook says nearly 50m users compromised in huge security breach.* The Guardian https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach

- Significant amounts of data closely related to the identity of the user may be shared, often in ways and for purposes that are not fully intended or understood by users due to the complexity or incompleteness of privacy policies. Shared data might include user's behavior tracking and using this data for personalized ads and customised content without the user's full awareness. For example, a study found several occurrences of third-party trackers embedded on a third party website getting the user's data when she authorizes that website to access her Facebook profile

The identity solutions developed by major social platforms offer convenience, allowing users to avoid using a multitude of username and password combinations (which also mitigates security risks). Yet, this comes at the cost of losing control over disclosed personal data, as:

- these solutions are most often of a lower level of assurance as they are disconnected from a verified physical identity, which makes fraud (such as identity theft) and cybersecurity threats more difficult to mitigate.
- the frequent practice of using one's platform profile to access a range of websites and services often involves non-transparent exchanges and cross-linkages of personal data between various online platforms and websites. For instance, research conducted in the US indicates that 74% of Facebook users did not know Facebook maintained a list of their interests and traits, and 51% did not feel comfortable with this[69]. This lack of transparency means that users are not always adequately informed about how their data is used, including for shaping the content presented to them (e.g. purchase recommendations).
- platforms' privacy policies are often long, fragmented and presented as 'clickwrap' agreements, i.e., as a condition of using the service, the consumer must accept the terms of those policies.[70] The architecture of user choice itself can also be designed in a way that discourages users from making pro-privacy decisions. As a result, too often users are not presented with genuine choices over the terms of their data processing by these platforms.

The European Commission's Communication on online platforms[71] suggests that, in order to keep identification simple and secure, consumers should be able to choose the credentials by which they want to identify or authenticate themselves and online platforms should accept credentials issued or recognised by national public authorities, such as electronic or mobile IDs, national identity cards, or bank cards. This is currently not the case.

2.2.4 Wider social and technological developments

The market is also being shaped by **social, economic and technological developments that are rapidly changing the electronic/digital identity solution landscape** and with it, user habits, priorities and concerns when transacting online. The pace of these changes is such that the Regulatory framework is considered no longer fit for purpose and needs to adapt as quickly as possible to the challenges they raise.

Traditional approaches to digital identity verification have been focused on the creation of static digital identities based on cryptographic tools like digital signatures and digital

[69] Pew Research Center. (2019). *Facebook Algorithms and Personal Data* https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/

[70] Competition and markets authority (2019) *Online platforms and digital advertising – market study interim report*

[71] European Commission. (2016) *Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe*

certificates. This represents the basic model on which most national eIDs and traditional Know-Your-Customer processes are built and are increasingly seen as cumbersome because of their lack of good integration with Internet-based services. Such approaches are being outpaced by dynamic verification models which use multiple sources (including, for instance, the user's mobile phone, his social media activity, geolocation, etc.), characterised by low levels of assurance (as identities are usually self-asserted) but high levels of user convenience .[72] This represents a fundamental change in technological paradigms linked to identity with wide-ranging implications on user expectations.

For example, this can be seen in the increasing demand for mobile-based solutions, helped by rapidly increasing mobile penetration around the world (estimated to reach 88% in 2025)[73] Since 2016, mobile has undertaken desktop and the main means of accessing websites (with a market share of 53% in 2018)[74] and is currently used to access online services in a variety of sectors[75]. The OPC also indicates that 90% of respondents consider the ability to use their eID on their mobile phone as very important or somewhat important. As a consequence, a vast majority of European citizens have come to expect services to be available on mobile. These services are structurally different because they are inherently coupled with cloud systems. The eIDAS technical specifications, by contrast, have been initially designed when most of the access to online public services where taking place based on computer session. Member States have been sceptical regarding the possibility of designing mobile-only eID solutions, six out of the 14 countries that have notified an eID schemes have notified mobile solutions. A key concern is that this would increase the user exposure to identity theft as a wider attackable surface is created through online mobile connection. This security pitfall can be challenging to be reconciled with evolving user preferences. [76]At the same time, the security of electronic identity data online is increasingly challenged by rising security breaches and online fraud[77]. Nowadays it is very difficult for individuals to have an idea of who is gathering information about them. Once in the digital world, it is very easy to store, copy or use our data, without consent. The increasing frequency of high-profile data security breaches has highlighted the relative lack of control over their personal sensitive data for many users [78] and created greater demand for security and trust.[79] Recent surveys show that 88% of consumers want more control over their data.[80] The eIDAS Regulation, in its current implementation, is ill suited to support a shift towards greater empowerment of users over their personal data, as:

---

[72] Domingo, A. I. & Enríquez, A. M. (2018). *Digital Identity: the current state of affairs.* BBVA. https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf

[73] ENISA. (2019). *eIDAS compliant eID Solutions*

[74] StatsCounter. (2020). Desktop vs Mobile Market Share Worldwide

[75] ENISA. (2019). *eIDAS compliant eID Solutions*

[76] Strategic interviews

[77] ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends - Jan 2019

[78] The European Union Blockchain Observatory and Forum Blockchain And Digital Identity Blockchain For Government and Public Services. (2019) *Blockchain and Digital Identity.* https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

[79] Domingo, A. I. & Enríquez, A. M. (2018). *Digital Identity: the current state of affairs.* BBVA. https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf

[80] Experian. (2010). 2020 *Global Identity and Fraud Report.* http://images.go.experian.com/Web/ExperianInformationSolutionsInc/%7B4c9cc02b-353a-4f07-9abe-2449234853dd%7D_global-identity-and-fraud-report-2020.pdf

- It provides for automated transfer of the full eIDAS minimum data set to the service providers. In December 2019 and therefore does not allow for a minimal disclosure of data or encourage privacy-by-design
- it does not enable a full data portability of citizens' and businesses' identity attributes due to the restrictive set of attributes available
- it does not support re-use of identity and KYC verification procedures (remotely or in persons)

Equally, businesses face significant challenges in navigating the complexity and risks (including regulatory) associated with their responsibility to protect such data and to verify the identity of their counterparts, given rapidly rising rates of identity theft and fraud in online transactions.[81]

Innovative solutions have already arisen in the private sector to provide an effective response to these phenomena. In fact, much of the most cutting-edge innovation in digital identity solutions is now coming from outside the core eID/TSP sector.[82] Demand for instant, secure and convenient online transactions and evolving cyber risks is already driving innovation in digital identity solutions, where technologies such as AI, IoT, analytics, biometrics or mobile intersect to establish and verify a claimed identity online. Consequently, the extent to which the EU leads on digital ID innovation and regulation will strengthen Europe's technological autonomy and the ability of European businesses to compete globally. [83]New technological trends, such as the expanded potential for application of mobile solutions, biometrics, artificial intelligence, analytics enabling real-time and continuous authentication, the Internet of Things, citizen-controlled data, analytics and blockchain, may help increase the availability and uptake of eID schemes that enhance user experience and mitigate cyber risk. [84]However, stakeholders have raised concerns that the development of biometrics for identity verification and authentication has not been accompanied by an increased level of scrutiny or guidance at the EU level despite the sensitiveness of the data at stake.

Further, these technological developments have also resulted in an increasing role for non-human entities in identification processes. Despite increasing demand, available solutions do not support identification of devices, sensors, monitors, to manage their access to sensitive and non-sensitive data. Business opportunities remain untapped and secure identification costs remain excessive, such as in banking and finance, as long as trusted public eID cannot be used widely and conveniently in the private sector and/or market-based solutions are not supported by regulation. [85]

Alongside technological developments, other factors in the wider European and global society are re-shaping the demand for electronic identification and prompting a change in approach by market operators and legislators. In particular, the ongoing public health and economic challenges brough about by the COVID-19 pandemic have both demonstrated

[81] The European Union Blockchain Observatory and Forum Blockchain And Digital Identity Blockchain For Government and Public Services. (2019) *Blockchain and Digital Identity*. https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

[82] Davidson, S. (2019). *Remote Identity Validation for High Assurance Certificates*. https://www.enisa.europa.eu/events/tsforum-caday-2019/presentations/ca-10-davidson

[83] European Commission. (2020). *Inception impact assessment*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-

[84] Domingo, A. I. & Enríquez, A. M. (2018). *Digital Identity: the current state of affairs*. BBVA. https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf

[85] European Commission. (2020). *Inception impact assessment*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-

the value of secure remote identification for all citizens to access essential everyday services and exposed the limitations of current approaches to eID by market operators and legislators alike.

Since the early months of 2020, COVID-19 has been forcing several countries worldwide into lockdowns and other extreme restrictions, and resulted in many citizens remaining isolated from social contact and increased demands on service providers and governments. This has left most countries, including in Europe, at a loss as to how to ensure continuity in business public service and social interactions in such an unprecedented mass emergency with no certain end date in sight. Additionally, it has created additional demands on public and private service providers, as well as governments. In particular:

- Governments have enacted various measures to contain the spread of COVID-19 whose success depends on their capacity monitor compliance by millions of citizens, such as restrictions on large public events and gatherings, restrictions on travel, new health and safety measures for places of work, business and public spaces, and obligations for COVID patients and all those that have come into contact with one to self-isolate (often attached to criminal sanctions and fines). These have put to the test public authorities' capacity to conduct such enforcement and monitoring through traditional means.
- Prolonged self-isolation of millions of individuals has created taxing demands on businesses both as employers and as providers of goods and services. In their role of employers, they have faced the greatest challenge in having to rollout remote working for their employees at an unprecedented scale and with various starting levels of digitalisation of their workflows. As goods and service providers, they have faced substantial disruptions to their supply chains and everyday transactions with suppliers and customers, which have gone as far as undermining their business models and creating substantial distress for their customers. A clear example can be found in the steep surge in online purchases since the start of the emergency, which has left many online merchants unable to manage the volume of orders received at peak times and significantly more exposed to fraud[86].
- Self-isolation of citizens due to COVID-19 has also forced a rethinking in how access to essential services – whether publicly or privately supplied – and the exercise of citizens' rights can be guaranteed in the face of significant disruptions and rising needs. For instance, the emergency has forced many countries to temporarily interrupt driver licensing services and to request additional documentation from freight road transport operators at border checks, which impacted essential goods transport and passenger transport within and among EU Member States[87]. A respondent to the OPC also identifies a gap with respect to electronic voting:

  "Electronic voting has been found as a missing service during the COVID-19 crisis. Many organizations, associations, etc. have not been able to securely hold necessary elections due to the lack of a trustworthy solution to handle anonymous voting with appropriate protection of the voter. A Qualified Trust Service Provider will be able to provide missing functionality, security and trustworthiness to the European society."

Meanwhile, some governments and businesses have found in digital identities a powerful tool to mitigate the challenges created by the pandemic, with various levels of success. In fact countries with higher levels of digitalisation and well developed digital identity systems,

[86] Experian. (2020). *Survey: The Impact of COVID-19 on Fraud and Identity Theft*

[87] IRU (2020) *COVID-19 urgent EU action needed on road borders, drivers and financial support*

such as Canada[88] and Estonia[89], have fared better in minimising disruptions to their economy and society. The response by citizens has also seen a step change in many countries, possibly by better awareness of the benefits of digital identification. For example, the number of credentials issued under SPID (the national eID system for Italy, notified under eIDAS) has doubled in March 2020 (at the peak of the emergency for the country) compared with March 2019, with an average 1,000,000 credentials issued per week.[90]

The results from the OPC also underline the increased demand for eID and trust services in the COVID-19 emergency. Nearly 60% of respondents have found the availability of the eID means or the electronic trust services (e.g. electronic signature) particularly useful during the lockdown measures introduced due to the COVID-19 crisis. A majority of respondents agreed that the eIDAS Regulation in general (64% of respondents), the eIDAS legal framework for cross-border eID in Europe (69% of respondents), and the availability of eSignature (77% of respondents), eSeal (70% of respondents), eTimestamp (66% of respondents), ERDS (68% of respondents) and website authentication (54% of respondents) in the EU should be extended as a result of the COVID-19 crisis.

While demonstrating the role of digital identity as critical infrastructure for the economic and resilience of Member States, the Covid-19 emergency has also underlined the importance of nurturing confidence by all users in trusted digital identities so that they are not excluded from the essential access to goods and services that these enable in a time of crisis.

2.2.5 End user demand for eIDAS-notified schemes

Secondly, since cross-border authentication of citizens will make up a small fraction of public sector use cases, broad application across public and private services will be needed to recover the cost of creating the notified schemes in the first place and ensure the eID ecosystem created by eIDAS effectively supports the deepening of the Digital Single Market within the EU. [91]

Despite the progress achieved on increasing the availability of notified eID, the actual take-up/ usage by citizens in terms of the number of cross-border authentications performed using notified eID schemes or identities issued has been limited. The evaluation study of eIDAS indicates that:

- While there is a clear trend towards an exponential growth of domestic transactions in recent years, the number of cross-border authentications remain low (<10 000 authentications per year) compared to the usage of eID at the domestic level (> millions authentication per year) and is unlikely to grow significantly in the future
- The number of unique users per eID scheme (based on figures for 15 Member States for both notified and non-notified national schemes) has grown in recent years, but adoption rates vary significantly across Member States. Figures show a range between 1% and 96% (or 103% for Estonia, the only country issuing eIDs to foreign citizens) and are partly driven by differences in national approaches to

[88] Baumgart, D.C. (2020), *Digital advantage in the COVID-19 response: perspective from Canada's largest integrated digitalized healthcare system.* npj Digit. Med. 3, 114 (2020). https://doi.org/10.1038/s41746-020-00326-y

[89] Krusten, M. (2020) What happens to a fully digitalised society during a pandemic lock-down?

[90] AgID (2020) *SPID: aumento sostenuto di identità digitali, 100mila a settimana*

[91] GSMA. (2018). *Mobile Connect for Cross-Border Digital Services Lessons Learned from the eIDAS Pilot*. https://www.gsma.com/identity/wp-content/uploads/2018/02/MC-for-cross-border-digital-services_eIDAS_Feb2018-Final.pdf. https://www.gsma.com/identity/wp-content/uploads/2018/02/MC-for-cross-border-digital-services_eIDAS_Feb2018-Final.pdf

issuing identities (e.g. universal or voluntary issuance, minimum age for obtaining such identities).

Based on primary and secondary data collection for this study, the key causes behind insufficient end user adoption and confidence are identified primarily in a **lack of wide usability of solutions across private and public online services, a lack of awareness and understanding of the benefits of eIDAS solutions, as well as a lack of user convenience and control over data protection & privacy.**

As for the first cause, the evidence available suggests that public-sector use cases are not high-frequency and high-interest for users. Stakeholders consulted have suggested that the average citizen in their country will need identification 1.5 times per year to access public services, whilst her need to identify for access to private services will be 10 times greater. Figures from Sweden, whose national eID scheme is provided by the banking sector, also indicate that private sector services account for the bulk of transactions requiring eIDs: only 7% of the total 4.1 billion transaction requests performed in 2019 are related to public sector services.[92] Therefore, private sector use cases can help create user acceptance and familiarity in digital authentication. Moreover, it is easier for the individual if they can use the same authentication method for both public and private sector use cases. [93]

Secondly, a number of studies conducted on eIDAS[94] have clearly shown awareness of the benefits of using eIDAS solutions among potential users (both end users and service providers with customer identification needs) to be low. Even for end users that have applied for an eID and see its advantages, the use itself may be unintuitive, time-consuming and not always functioning due to several reasons including a mismatch of data between countries and the inability to authenticate when overseas.[95]

In terms of the lack of user convenience and control over data protection & privacy the significance of user-centricity in the design of digital public services has been underscored recently by the Tallinn Declaration of 6 October 2017, signed by all Member States and EFTA countries. Member States, however, have lacked a coordinated approach to the design and roll-out of the cross-border authentication user journey. Combined with the complexity of cross-border utilisation of these eIDs (entailing interfaces provided by multiple entities in two different countries) this has sometimes led to poor user experience.[96] Poor user experience seems to be the prevailing source of users' reluctance in using notified eID schemes, while the eIDAS framework per se is generally rated highly on trust by stakeholders. As part of the OPC, 73% of respondents mentioned that eID under eIDAS

---

[92] Deloitte, VVA, Spark Legal Network, Ecorys. (2020). Study to support the evaluation of eIDAS - Final Report. Unpublished.

[93] GSMA. (2018). *Mobile Connect for Cross-Border Digital Services Lessons Learned from the eIDAS Pilot*. https://www.gsma.com/identity/wp-content/uploads/2018/02/MC-for-cross-border-digital-services_eIDAS_Feb2018-Final.pdf. https://www.gsma.com/identity/wp-content/uploads/2018/02/MC-for-cross-border-digital-services_eIDAS_Feb2018-Final.pdf

[94] See, for example: PwC EU Services EEIG. (2018). *Study on a marketing plan to stimulate the take-up of eID and trust service for the Digital Single Market*. https://ec.europa.eu/futurium/en/system/files/ged/study_on_marketing_plan_takeupeidas_final_report.pdf ; Deloitte , The Lisbon Council. (2019). *eIDAS study on pilots for replication of multipliers: supporting the uptake of eIDAS services by SMEs*. https://op.europa.eu/en/publication-detail/-/publication/712f9ce2-5042-11e9-a8ed-01aa75ed71a1/language-en

[95] Deloitte, Ecorys, Spark Legal Network, VVA. (2020). *Study to support the Evaluation of the eIDAS Regulation: First Interim Report* (unpublished).

[96] European Commission. (2018). *The user experience of eIDAS-based.* https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Final+report%3A+The+user+experience+of+eIDAS-based+eID%3A+Looking+ahead

has led to an increase of the certainty on the authenticity of the users' identity, and 66% report an increase in service security.

In previous user experience research conducted on eIDAS, several participants mentioned the complexity and low user-friendliness of certificate-based solutions as a recurring issue preventing the broader adoption of such solutions in the market. For end users, the mandatory use of a material support such as a smartcard or a USB token for qualified solutions makes the solutions complex to implement and manage for the business service providers. Additionally, the lack of convenience of these solutions for the business service users results in limited adoption among business service users and reduces the potential for business service providers. [97] Recent business surveys show that 75% of businesses want advanced authentication and security measures that have little or no impact on the digital customer experience.[98]

The lack of widely available solutions that guarantee cross-border recognition and control over data protection & privacy is also a factor preventing all European citizens from being able to reap the benefits of the Digital Single Market. While citizens in some Member States do currently have access to options that meet these requirements thanks to eIDAS, such access is not guaranteed to all. As previously stated, at current 59% of the European population is covered by eIDAS-notified schemes; only a fraction has access to notified schemes that can be used for private sector transactions. Further, the extent to which these schemes are consistent with privacy by design principles is variable, as some concerns[99] have been expressed over the effectiveness of the eIDAS Regulation in promoting the effective application of such principles.

2.3 The eIDAS Regulation

The main objectives of the eIDAS regulation, and the relevant definitions and articles for the purposes of this study, are described below.

2.3.1 eID

2.3.1.1 Ensure mutual recognition and acceptance of notified eIDs

Article 3 of the eIDAS Regulation defines electronic identification as the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person. The following definitions are also provided in the article:

- 'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service
- 'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons

Article 6 of the eIDAS Regulation sets out the principle of mutual recognition of eID means to access online public services. The obligation of mutual recognition consists in ensuring that notified eID schemes issued by other Member States be recognised if electronic

[97] European Commission. (2018). *The user experience of eIDAS-based.* https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Final+report%3A+The+user+experience+of+eIDAS-based+eID%3A+Looking+ahead

[98] Experian. (2018). *The 2018 Global Fraud and Identity Report.* https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf

[99] See for example The Council of European Professional Informatics Societies. (2015). *Position on the Electronic identification and trust services (eIDAS)* and ABC4Trust. (2015). *ABC4Trust Position on the eIDAS Regulation*

identification using an eID means is required under national law or by administrative practice to access an online public service provided in a given Member State, as long as they can provide the minimum level of assurance required by the online public service in question. Under this obligation, Member States are mandated to adapt their respective technical systems within one year of the publication of the notification of an eID scheme in the Official Journal of the European Union.

Article 12 of the eIDAS Regulation and implementing act 2015/296 articulates the arrangements for the cooperation between Member States, including the peer review of eID schemes as part of the notification. By this process, experts representing all Member States in the Cooperation Network on eID can participate on a voluntary basis in a peer review of the interoperability and security of a notified scheme (prior to its formal notification). As such, the process is designed to build helps to strengthen mutual trust and cooperation between Member States, and build their confidence in the interoperability and security of eID architecture schemes (as per Article 7 of the eIDAS Implementing Decision 2015/296).

2.3.1.2 Ensure cross-border interoperability of eID

According to Article 12 of the eIDAS Regulation, notified national eID schemes shall be interoperable and an interoperability framework shall be set up for this purpose. The article set out the architecture of the eIDAS network based on national nodes, foreseeing the adoption of technical specifications notably for the eIDAS minimum data set and message format, as well as minimum technical requirements in relation to the assurance levels of the notified eID schemes.

2.3.1.3 Ensure usage of notified eID by public and private sectors

Article 7 also establishes a process by which Member States can make their national eID schemes available for cross-border and cross-sector use, with the aim to **ensure usage of notified eIDs by public and private sector entities**.

2.3.2 Trust services

2.3.2.1 Ensure trust and confidence in the legal certainty and security of trust services

Article 3 of the eIDAS Regulation defines a trust service as an an electronic service normally provided for remuneration, consisting of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- the creation, verification and validation of certificates for website authentication; or
- the preservation of electronic signatures, seals or certificates related to those services

Trust service providers can be qualified or non-qualified. Qualified trust service providers (QTSPs) are trust service providers that have been granted the qualified status by the Member State's designated supervisory body and who provide one or more qualified trust services.

The Regulation provides for non-discrimination of electronic forms vis-à-vis the paper equivalent, establishing that trust services compliant with the requirements laid out in the Regulation 'shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form'. Notably, Article 4 prohibits restrictions of trust services in the territory of a Member State by a trust service provider

established in another Member State, providing a building block for the internal market and promoting fair competition and growth of the cross-border use of trust services.

Trust service providers and trust services deemed to comply with the requirements laid down in the Regulation shall be granted the status of 'qualified'. Under the Regulation, QTSPs benefit from a presumption of reliability and mutual recognition between Member States for the specific service for which they have qualified status. Article 24 lays down further specific requirements for QTSPs. In particular, the article set out that when issuing a qualified certificate QTSPs shall verify to whom the qualified certificate is issued by either the physical presence of the natural person, remote electronic identification means or by using other identification methods recognised at Member State level. Further, QTSPs must provide any updates of change to its organisation to the supervisory body, in order for the supervisory body to maintain the trusted list.

2.3.2.2 Ensure an optimal scope and level of governance

The supervision framework established for the trust services under the Regulation comprises of three main bodies – the supervisory body, conformity assessment body (CAB) and the national accreditation body. Each Member State is obliged to establish one of each of these bodies for supervision purposes under the eIDAS Regulation.

The role[100] of the supervisory body is defined in Article 17 as initiating and supervising qualified trust service providers (QTSPs) established in the territory of the designating Member State(s), with the aim of ensuring (through ex ante and ex post supervisory activities) that the QTSPs continue meeting the requirements of the Regulation.

Additionally, Article 18 of the Regulation provides for the principle of mutual assistance between supervisory bodies, ruling that a supervisory body shall provide assistance upon a justified request from another body on matters such as information requests and requests to carry out inspections related to conformity assessments and joint investigations where appropriate.

Under Article 20, which governs the supervision of QTSPs, these are to be audited at their own expense at least every 24 months by a conformity assessment body in order to confirm that the QTSP and the QTSs it provides meet the requirements laid down in the Regulation. This provision tackles the issue of market fragmentation and a lack of trust that occurred as a result from the patchwork supervision that occurred under the old framework. The provision lays down a common level of supervision to be implemented in all Member States, thereby also in terms of costs.

2.3.2.3 Creating a fairer playing field for trust service providers

The Regulation establishes a European wide supervision regime that aims to level the playing field for trust service providers, enhance trust and confidence in services offered by a service provider established in another Member State, and thereby increase the take-up of services in the European market.

According to Article 21, Conformity Assessment Bodies (CABs) are responsible for providing a conformity assessment report for the purposes of initiating QTSPs and conducting conformity assessments at later stages to ensure that the necessary regulatory requirements are being met. In order to be initiated, Article 21(1) states that trust service providers must ask their relevant CAB to produce a conformity assessment report confirming whether or not the trust service provider meets the requirements laid out in the

[100] Article 17(3)(a) and (b)

Regulation. The trust service provider must then provide this report to the supervisory body within three days of it being made available by the CAB to the trust service provider. Conformity activities carried out by the CAB include calibration, testing, certification and inspection. Under Article 18 of the Regulation, all CABs must be formally accredited by the Member State's appointed national accreditation body, who has authority from the derived state.

Article 22 requires each Member State to establish, maintain and publish trusted lists (which can include both qualified and non-qualified TSPs), including information related to the qualified trust service providers for which it is responsible, including their history. These are meant to provide a reliable source to validate and verify the status of a trust service provider and its trust service at any given point in time. Following the initiation of a QTSPs, the supervisory body is obligated to notify the Commission on any changes made to the relevant Member State's Trusted List.

2.3.2.4 Stimulate the take-up of trust services

Article 23 introduces the EU Trust Mark[101], which aims to ensure trust and confidence in the legal certainty and security of the TSPs and trust services being offered. Only QTSPs can use the EU trust mark to signal in an user-friendly manner that they provide eIDAS-compliant services.

Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 also contributes to this objective laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies. This requires Member State public authorities to put in place the necessary technical means that allow them to process electronically signed documents when using an online service offered by, or on behalf of, a public sector body.

2.4 Problem definition

2.4.1 What are the problems?

2.4.1.1 State of play of the implementation of eIDAS:

As regards eID: Since the entering into force of the eID part of the Regulation in September 2018, only 14 Member States[102] have notified at least one eID scheme, and four Member States have notified multiple schemes[103]. In total, 19 eID schemes have been notified so far[104]. By March 2021 three Member States[105] have pre-notified their schemes. For the 59 % of EU citizens that do have the possibility to use trusted and secure eID scheme across borders, in most of the cases they do not respond to their needs.

---

[101] the form of the EU Trust Mark is instead set out in Commission Implementing Regulation (EU) 2015/806 of 22 May 2015

[102] BE, CZ, DE, DK, EE, ES, HR, IT, LV, LT, LU, NL, PT, SK, The United Kingdom notification of UK.GOV Verify (on 2 May 2019) is not included in this analysis.

[103] Belgium, the Netherlands, Italy and Portugal. A number of notified eID schemes includes multiple eID means (e.g. in case of Estonia the eID card and Mobiil-ID, amongst others).

104 Overview of pre-notified and notified eID schemes under eIDAS: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

[105] France, Malta and Sweden

Many Member States services that have notified an eID have not made accessible to holders of eIDAS eIDs many services accessible to nationals due to technical implementation weaknesses at the level of Member State.[106]. For example, using a notified eID to access an online public service of the tax authorities in another Member State is denied because the back bone services of the tax authority have not been connected to the eIDAS Interoperability framework.

As regards trust services, there are currently 202 active qualified trust service providers[107] operating in 28 of the 31 EU and EEA/EFTA countries. Qualified eSignatures are the service provided most on the market (158), followed by qualified time stamps (114) and qualified eSeals (107). Out of the five core trust services (Qualified certificate for electronic signature, Qualified certificate for electronic seal, Qualified time stamp, Qualified certificate for website authentication, Qualified electronic registered delivery service), the latter service is the most limited one, featuring only 20 active services in seven Member States[108] at present. The eIDAS Regulation has successfully defined the legal effects and provided a well-functioning framework for the provisioning of qualified trust services, electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services and electronic documents across borders.

More than 5 years after the adoption of the eIDAS Regulation, mixed conclusions must be drawn on its success.

For trust services, the eIDAS Regulation has created a European market with common rules for the supervision of Qualified Trust Service Providers and the creation of legal effect of e-signatures, e-seals, etc., across borders. Although there are some weaknesses in the harmonisation of supervisory procedures and in the implementation of Qualified Website Authentication certificates (QWACs), trust service providers confirmed to more than 70% that the Regulation had overall improved trust and confidence in the security, quality and availability of trust services[109].

For eID, a more critical conclusion must be drawn based on a number of factors, partly related to the regulatory shortcomings of the Regulation and its implementation. More importantly, there have been fundamental changes in what users come to expect, in technological developments, and in changes to the market given the sharp increase in number of services online and a shift away from the reliance on digital identify alone to the provision of digital attributes. Moreover, there is also a shift towards more user centric electronic identify solutions and solutions allowing users to control all aspects of their digital identity and protect personal data.

---

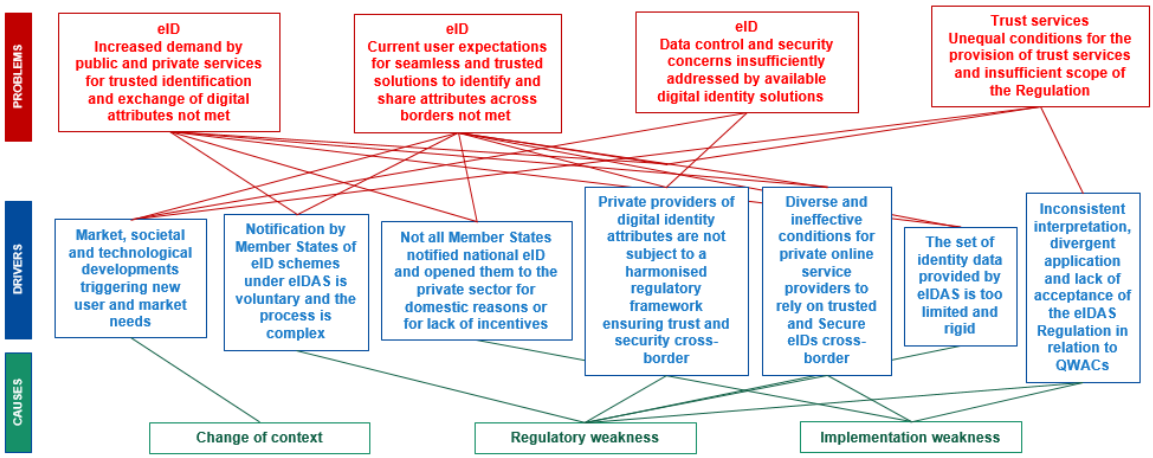
[106] As identified by the eIDAS evaluation, in 2019 about 67% of nodes could receive identification requests from abroad although in principle full coverage should have been reached by September 2018 when mutual recognition applied for the first national eID scheme. In September 2020, only 22 out of 30 countries (27 EU Member States and Iceland, Norway, Liechtenstein) had enabled the receiving function of their eIDAS nodes. Four other eIDAS nodes are still testing their receiving capability, while five eIDAS nodes are not operational. In addition, although 19 eID schemes of 14 Member States had been successfully notified, not all of these 14 Member States had nodes with sending functions fully operational.

[107] State of play in April 2021: https://webgate.ec.europa.eu/tl-browser/#/dashboard

[108] BE, BG, DE, ES, FR, NL, SI,

109 See eIDAS evaluation, chapter 5.

Figure 1 - Problems, drivers and causes



2.4.1.2 *Increased demand by public and private services for trusted identification and exchange of digital attributes not met*

The eIDAS Regulation focuses on access to cross-border public sector services, and has been able to offer this access only for a limited number of them (see below). However, since its adoption in 2014, the demand for secure and trusted identification and exchange of attributes has increased fundamentally both for access to public and private services.

As regards the ***private sector***, market demand for trusted and secure identification has substantially increased in sectors such as finance, transport or health. This is due to the general evolution of digital transformation and the fact that simplification of processes and considerable cost savings are possible thanks to a link of private sector use-cases with secure and trusted eID. This includes for instance facilitating a fully online customer on-boarding process in banking and insurance with a high level of security and data protection.

However, cross-border private sector use cases using government eIDs notified under eIDAS are currently very limited[110]. Even if the Regulation encourages Member States to allow private online service providers to offer the possibility to authenticate using a notified eID, not all notified eIDs are allowed to be used by the private sector even at national level. In 2018, eID schemes of 12 Member States could be used by the private sector at national level[111]. For example, in the Czech Republic,[112] holders of the national eID can use it to access health insurance companies[113], online gaming and betting websites[114], and a law

[110] The usage by the private sector is limited because there is no compulsory acceptance for the private relying parties, as it is the case for the public sector mutual recognition.

[111] In a consultation of EU-28 national experts in June 2018 conducted by the European Commission, at least 12 EU Member States declared that they allow the reuse of at least one eID scheme by domestic private relying parties for national transactions. Nine among them have declared that they will open this possibility to private relying parties established outside their national territory. At the same time, four Member States shared that they are currently not allowing the reuse of their national eID scheme authentication service by private relying parties at the national level and will unlikely allow this possibility to private relying parties established outside their territory.

[112] Identita.cz, Qualified online service providers, see : https://www.eidentita.cz/Home/Ovm

[113] https://www.ozp.cz/ and https://portal.cpzp.cz/

[114] https://www.sazka.cz/

firm[115] on top of eGovernment services. The Danish NemID can be used to authenticate to online banking[116]. In Germany, the list of authorised relying parties is also published and includes banks, notaries, pension insurances and system providers for accountants and attorneys[117].

Overall, the eIDAS evaluation shows that cross-border use of notified eIDs by the private sector is practically inexistent due to questions of liability and the lack of viable commercial models, complexity of connecting to the nodes and limitations of the person dataset (See below in the drivers section).

eIDAS indeed cannot address these new market demands given its inherent limitation to the public sector, the complexity for online private providers to connect to the system, its insufficient availability in all Member States and its lack of flexibility to support a variety of use cases (see section on drivers). Furthermore, identity solutions provided outside eIDAS cannot seamlessly respond to the new market needs. Social media providers cannot offer a direct link to trusted and secure eID, which is essential for legal certainty and to address e.g. liability issues. Their offers are therefore limited to certain private sectors such as e-commerce. While certain private providers, such as Banks, are able to offer digital identification and authentication with higher levels of assurance, their services remain closed to their own customers or, in those cases where they are also offered to external users, such identification means do not benefit from cross-border legal recognition which limits use cases and prevents scaling-up[118].

As regards access to ***public services***, demand has also evolved due to digitisation. An increase in mobility (about 30% of EU population travel yearly to another Member State) and changes in user needs and preferences point to an increase in the demand to access public services online across borders. However, eIDAS focuses mainly in the needs of those EU citizens of working age residing in another EU Member State, which represents in number only around 3% of EU population[119].

Moreover, the core purpose of eIDAS, to enable the cross-border access to those public online services could also not be entirely fulfilled. Even in those Member States which notified a national eID under eIDAS, substantial barriers to access public online services persist. The number of services connected to the national nodes is considerably smaller than the number of services declared as being accessible via the domestic eID scheme. On the basis of available data it seems that only about half of the services accessible through domestic eID are connected to the national eIDAS node[120].

---

[115] https://www.ak-vych.cz

[116] https://www.netbank.nordea.dk/netbank/index.jsp + https://danskebank.dk/privat/find-hjaelp/netbank-letbank-og-apps

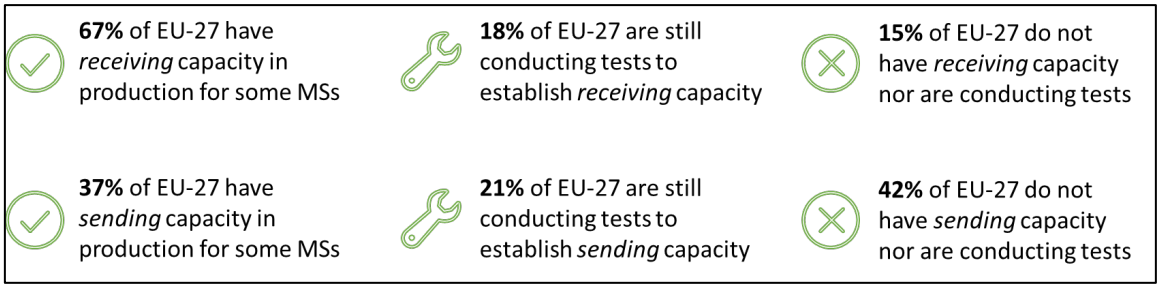
[117] Bundesministerium des Innern, für Bau und Heimat, Granted authorization certificates, see: https://www.personalausweisportal.de/DE/Service/Downloads/Erteilte_Berechtigungszertifikate/Erteilte_Berechtigungszertifikate_node.html

[118] Examples include dedicated digital identity companies, such as Onfido or WebID.

[119] https://ec.europa.eu/eurostat/statistics-explained/index.php/EU_citizens_living_in_another_Member_State_-_statistical_overview

[120] See eIDAS evaluation, page 22

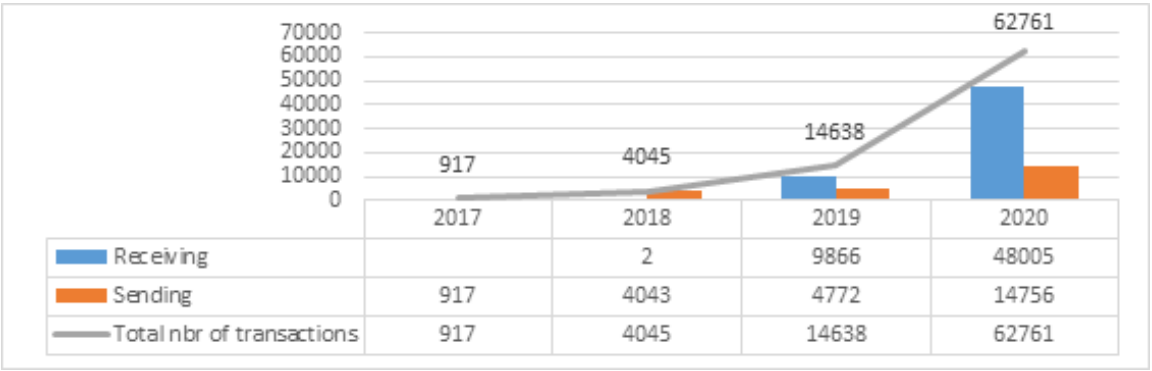
Figure 2 - eIDAS node sending and receiving capacity across EU



Only 14% of providers of seven key public services across all Member States allowed cross-border authentication with a notified eID. The overall number of services connected to the national nodes is considerably smaller than the number of services available for access via the domestic eID schemes. Data provided by Member States on the number of public service providers connected to eIDAS nodes is very different: While Belgium reports for 2018 over 1000 public service providers, Germany reports 95 service providers for 2020.

The number of cross-border authentications and especially the number of receiving transactions provides an estimate on the current usage of notified eID schemes, as it is related to the number of use cases where citizens request access to an online service across borders.

Figure 3. Evolution of the number of yearly cross-border authentications in Austria, Czechia, Estonia, Netherlands, Luxembourg, and Sweden



	2017	2018	2019	2020
Receiving		2	9866	48005
Sending	917	4043	4772	14756
Total nbr of transactions	917	4045	14638	62761

eIDAS cannot fulfil the current demand due to implementation weaknesses in the deployment of the eIDAS interoperability framework, difficulties in identity matching[121], but also due to failure of granting access to a large number of public online services by Member States to users identifying from abroad with an eID notified under eIDAS.

As regards the ***market demand for credentials digitally proving attributes,*** such as medical certificates or professional qualifications, they are currently not covered by eIDAS. Member States and service providers have therefore been forced to develop proprietary trust and interoperability frameworks to ensure the security of these services and/or their recognition across borders. This includes health (ePrescriptions or medical certificates), travel (facilitating travel and border control through information in electronic machine readable documents) and education (Europass Digital Credentials)[122]. A specific EU

[121] Problems related to identity matching can prevent citizens using a notified eID from accessing online public services in cases when the unique identity of the person cannot be established, or when a person cannot be uniquely linked to an existing record in another Member State (see below in the Section on Drivers).

[122] https://ec.europa.eu/futurium/en/europass/europass-digital-credentials-infrastructure

student eCard support structure within the CEF programme has been created to demonstrate in practice the ability for academic and non-academic services to exchange student identity data[123] and the Horizon 2020 project Future Trust has also piloted[124] the possibility to combine academic ID and national ID in order to issue trustworthy certificates for creating an EU Student eCard[125]. A recent example is the ***Digital Green Pass Regulation***[126], which foresees the development of an independent interoperability and trust framework for cross-border travel certificates by mid-2021.

Example 5 – Attributes / Credentials: Digital Identity can provide trust and security to attributes and credentials in various areas. An EU-wide trust framework for attributes and credentials linked to strong identity verification would for example be able to protect sensitive health data and facilitate its exchange across borders upon user consent. In the absence of an existing EU framework for the attestation of digital attributes and credentials linking them to trusted eID, a specific regulatory framework for the swift provision of certificates to prove medical test results ("Digital Green Certificate") has been necessary in March 2021.

2.4.1.3 Current user expectations for seamless and trusted solutions to identify and share attributes across borders not met

Users today expect seamless online journeys, mobile applications and single-sign-on solutions that can be used for online services in the public and private sector, covering all use cases for identification ranging from pseudonymous log-on to an online platform to secure identification for e-health or e-banking. Secure online identification and the exchange of attribute credentials is becoming more important as the number of identity-sensitive and personalised services increases. The ability to identify digitally will become an important factor of social inclusion and the provision of digital identity a strategic asset.

New technological solutions are adopted by the public and private sectors that aim to address the evolving needs of citizens and businesses. ***Self-sovereign identity (SSI) solutions*** offer a user-determined environment that facilitates data protection and control. Digital wallets allow the user to manage and exchange their own identity-related information, attributes and credentials. Some Member States are moving into this direction, which, unless regulated at EU level, will further increase the disparity between national systems.

However, today many citizens do not even have access to trusted and secure ***government eID means*** allowing them to access services across border. Six years after the adoption of eIDAS, the eIDAS framework covers only about half of the EU population[127]**,** leaving 41% of EU citizens without the possibility to use any trusted and secure eID scheme across borders.

Some Member States have involved the ***private sector in the provision of eID means*** and their services are recognised and used for access to online public and private services.

---

[123] CEF Programme 2019, see: https://ec.europa.eu/inea/sites/inea/files/cef_telecom_work_programme_2019.pdf

[124] eID.AS, FutureTrust releases eIDAS-Portal to kick-off "EU Student eCard" and demonstrators for eMandates, eInvoices and eApostilles, see : https://www.eid.as/news/futuretrust-releases-eidas-portal-to-kick-off-eu-student-ecard-and-demonstrators-for-emandates-einvoices-and-eapostilles/

[125] https://ec.europa.eu/digital-single-market/en/eu-student-ecard

[126] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate), COM/2021/130 final

[127] In theory, 59% of the EU population currently has access to a notified eID scheme, see evaluation SWD, p. 25

However, their cross-border recognition relies on a decision by Member States to notify them under eIDAS. So far, only few have recognised private schemes, notably Belgium (ItsMe), Italy (SPID) or Sweden (BankID).

Alternative ***digital identification solutions by private providers*****,** not recognised by governments, do exist. However, as mentioned above they only address some private use cases not requiring high level of security. Other more secure solutions offered by private providers lack common frameworks or standards as regards for example, the levels of assurance that they provide. They can therefore not scale up and be recognised across borders for access to public or private services which require a certain level of trust.

Without access to seamless and trusted identity solutions recognised cross border, citizens and businesses will have to rely on solutions that are not linked to their legal identities issued by Member States and are therefore less secure. This contradicts the increasing user demand for a secure digital identity to access all online services in the EU that gives users control over the use of their personal data and allows for the exchange of personal data attributes and credentials.

2.4.1.4 Data control and security concerns insufficiently addressed by available digital identity solutions

There are security risks involved in providing personal data online or in information systems for authentication purposes. A data breach occurs when a cybercriminal infiltrates a data source and extracts confidential/private information, and many security incidents mainly affect personal data. For example, in April 2021 it was reported that data including phone numbers, Facebook IDs, names, birthdates and in some cases, e-mail addresses from 500 million Facebook users had been leaked online[128].

An average person has more than 90 user accounts (digital identities) online. Having many accounts leads to reusing passwords, which increases the risk of identity theft and the leaking of personal data. In 2019, over 4.1 billion personal data records were exposed due to data breaches. Email addresses were exposed in 70% of reported data breaches and passwords were exposed in 65% of reported data breaches. A recent Eurostat survey showed that 75% of EU citizens use low-level security identity tools provided by the private sector (e.g. password and username or email address) with potential risks to the integrity of personal data or even identity theft. According to a Gigya survey, more than 80% of consumers admit to having quit an online registration form because they were uncomfortable with the amount or type of information requested. A recent Eurobarometer survey shows that 88% of consumers wish for more control over their data[129].

However, neither public nor private offers fully respond to this demand. Existing eID under eIDAS is not sufficiently widely usable for identification in the private sector to represent a viable alternative and has inherent limitations to discretional data disclosure for the user. In addition, identification provided by large online platforms often does not allow for the effective protection of personal data, as evidenced by major data breaches and enforcement actions over the last decade, but is used by service providers given the large market power and customer base of platforms:

Platforms and social media allow users to authenticate to third-party applications using their social network profile. They frequently require that users sign up to/register with the

[128] https://www.businessinsider.fr/us/stolen-data-of-533-million-facebook-users-leaked-online-2021-4

[129] Eurobarometer 503, Attitudes towards the impact of digitalisation on daily lives, December 2019

platform's own service in order to use another of its products (e.g. an operating system, social network, etc.)[130]. Although the GDPR applies, data management, including activity data management, is not transparent in these situations and often the user has no other option than to consent to the disclosure of data in return for using the platform's identification service. As mentioned by the European Data Protection Supervisor:

"[*t*]*he concern of using data from profiles for different purposes through algorithms is that the data loses its original context. Repurposing of data is likely to affect a person's informational self-determination, further reduce the control of data subjects' over their data, thus affecting the trust in digital environments and services"*[131].

While ***eIDAS notified eIDs*** offer a high level of security, it has limitations as regards the principle of data minimisation. For authentication to online public services cross-border, it is compulsory to exchange the full minimum eIDAS data set and there is no possibility for the user to limit the transmitted personal data to the minimum required for a specific transaction. For example, eIDAS does not support so called *"**zero-knowledge claims**"*, which allow a user to certify that he or she is above 18 years of age, without having to disclose her/his date of birth. Currently, even national eIDs offering a high level of security do not allow users to store data securely in the same place and apply full control on data release. Overall, eIDAS today cannot respond to user expectations for full control of personal data, and also private alternatives do not offer this possibility. The general shift towards a more comprehensive identity ecosystem that integrates attributes and credentials, some of them carrying sensitive data such as in the health sector, makes it necessary to develop eID ecosystems that are able to effectively protect personal data and offer full user control.

2.4.1.5 Unequal Conditions for the Provision of Trust Services and insufficient Scope of the Regulation

Although the evaluation of the eIDAS Regulation concludes that the regulatory framework has successfully established legal certainty on liability, burden of proof, legal effect and international aspects of trust services, it also shows that there is room for improvement regarding a harmonised application of ***supervisory procedures*** and ***processes for identity proofing***, in particular when these processes are carried out remotely. Trust service providers (TSPs) must verify, in accordance with national law, the identity of the natural or legal person to whom a qualified certificate is issued. Since identity-proofing methods are defined in different ways at national level, some trust service providers face market-entry barriers. For example, remote identification using video identification is allowed in some Member States and not in others. This creates an uneven playing field benefitting trust services providers established in those Member States where the use of video identification is allowed.

In addition, there are national differences in the way the conformity assessment of qualified trust services providers is carried out, which requirements apply and which standards are used. As the eIDAS Regulation does not regulate these aspects, differences in the application of the rules for national supervision between Member States raise challenges regarding a comparable level of trust and security of the services provided and of a common level playing field. For example, the evaluation shows that less than 50% of the Qualified Trust Service Providers reference specific standards (such as ETSI EN 319401) to prove compliance with the Regulation. Furthermore, only 15 Member States have introduced

[130] DMA Impact assessment - SWD(2020)363 final

[131] EDPS Opinion on online manipulation, Opinion 3/2018, 19 March 2018, p. 15 and EDPB report on social media and impact of profiling on competition, page 7

specific national procedures for the qualification of trust service providers. In other Member States, the lack of procedures creates uncertainty as to the criteria against which the trust service provider has been evaluated to ensure conformity with the Regulation. As regards the different practices in conformity assessment, the lack of a more harmonised approach to auditing with regards to the form and content of the conformity assessment reports has caused, according to ENISA[132], some "incongruences in the qualifications of TSPs in different countries as well as their qualified trust services, undermining trust and confidence".

The problems described for the provision of trust services are also linked to the absence of a common governance structure at EU level similar to that of the Cooperation Network for eIDs allowing Member States to jointly address them. In the evaluation, some supervisory authorities noted that the role of FESA[133] should be formalised to address the need of consistent application of eIDAS chapter on trust services in all Member States. Currently, FESA is an unofficial body and its activities depend on the initiatives of the representatives of the national bodies.

Risks of market barriers have also been identified for ***eArchiving services***. The eIDAS Regulation requires archiving the signatures of electronic documents but does not specify requirements and which standards to use. This has led several Member States to develop competing national rules. As part of the consultation process, a number of Member States and the majority of trust service providers consulted suggested expanding the eIDAS Regulation to a new trust service for eArchiving.

There is also need for improvement concerning the efficiency of a particular trust service, the provision of ***Qualified Website Authentication Certificates (QWACs)***. QWACS have been created by the eIDAS Regulation to enforce EU rules on a 'right to know' regarding the identity of websites[134]. They offer traders and consumers a trusted and secure way of identifying the entity responsible for a specific website in a transparent way. Outside the browser environment, QWACs are used in the EU to secure payment services where full assurance on the identity of the entity behind a website is required by law.

Despite the introduction of these certificates by the eIDAS Regulation, web browsers refuse to include them in their root stores and to display them clearly, which makes these certificates unusable for traders and consumers. Although the Commission initiated a dialogue in 2018 to promote implementation of QWACs in the browser environment, web-browsers continue to refuse supporting QWACs and have been unable to present alternatives with the same degree of legal assurance. Supporting a higher level of security, transparency and trustworthiness as offered by QWACs is not considered necessary by web-browsers and not foreseen by US legislation where most browsers are located. Web browsers are primarily concerned about ensuring the secure and trustworthy link to a

[132]ENISA study of January 15, 2019: Towards global acceptance of eIDAS audits; https://www.enisa.europa.eu/publications/towards-global-acceptance-of-eidas-audits

[133] The Forum of European Supervisory Authorities (FESA) for trust service providers, is a forum open to national bodies responsible for supervision and/or trusted lists in accordance with the eIDAS Regulation. The scope of FESA is to support the cooperation, information and assistance among the members and to facilitate the exchange of views and agreement on good practices: http://www.fesa.eu/

[134] This 'right to know' is established in articles 2 and 3, 12, 101, 102, 114 and 169 of the Treaty on the Functioning of the European Union and article 5 section 1 letter (b), article 6 section 1 letters (b) and (c) and article 8 section 4 of the 2011/83/EU Directive on consumers rights. In order to allow consumers and all other interested parties to know the identity and reliability of a company and have full access to the most relevant information concerning a company, Member States are bound by article 14 of the Directive 2017/1132/EU that codifies certain aspects of company law.

domain and less about ensuring the identity of the entity behind the website with a high level of assurance as provided by QWACs.

Alternative solutions to QWACs, such as TLS certificates applied by web browsers, do not offer the same legal protection as they do not enable the consumer to trace a website back to the identity of the person or to the legal entity behind it. In addition, they do not assure that this person or legal entity is genuine and legitimate, which is important to prevent identity fraud. TSL certificates only inform about interaction with an identified entity. However, they cannot distinguish the identity of the actual owner of the site from the identity of an intermediary.

In particular, for websites run by intermediaries or trading companies[135] only QWACs can guarantee identity of the entity behind a website with a high level of assurance. The lack of recognition of QWACs by web-browsers may also conflict with the protection of fundamental rights of consumers as enshrined in articles 12, 101, 102, 114 and 169 of the Treaty on the Functioning of the European Union and with EU Consumer protection legislation, in particular Directive 2005/29/EC[136].

2.4.2 What are the problem drivers?

The following problem drivers are linked to three dimensions, which intersect and reinforce each-other: regulatory shortcomings, implementation weaknesses and changes in context. These links are indicated as appropriate below.

2.4.2.1 Market, societal and technological developments triggering new user and market needs (change of context)

The context for the eIDAS Regulation in 2021 is fundamentally different to 2014, the year of its adoption. Various developments have created new demands that cannot be answered effectively by the eIDAS Regulation in its current form. The following elements summarise these developments, which are also referenced in other parts of the impact assessment as strong and overarching factors of change:

- With the ubiquity of smartphones, the overall progress in digital transformation and the emergence of new user determined technologies such as self-sovereign identity, users expect to identify online and mobile with a single log-in solution using the same eID for public and private use-cases as confirmed by Eurobarometer data (see above).
- The push for further digitalisation in public administration and the economy accelerated by the ongoing pandemic[137] has created emerging offers for a variety of digital credentials and attributes to affirm personal and professional situations, claims and entitlements in a digital form. Today, these offers cannot relate to an overall technical and legal interoperability framework that inspires trust and security through the link to public eID and a focus on the protection of personal data. For this reason, the public sector pursues the development of various proprietary and insular solutions, for example in ehealth. In the private sector, large online platforms are

[135] Following the definition of article 1 of the 2011/83/EU Directive on consumers rights.

[136] Directive 2005/29/EC concerning unfair business-to-consumer commercial practices, protecting the right of consumers to know the legal entities they are interacting with, their geographical location to the point that providing misleading/inaccurate information or no information at all on the true identity of the business/trader, amounts to misleading or aggressive commercial practice (and fall just short of consumer fraud).

[137] https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever#

preparing personal digital wallets typically connecting identity attributes with payment credentials

These developments of the market, technological and societal change and a shift in user behaviour and expectation described in the second problem (Current user expectations for seamless and trusted solutions to identify and share attributes across borders not met) are factors that reinforce each other and create a strong pull-effect for a personal, seamless, user-determined digital identity platform that allows to share different forms of identity data under full user-control.

Built on trusted and secure national eID, the eIDAS Regulation is in a privileged place to respond to these developments with a user-controlled personal digital tool that allows for the linkage of national eID and private and public credentials in a seamless way.

2.4.2.2 Notification by Member States of eID schemes under eIDAS is voluntary and the process is complex (regulatory weakness)

The ***absence of a regulatory obligation*** for Member States to notify a national eID scheme and submit it to the mutual recognition process is identified in the evaluation as a decisive factor for the problem that not all EU citizens and businesses can have secure identity means to access online services securely in a cross-border context. The introduction of a mandatory requirement, in the Single Digital Gateway Regulation, to use notified eIDs from December 2023[138], seems to have triggered the recent increase in the number of notifications[139].

Moreover, ***the notification process is long, complex*** and suffers from inconsistent interpretation and application of the mutual recognition requirements. Multiple stakeholders consider the peer review processes as cumbersome and inefficient[140]. A key aspect of inconsistent interpretation among Member States concerns the requirements for levels of assurance. To support mutual recognition of national eID schemes under eIDAS, Implementing Regulation 2015/1502 defines three levels of assurance - low, substantial and high – and establishes minimum technology-neutral requirements and procedures to achieve compliance. However, there has been disagreement among Member States how these requirements should be interpreted in practice, and there is no commonly agreed methodology for demonstrating compliance[141]. The lack of references to relevant standards in the implementing act negatively affects the effectiveness and efficiency of the process to achieve mutual recognition and therefore the availability of trusted and secure eID solutions. These weaknesses particularly affect mobile schemes, which benefit from high convenience and user uptake.

Currently it takes on average 9 months from the pre-notification[142] of an eID scheme until its publication in the Official Journal of the EU. In addition, there is a 12-month delay for the

[138] Articles 13 and 14 of Regulation (EU)2018/1724 requires Member States to ensure cross-border access to a number of online procedures by means of eID, eSignatures and eSeals from 12 December 2023 on.

[139] Sweden, France and Malta pre-notified in late 2020/early 2021.

[140] For instance, more than 1 in 4 respondents to a survey of Member States developed for the evaluation of eIDAS disagree with the statements “The mandate, working methods and operation of the Cooperation Network are adequate” and “The Cooperation Network has been effective in completing its mandated tasks”. Position papers review and other survey and interview data collected suggest this is a widely shared view among stakeholders.

[141] eIDAS evaluation study, p. 52

[142] Prenotification is a step preceding the notification where MS submit the draft notification documents to be assessed in the peer-review

application of mutual recognition following such publication. Hence, it takes almost 2 years for citizens and businesses to take advantage of cross-border authentication.

2.4.2.3 Not all Member States notified national eID and opened them to the private sector for domestic reasons or for lack of incentives (implementation weakness)

In March 2021, the intention to notify national eID under eIDAS remained unclear for ten Member States[143]. This diverse group includes countries with eIDs at different stages of development at national level.

The reasons for not notifying existing schemes are diverse and cannot be determined clearly in all cases given the lack of structured information[144] and the fact that notification is voluntary and a political decision by each Member State. It is likely that for some Member States, existing eID schemes are not considered sufficiently technically mature to ensure interoperability with other national schemes within eIDAS[145]. For some other Member States, the system of mutual recognition, which is technologically neutral and based on functional security requirements, leaves a relatively wide margin of interpretation in relation to security levels that can be reached by certain technologies (e.g. mobile eID schemes). In addition to the absence of strict rules and requirements for the peer review process, outcomes are to a certain degree unpredictable which may act as a disincentive for notification. For other Member States, the necessary national regulatory frameworks may be absent or under review[146]. In addition, the low overall number of accessible public online services abroad act as addition disincentive. Ultimately, investments into infrastructure are required to upgrade existing eID, which also raises questions of technological choice considering existing legacy systems and given the absence of accepted standards at European level. As a result, the current system of eIDAS, based on ensuring interoperability through nodes is still not entirely operational, although all Member States are required to accept incoming identification requests from eIDAS.

Even if all Member States would notify swiftly, the existing framework based on mutual recognition of eIDs is not fit for purpose considering the current shift towards the reliance on verified digital attributes and credentials. For the provision of attributes and credentials, a federated system of IT nodes based on technological neutrality and mutual recognition is not practical. It is unlikely that the diversity of use cases and high number of attributes and credentials in different areas can be bound efficiently into the exiting interoperability system, even if this is upgraded. Technical shortcomings associated with such a solution, like response delays or denials of service would act as a strong disincentive to private providers using the system and could not offer the same seamless user-journeys than the standards-based systems the private sector is developing.

One of the limiting factors affecting Member States incentives to notify eID schemes stems from the limited scope of the eID framework, which focused on very limited public sector use cases, mainly those to address the needs of EU citizens residing in another Member States than their country of origin. Although a rapid increase of digitalisation has triggered an increase of demand to access cross border online public and private services where

[143] These Member States included: AT, BG, CY, GR, HR, HU, IR, PL, RO, SI.

[144] One of the identified shortcomings of the regulatory framework, in particular for eID part, is the lack of monitoring and reporting obligations.

[145] This may apply e.g. to e.g. CY, EL, IE.

[146] This may i.e. include AT.

user authentication is needed, the current shift to attributes and credentials which cannot be expressed by the existing eIDAS system may act as a disincentive for notification.

Although Member States can also notify or recognise private identity solutions only few have done so. Entrusting a private provider with operating a national eID is a sensitive political choice and issues of costs and liabilities, competition, interoperability with eGovernment services, trust and reasons of national sovereignty may be engaged. When Member States have functioning eID schemes provided by the private sector (e.g. banks or telecom companies), they might hesitate to notify those schemes since it would imply accepting the liability for the functioning of a scheme they do not control, in the cross-border context. In cases where Member States have no control on the provision of a private sector scheme, they may be reluctant to take such liability without firstly clarifying the liabilities and responsibilities in the national regulatory framework that governs the notified eID provided by the private sector provider.

In addition, eID schemes notified by some Member States do not always cover all levels of assurance with the result that not all online public services abroad will be accessible for users of this Member State[147]. Several Member States have notified only smart-card based eID schemes. These systems are not fully mobile and their take-up at national level is limited.

Notified national eID schemes are not by default open to the private sector and the eIDAS Regulation does not include a requirement for this purpose. Even if the Regulation encourages Member States to allow private online service providers to offer the possibility to authenticate using a notified eID, few notified eIDs are allowed to be used by the private sector on national level and none on cross-border level for questions of costs and liabilities and technical issues of connecting private service providers to eIDAS nodes.

2.4.2.4 Private providers of digital identity attributes are not subject to a harmonised regulatory framework ensuring trust and security cross-border (regulatory weakness)

Currently, eIDAS exclusively regulates government eID solutions or solutions by private eID providers that are notified and guaranteed by a Member State[148]. Other digital identity solutions do not provide official identities of a person and in most cases are not recognised by governments, banks or telcos[149].

Identification attributes issued by the private sector (e.g. banks) are not covered by the eIDAS regulation and operate without legal effects across borders and without legal certainty about liability or transparency over security levels. Services have arisen both in the public and private sector to enable citizens to prove who they are or to prove their attributes/characteristics, without the need to provide physical documents. However, their cross border legal effect and the level of security is not ensured as a legal framework for this purpose is missing.

The identification of objects and devices follows international standards, which are out of scope of eIDAS. However, scenarios where things and IoT devices need to be linked in a

[147] The minimum level of assurance for incoming identification requests is determined at national level. For instance, if the required level of assurance is 'high' an eID notified at level 'substantial' will not be able to access the service.

[148] Article 7(a) of the eIDAS regulation

[149] There are examples where social logins are implemented by governments for certain non-sensitive public services that do not require a legal identification of the user – see: https://toolbox.estonia.ee/

trusted way to owners are increasingly frequent and can be achieved by linking attributes and credentials to secure and trusted eID. The absence of a regulatory framework at EU level for the provision of trusted and secure attributes and credentials also affects the possibilities to link IoT devices to trusted and secure eID of physical or legal persons. The number of connected devices installed globally could more than triple from 23 billion in 2018 to over 75 billion in 2025[150]. Traditional identity solutions focus exclusively on people and are not built for linking people and devices. Consultations with Member States and industry representatives stressed the need for a trusted and secure link between the identification of devices and the identities of physical and legal persons in order to protect against cybersecurity attacks of novel technologies, such as IoT, autonomous driving, 5G or smart devices[151]. For example, there are emerging use cases linking devices to their owners. Electronic certificates linked to a car can be stored on a mobile device and by means of encryption allow the user to open it and drive. The portability of such certificates would also allow him to pass it on for use by others. Relying on international standards establishing the identity of things, once linked to a person using attribute certificates, the digital identify wallet environment will allow the user to securely store multiple keys from numerous providers.

2.4.2.5 Diverse and ineffective conditions for private online service providers cannot rely on trusted and secure eIDs cross-border (regulatory and implementation weakness)

The limited reliance on notified eIDs by private online service providers is mainly due to two reasons[152]. First, each Member State remains free to set the conditions for the use of its national eIDAS infrastructure by private online service providers, leading to diverging national approaches. In addition, there is no guidance at national or EU level on pricing[153] (including revenue-sharing mechanisms), liability and support structure, responsibility for billing and payments and dispute resolution mechanisms[154] related to private sector use of notified eIDs. The impact assessment supporting the original proposal for the eIDAS Regulation already noted that, for example, pricing and liability rules for use by private services are set by the notifying Member State and differ considerably, with the result that only very few private services are connected to the eIDAS network[155].

Second, limited use by the private sector is due to lack of common standards of notified eID means which requires a connection via nodes and cannot offer a swift and seamless user-journey. Even if all notifying Member States potentially opened their eIDAS nodes to the private sector services providers across the Union, the diversity of national conditions for the use of the national eID infrastructures will still make it very difficult for the service providers to build a sustainable business plan or to accurately estimate the potential of this openness to expand their business cross-border. Overall, the lack of harmonised rules

[150] NewGenApps (2018), 13 IoT Statistics Defining the Future of Internet of Things, https://www.newgenapps.com/blog/iot-statistics-internet-of-things-future-research-data

[151] 33% of all respondents to the OPC on eIDAS considers that the revision of eIDAS must include provisions of identification of non-human entities (e.g. AI agents, IoT devices)

[152] eIDAS evaluation report page 23

[153] Currently, relying on a notified eID scheme to access public services is free of charge

[154] GSMA. (2018). Mobile Connect for Cross-Border Digital Services Lessons Learned from the eIDAS Pilot. https://www.gsma.com/identity/wp-content/uploads/2018/02/MC-for-cross-border-digital-services_eIDAS_Feb2018-Final.pdf

[155] Evaluation Study, p. 82

prevents the cross-border and cross-sector use of eIDs by the private sector, limiting the usability of notified eIDs.

"…key factors for the private-sector take up of formal eIDs therefore depend on: a) the availability of open technical systems b) the establishment of clear rules for use of eIDs and for eAuthentication processes c) the establishment of clear liability rules." [156]

2.4.2.6 The set of identity data provided by eIDAS is too limited and rigid (regulatory weakness)

For each identification, eID under eIDAS transmit a minimum data set, which includes first name(s) and family name(s); date of birth and a unique identifier (as persistent as possible in time). This minimum data set is compulsory for cross-border authentication to access online public services. Given the focus of eIDAS for public service identification, there is no possibility for the user to add additional data that is necessary in order to access certain private sector services[157] or to facilitate compliance with specific sectorial regulatory requirements[158]. The number of cases for which notified eIDs can be used are therefore in practice limited.

In contrast, there is also no possibility for the user to limit the transmitted data to the minimum necessary for the authentication to a specific service. Access to certain services requires less data (for example to purchase alcohol one only needs to prove age). The GDPR introduced the concept of 'privacy by design'[159], making explicit reference to data minimization. On top of this, it introduces the obligation of privacy by default, going a step further into stipulating the protection of personal data as a default property of systems and services. The current eIDAS system does not allow the user to actively enforce these provisions in the GDPR and to control which data to share and with whom.

In addition, the rigid data set for notified eIDs makes it also difficult to ***match identity*** records as the current minimum dataset is often not sufficient to uniquely identify a person[160]. Such difficulties typically occur when a person owns different notified eIDs which makes matching the identity to a record difficult using automated means. Problems of identity matching limit the usability of notified eID and is predominantly linked to the cross border use of eIDs since at national level citizens can more easily be identified relying on national identifiers and unique national data sets[161].

Some service providers require a national registry number to grant access to online public services in order to avoid identity matching problems. However, not all Member states issue

---

[156] Ducastel, N. et al. (2012). Study on Impact assessment for legislation on mutual recognition and acceptance of e-Identification and eAuthentication across borders. European Commission. https://ec.europa.eu/digital-single-market/en/news/study-impact-assessment-legislation-mutual-recognition-and-acceptance-e-identification-and-e

[157] For example, the financial sector may need proof of nationality, address or occupation, not currently under the minimum data set provided by notified eIDs

[158] E.g. the Payment Services Directive requires additional attributes such as 'country of tax residency' as part of the Customer Due Diligence processes.

[159] As per Article 25(1) of GDPR

[160] Over 70% of Member States responding to a survey in the context of the eIDAS evaluation confirmed this.

[161] Effective identity matching is a key requirement for interoperability and access to services and a pre-condition for the seamless use of European Digital Identities, the absence of which prevents the opening up of services, extending the eIDAS Regulation to the private sector and the proper application of the Once-Only Principle at EU level (Article 14 of Regulation (EU) 2018/1724)

such a number and include it in the data set. Obtaining it may require physical presence which is an obstacle for users from abroad even in case they are eligible to obtain a national registry number and to access a service.

Several Member States have identified identity matching as a key challenge for the revision of the eIDAS Regulation. Full assurance on record matching / identity matching is a precondition for a seamless cross-border functioning of a European Digital Identity for persons, companies and devices[162]. Without full assurance on identity matching, Member States will be reluctant to open services and agree to an extension of eID / eIDAS to the private sector.

2.4.2.7 Inconsistent Interpretation, divergent application and lack of acceptance of the eIDAS Regulation in relation to QWACs (regulatory and Implementation weakness)

Although the evaluation concluded that eIDAS has been successful in establishing an EU market for trust services, significant barriers remain for trust service providers, which hinder competition.

It is currently left to the discretion of supervisory bodies in each Member State how qualified trust service providers should be supervised. Furthermore, national conformity assessment bodies do not apply common standards in the conformity assessment of the qualified trust services and their providers. Nor is there a common approach on the scope and content of the conformity assessment reports issued as part of the assessment process[163]. According to the evaluation report about 50% of Member States have implemented procedures at national level for the qualification of Trust Service Providers (TSPs) however half of those procedures do not reference applicable standards. For the remaining Member States there is no public information or guidance to the criteria applied to a TSP, the required scope of the conformity assessment, and how and by whom it should be performed, whether there exists a review process by the national supervisory body, nor its content or duration.[164]

Different national rules, non-harmonised applications, differences in fees[165] and certification periods create risks of forum-shopping. Choosing Member States where supervisory authorities and conformity assessment bodies may be more lenient in assessing the functional requirements of the regulation, negatively affects trust and confidence in qualified trust service providers.

---

[162] The issue of identity matching is a strongly contributing factor to the poor performance of eIDAS notified eID in a cross-border context, and limits is usability. The eIDAS evaluation recommends e.g. to introduce a centralized repository for identity matching that would allow service providers perform the required identity matching automatically.

[163] Swedish Post and Telecom Authority's standpoint on eIDAS Regulation. (2020). (unpublished); Luxembourg Position on The Review of the Eidas Regulation. (2020). (unpublished).

[164] Different practices in conformity assessment have been criticised by the majority of Member States and stakeholders consulted on the eIDAS revision. In 2019, ENISA (see https://www.enisa.europa.eu/publications/towards-global-acceptance-of-eidas-audits) highlighted that the lack of a standardised approach to auditing TSPs was major shortcoming of the conformity assessment scheme. While providing that a conformity assessment report (CAR) should be produced and used by the Supervisory Body to determine the qualified status of TSPs, the eIDAS Regulation does not specify the form and depth of the analysis of a CAR. By leaving it to Supervisory Bodies to measure whether a TSP has reached the status of "qualified" or not, this seems to have resulted in “incongruences in the qualification of TSPs in different countries as well as their qualified trust services” with a negative impact on the trust service market and the associated risk of “Undermining trust and confidence in the quality of eIDAS-regulated QTSPs and services in the European Union.” (excerpt from the evaluation report)

[165] Audit costs can vary up to four times from one CAB to the other, for the same solution, depending on the severity of CABs’ approach

A specific problem is connected to diverging national practices relates to remote identity verification. Remote identity verification is the process of validating a person's attributes and verifying if they really are who they say they are without a physical face-to-face interaction. Such verification can instead be made through biometric identification or by verifying identity documents remote via video conference or video assisted automatic identification. Despite a common legal basis in the eIDAS Regulation which defines the circumstances for remote identification, there is a significant lack of harmonisation in applying these requirements across Member States:

Remote identification methods are currently left to the discretion of each Member State supervisory body, without any clear equivalence requirements applying to the physical presence mentioned in Article 24(1)(b)[166]. Consequently, the same remote identification methods can be accepted in some Member States and rejected in others.

The provision and use of website authentication services are entirely voluntary for web site owners. However, when web site owners choose to use QWACS, the browser must display information about its content to the user.

Since the adoption of the eIDAS Regulation in 2014, web-browsers have not accepted the use of these certificates by website owners and do not display their content. The Commission has been engaging in a dialogue with web-browser vendors and ETSI since 2018 to find common ground and look for alternative technical implementations of QWACs fulfilling the eIDAS legal requirements. As web-browsers intend to retain full control over certificates included in their root stores and their technical expression, different (technical) means of expressing QWACs in the browser environment in full compliance with the eIDAS Regulation were suggested by the Commission but rejected by web browsers[167]. Alternative solutions proposed by browser vendors do not fulfil the legal requirements of eIDAS and certain browsers entirely refuse to display certificates by external providers, such as providers of QWACs, using TLS certificates[168]. This also includes legal identity identifiers and identifiers associated with requirements for the financial sector[169].

2.5 Evolution of the problem

The evolution of the problems described should be seen in the light of expected trends on the identity market. Globally, an increase in demand for digital identity solutions is expected, with a predicted annual market growth ranging from 13%[170] to 20%[171]. In addition, it is likely that user expectations with regard to control of personal identity data[172] and effective

[166] FESA. (2020). Position Paper On the review of the eIDAS Regulation FESA's answer to the European Commission's consultation.

[167] Browser vendors are taking further steps to assert control over the browser environment, reducing third party assertions of trust by setting up own root store programs and issuing own certificates as trust service providers.

[168] The TLS protocol is the encryption layer used to bind identity information to the entity behind a website providing a high level of trust. While the eIDAS Regulation does not mandate a particular type of security protocol, experts agree that TLS is the only means by which a high level of trust can be achieved, as set out in the relevant ETSI standards

[169] The Commission has received information that the dominant position of certain web-browsers and their restrictive access policy for external certificates have led to quasi market lock-out situations for specific companies.

[170] The Insight Partners. (2020). Europe Identity Verification Market to 2027

[171] Flood, G. (2019). Global Digital Identity Market to Hit $15BN By 2024. Think.Digital Partners. https://www.thinkdigitalpartners.com/news/2019/05/28/global-digital-identity-market-to-hit-15bn-by-2024/

[172] Eurobarometer 503 (Attitudes towards the impact of digitalisation on daily lives, December 2019): 63% of respondents want a secure single digital ID for all online services that gives them control over the use of their data, 72% of respondents want to know how their data are used when they use social media accounts.

technologies for fraud and identity theft prevention will continue to increase. Continued growth in mobile penetration strengthens the demand for convenient and secure mobile platforms and solutions[173]. Large private providers and online platforms are investing into providing secure identification, in particular for payment services[174]. The combination of convenient technological solutions and market power will in the medium term allow online platforms to offer secure identification for all use-cases, including public online services. This will continue to put political pressure on Member states to avoid the replacing of public eID and fear a de facto privatization of identification of physical persons in the digital world.

In the light of these expected trends, a no change scenario for the eIDAS Regulation may have the following impacts on the problems and drivers:

Not all EU citizens and businesses will have access to seamless user-centric trusted and secure digital identity solutions that can be conveniently used to authenticate to cross-border and cross-sector online services. In the absence of clear rules and incentives for private sector adoption of notified eIDs their usability will remain limited. Only a few national eID solutions that are able to integrate private services and align with user preferences are likely to see continued growth in adoption at national level. Their cross-border use is unlikely to improve in the absence of regulatory change at EU level.

In the absence of a common solution for identity matching, cross-border usability of eIDs will remain limited and this would also pose a risk to the functioning of other EU legislation, such as the Once-Only Principle under the Single Digital Gateway Regulation.

Market fragmentation for private digital identity solutions is likely to grow in the absence of a unitary regulatory framework at EU level. It is likely that a few powerful players (e.g. online platforms), able to capitalise on technology and customer base, will take a large share of the digital identification market while smaller independent providers will see their market share reduced. This is likely to create dependencies for online service providers, user lock-in and a decrease in value creation as well as presenting a challenge to the EU's digital autonomy.

Users will not be able to control the use of their identity data in the absence of clear, uniform data protection and privacy safeguards for identity providers including online platforms. Online payment fraud is anticipated to grow[175].

Stakeholder trust, interoperability of trust services and further unequal market access are likely to suffer from a continuous inconsistent application of the regulation by supervisory authorities. Market fragmentation, growth below potential and limitations to international reach are other possible effects.

A continuing refusal of web-browsers to support QWACs would leave the enforcement of consumer and privacy rights exclusively with supervisory bodies and transparency for citizen could not be ensured. On the contrary, a support of QWACs by web-browsers could

[173] Deloitte. (2018). Trends in electronic identification: An overview - value proposition of eIDAS eID. European Commission. https://ec.europa.eu/cefdigital/wiki/download/attachments/78549570/Trends%20report%20on%20electronic%20identification_for%20publication_v.1.1.pdf?version=1&modificationDate=1551198712785&api=v2

[174] Google Pay, Apple Pay, Lybra

[175] 42.7 MEUR are expected to be spent on fraud detection and prevention software between 2017 and 2022. According to IBM Security and its '2018 Cost of Data Breach Study', the average total cost of a data breach, the average cost for each lost or stolen record (per capita cost), and the average size of data breaches are on the rise and expected to continue growing.

create a competitive advantage for the security and transparency of online transactions in the EU.

On this background, the President and the European Council have called for a secure and trusted digital identity for all that protects data and can be used for public and private online services. This offer can only be attractive to the user if it includes the widest range of use-cases in one application – from highly sensitive eGovernment and ehealth applications to pseudonymous log-on options to online platforms. In addition, the offer must be as user-friendly as current platform solutions offering seamless user-journeys and short response times.

2.6 Justification for EU Action

As indicated in the EC Better Regulation Guidelines, and after having established the existence, scale and causes of the problem, an impact assessment analysis should verify whether Member States could resolve such problem sufficiently and whether the EU has a competence to act and is based placed to do so.

2.6.1 Legal basis – Does the EU have the right to act?

Based on the various legal discussions held with the EC and depending on the policy option chosen and the specific design of the rules concerned, this report considers Articles 114, 16 and 21 TFEU, as possible appropriate legal bases for EU action.

2.6.1.1 Article 114 TFEU

The actions included in PO 1, PO 2 and PO 3 (as described in Chapter 4) result from the ongoing review of the eIDAS Regulation, which is a regulatory obligation included in Article 49 of the Regulation. As the nature of the objective and content is predominantly related to the functioning of the internal market, the proposals also fall within the area of shared competence of the EU in accordance with Article 4 (2) (a) and Article 26 TFEU.

By adopting the measures as presented in PO 1, PO 2 and PO 3, further obstacles to the Single Market for digital services could be overcome as, the proposals further address the proper functioning of the internal market for which the required powers have been conferred to the EU on the basis of Article 114 TFEU. Indeed, the problem definition (see Chapter 2) has shown that the use of trusted, convenient and widely usable digital identities and related trust services for online services is hindered by market inefficiencies, low adoption rates, low confidence, insufficient legal certainty and coherence, and related issues with eIDAS solutions which should now be addressed. It should be noted in that regard that the eIDAS Regulation, including its predecessor Directive 1999/93/EC, were also based on Article 114 TFEU (at the time of the Directive 1999/93/EC, Article 95 of the Treaty establishing the European Community). The policy objectives and instruments proposed by this initiative are aligned with these legislative acts and generally share the same purposes and aims at addressing the same challenges and complexities.

2.6.1.2 Article 16 TFEU

In relation to PO 2 and PO 3 (as described in Chapter 4) in particular, this initiative may also be based on Article 16 TFEU. As this article states that everyone has the right to the protection of personal data and as person identification data is inherently personal data, taking actions to ensure the security and transparency in how identity data is used, falls into the scope of this provision.

Currently, it is observed that due to the unreglated framework regarding electronic identification services in the private sector, EU citizens are increasingly relying on online identity service providers which do not provide users with adequate levels of assurance,

control or transparency in relation to the use of their personal identification data compared to using physical ID cards or passports in the physical world. According to Policy Option 2 measure 2.6, the proposal indeed purports to increase the level of trust when Trust Service Providers and Online Platforms with significant network effect would be using person identification data by adopting further layers of security & privacy measures, notably data separation between (i) data collected for the purpose of user identification and the provisioning of digital identity services and (ii) data generated by the user's subsequent activity on the service provider's website, and increased transparency as to as to the use of user's data for any other purpose other than user identification and the provisioning of digital identity service in an online environment. By addressing critical obstacles in the online digital market, which was inherently built without privacy in mind, as well as promoting the free movement of such data, PO 2 and PO 3 hence address the goals set out in Article 16 TFEU.

2.6.1.3 Article 21 TFEU

Finally, and in addition to Article 114 and 16 TFEU, PO 2 and PO 3 may also be based on Article 21 TFEU. Article 21 TFEU confers on EU citizens the right to move and reside freely within the territory of EU Member States, and provides for the possibility for the EU to act and to adopt provisions with a view to facilitating the right to move and reside freely within the EU if action to attain this objective is necessary to facilitate the exercise of this right. PO 2 and PO 3 should be considered as facilitating the exercise of freedom of movement, as identification in an online environment is a fundamental part of the EU citizenship which was created by the 1992 Maastricht Treaty. Indeed, the introduction of citizenship of the EU "constitutes, for the citizen, the guarantee of belonging to a political community under the rule of law" and such citizenship "raised citizens' expectations as to the rights that they expect to see conferred and protected"[176]. While the objective of Regulation (EU) 2019/1157 was to mitigate the risks of falsification and document fraud in the *physical world*, as well to do away with practical difficulties for citizens related to paper identification when they are addressing their right to free movement, PO 2 and PO 3 aim to resolve fundamentally the same issues in the *online world*. This IA report shows that EU citizens are today unable to effectively rely on trusted and secure sources of identification in an inherently cross-border *online environment* and are required to increasingly rely on online identification services which are not similarly trusted, do not adequately protect personal data and may be subject to crime, falsification and fraud. By addressing these hurdles, this proposal facilitates the exercise of the freedom of movement of EU citizens for which powers have been granted to the EU on the basis of Article 21 TFEU.

2.6.2 Subsidiarity: necessity of EU action

Member States rely on their national regulatory competences to deploy national eID schemes and trust services with the aim to facilitate access to public and private services and trusted online transactions for citizens and businesses. The eIDAS regulation provides the regulatory framework for the mutual recognition of national eIDs and the provision of trust services.

Despite efforts to ensure the proper cross-border functioning of national eIDs and trust services under eIDAS, the evaluation of the regulation concluded that the results for eID fall short of expectations. The number of transactions and the cross-border availability of public services is very limited. Member States have not been successful in integrating online services provided by the private sector into notified eID. This hampers the access to both

176

Resolution on the second report from the Commission on citizenship of the Union (COM (97) 0230 C4-0291/97), *OJ* C 226, 20.7.1998.

public and private cross-border online services for citizens and businesses, and is ineffective in ensuring the proper functioning of the internal market.

Intervention at national level cannot provide the framework needed for a European Digital Identity which is generally available, usable for public and private services across the EU and able to protect personal data and privacy. Ensuring access to cross-border public and private online services in a secure and trusted manner for all EU citizens can only be achieved at European level.

2.6.3 Subsidiarity: added value of EU action

In order to ensure effectiveness and interoperability of the European digital identity, action at EU level would produce greater benefits compared to action taken solely at Member State level. National measures in eID and trust service fields are subject to obvious limitations in the national context and their direct benefits would be largely or exclusively limited to a single Member State (or several Member States in case of data exchange and other forms of bilateral or multilateral cooperation). On the other hand, addressing systemic problems in relation to the free movement facilitated by the extensive use of eID and trust services to access goods and services all over Europe would receive a better response on an EU scale. Relying on national initiatives is likely to entail a lack of focus and fragmented results in tackling the main problems and their drivers.

The Conclusions of the European Council in October 2020 underpin the above and demonstrate Member States' agreement that national action alone would not suffice to reach the set objectives. Thus, the European Council stresses the need for action at European level, complementing the Commission's call for revising eIDAS in its Strategy on Shaping Europe's Digital Future and the commitment to deliver a secure European Digital Identity by the President of the Commission in her State of the Union Speech

Moreover, the eIDAS regulation is setting the standards for trust services globally. To support the international competitiveness of European businesses it is necessary to ensure the regulatory framework for trust services remains relevant and effective.

3 DEFINITION OF OBJECTIVES

The table below suggests a hierarchy of objectives for the review of the eIDAS Regulation. Objectives are set at three levels, which then feed into the policy options:

General objective(s): These are treaty-based goals which the revised framework for trust services and is intended to contribute. The policy ambition would be to foster the achievement of the Digital Single Market, enabling European citizens and companies to digitally access in a secure and trusted way digital services all over the EU and to fully control their identity data. These general objectives thus address:

- the functioning of the internal market as specified in Article 114 of the TFEU, providing a response to the issues that have not been fully addressed by the eIDAS Regulation in its current form. The drivers identified in the problem definition – and particularly persistent market inefficiencies and insufficient legal certainty and coherence - contribute to the perpetuation of barriers in the Digital Single Market, which constitutes a legitimate legal basis for intervention as per Article 114 of the TFEU.
- the political mandate received by the European Commission from the Conclusions of the Council meeting on 9 June and 1-2 October 2020 and expressed in the State of the Union speech of the President of the European Commission on 16 September 2020[177]. Both of these statements place a clear demand on the European Commission to work towards providing accessible and usable EU digital EU.

Specific objectives: these relate to the specific objectives of the policy interventions to be considered in order to meet the general objective. Multiple such objectives can be articulated:

- **Provide access to trusted and secure digital identity solutions for all EU citizens and businesses that can be used cross borders, meeting user expectations and demand.** Achieving this objective,would mean that the expectations user have to access seamless and trusted solutions to identify electronically and share electronic attestations of attributes cross-border can be met. Every EU citizen will have access to secure and user-friendly solutions for electronic identification that are capable of providing access to online public and private services in the EU. Fully achieving this objective will rely, not only on the capacity of Member States to issue eIDs to their citizens and to notify them, but also on new possibilities to be offered by private and public providers of secure and trustworthy identity data and attributes. This would also provide a practical and secure alternative to platform log-on services, while at the same time offering different levels of assurance and trust and the possibility to exchange the necessary data linked to identity for various public and private sector use-cases. The drive for digital transformation instilled by the COVID context, the political commitment of the Member States expressed in the October Council Conclusions and the fact that most Member States are planning to use the Recovery and Resilience funds to reinforce their digital identities, on top of their digital transformation agendas, provides the confidence that time is ripe for a change.

  This objective specifically responds to the following problem drivers “Notification by Member States of eID schemes under eIDAS is voluntary and the process is complex”, “Market, societal and technological developments triggering new user and marked needs”, “Not all Member States have notified national eID and opened them to the private sector for domestic reasons or for lack of incentives”, “Private providers

[177] Please see Section 2.1 for the relevant excerpts from the two documents and related references.

of digital identity attributes are not subject to a harmonised regulatory framework ensuring trust and security cross-border".

- **Ensure that public and private services can rely on trusted and secure digital identity solutions cross border**: responding to market and technological developments and evolving user needs, citizens and businesses would be offered the possibility to use eIDs issued in one Member State together with electronic attestation of attributes and credentials linked to that their eID to access online public and private services across the EU, as well as other services relying on the use highly trustworthy digital identification solutions, for example when renting a bike or presenting a digital certificate required to cross a border. This would apply for to online and offline services that requiringe users to identification identify with a high level of assurance and providing additional and trustworthy proofs in electronic forms (such as residence, place of birth, other identity credentials such as "student", "adulthood" / "seniorhood", etc.). For online service providers, it would mean that access to services no longer will have to be limited to citizens and businesses holding electronic identity solutions issued for specific sectors or a specific Member State. It would solve the problem of lack of uniformity, lack of identity data and interoperability preventing service providers from easily providing services requiring the use of secure and trust worthy digital identity solutions to all EU citizens.

  Fully achieving this objective would require that all citizens and businesses have access to a notified eID that can be used to access services in other Member States and a mechanism to ensure that electronic attestations of attributes can be issued and provided to service providers requiring it. Fully achieving this objective will also require that regulated sectors are obliged to accept notified eIDs and electronic attestations of attributes, and that the convenience of use and the level of trust provided by these solutions will encourage the wider uptake of eIDAS compatible electronic identity solutions by in non-regulated sectors. Fully achieving this objective will also require that appropriate business models are found at the EU level.

  This objective responds to the following drivers "Notification by Member States of eID schemes under eIDAS is voluntary and the process is complex", "Not all Member States have notified national eID and opened them to the private sector for domestic reasons or for lack of incentives", "Private providers of digital identity attributes are not subject to a harmonised regulatory framework ensuring trust and security cross-border", "Market, societal and technological developments triggering new user and market needs".

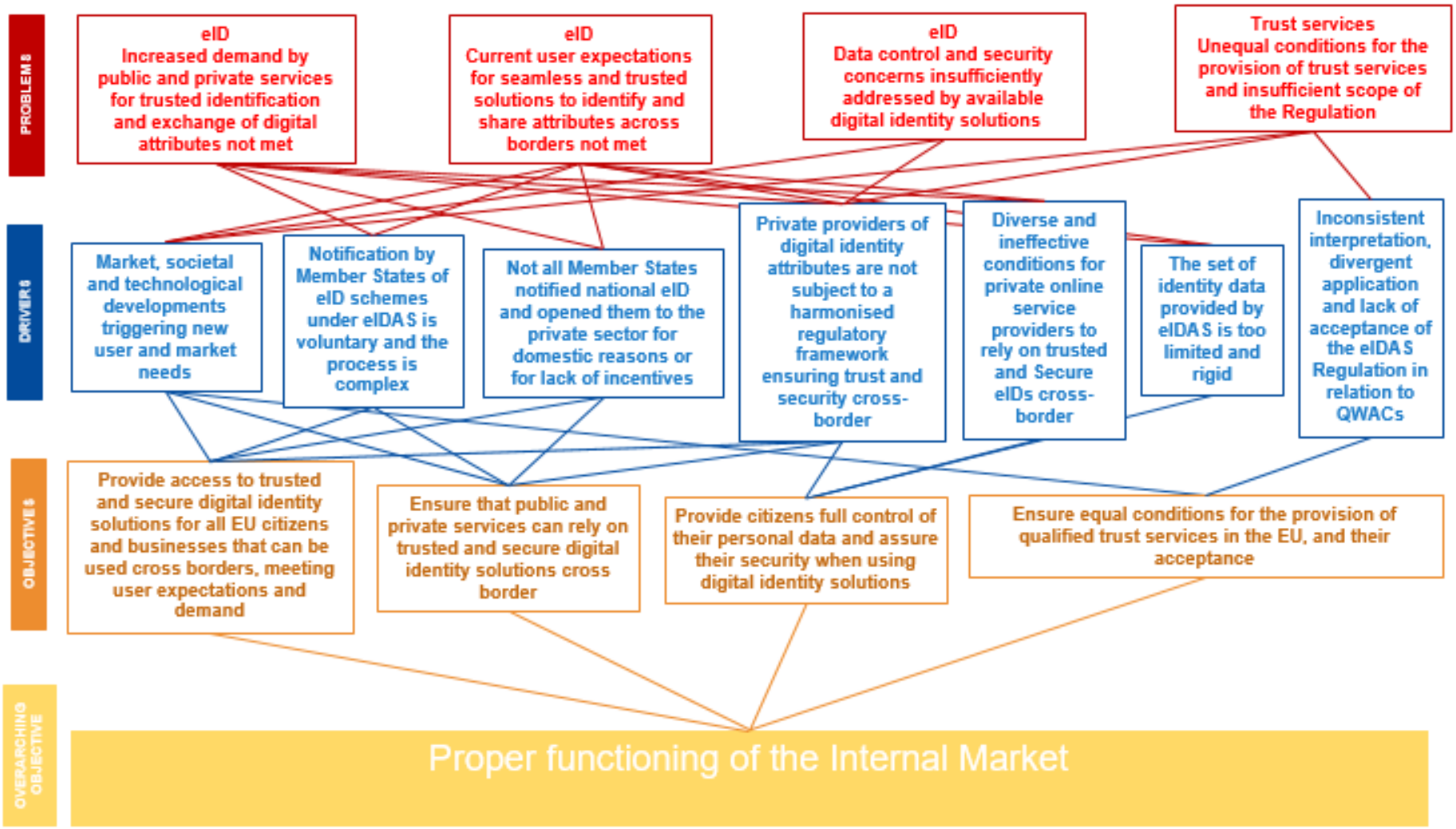
- **Provide citizens full control of their personal data and assure their security when using digital identity solutions**: Achieving this objective would mean that users can manage and control their own identity data when using digital identity solutions. This will be done through trusted and secure government eID schemes and by the availability of a digital identity wallet and by using private qualified trust service providers of identity-related data and attributes. This objective responds to the following problem drivers: "Private providers of digital identity attributes are not subject to a harmonised regulatory framework that ensures their trust and security for cross-border use", "The set of identity data provided by eIDAS is too limited and rigid "and "Diverse and ineffective conditions for private online service providers to rely on trusted and secure eIDs cross-border.

- **Ensure equal conditions for the provision of qualified trust services in the EU and their acceptance**. Achieving this objective would mean that qualified trust service providers will be able to rely on fully harmonised rules across the EU for the provision of services, including the rules on remote identification, based on fully transparent procedures for the accreditation of trust service providers and a fully harmonised supervisory regime. Achieving this objective would also mean that the

scope of the eIDAS Regulations covers all trust services requiring a common European approach, including the provision of qualified electronic archiving services. Achieving this objective would also mean that all qualified trust service can be relied upon by end-users. For example, that visitor to a website can rely upon Qualified Web Authentication Certificates made available in the browser environment, helping to protect against phishing attacks and fraud. This objective responds to the following drivers: “Market, societal and technological developments triggering new user and market needs" and “Inconsistent interpretations, divergent application and the lack of acceptance of the eIDAS Regulation in relation to Qualified Web Authentication Certificates".

Operational objectives: these are defined in terms of the specific policy interventions that could be deployed to ensure the specific objectives are met further outlined in the options for reform box. These are described in more detailed in the next section .

Figure 4. Problems, drivers and objectives



4 POLICY OPTIONS

4.1 Baseline scenario (policy option 0)

Under the baseline scenario, the Commission would not propose any changes to the current legislation, and the eIDAS Regulation and its framework would therefore remain in force without any extension or modification. The baseline would integrate measures envisaged under secondary legislation that could be enforced without any changes brought to the Regulation (implementing acts foreseen in the Regulation but not yet adopted) or implementing acts which were adopted and which could be potentially amended to further optimize the system. Similarly, positive spill-overs stemming from other pieces of legislation (e.g. Digital Markets Act) would be considered under the baseline.

Improvements would be also brought by upgrading most of the soft-law instruments. However, even updating certain existing guidelines without an enabling legislative change in the Regulation might be difficult given the current conflicting positions by Member States on issues such as remote identity proofing and associated levels of assurance.

Generally, under the baseline scenario, it is expected that the weaknesses of the current legal framework, as identified in the context of the eIDAS evaluation will persist and even amplify. The ambition to provide all EU citizens with a trusted and secure identity enabling access to a wide range of public and private cross-border digital services and with control over identity data would not be achieved under the baseline.

Consequently, in the light of the limited scope of the measures available, the baseline would not provide the tools needed to fill the current gaps raised by the increasing demand for cross-border use of data linked to identity (attributes) as enabled under option 2, and the convenience, versatility and the security needed to manage these attributes, as enabled by the European digital wallet, as put forward under option 3.

However, as part of the baseline, certain actions could produce positive effects by amending existing implementing acts for eID with the aim to facilitate Member States' journey through the notification process. For instance, a smoother peer review process and better cooperation mechanisms between Member States could be exploredAs part of the baseline scenario, providers of core platform services that are designated as gatekeepers would be obliged to offer access to and interoperability with the same operating system, hardware or software features under equal conditions for alternative providers of eID solutions, e.g. national eID notified under eIDAS. Designated gatekeepers will additionally be required to allow alternative applications access to their mobile infrastructure. Together, the obligations in the DMA should facilitate the distribution of alternative eID solutions in the digital economy. The implementation of these requirements would rely on the obligation for designated gatekeepers proposed by the Commission under the

Digital Markets Act draft Regulation[178], however not all providers of core platform services would be covered by the obligation.

Standardisation activities also carry the potential to improve the baseline scenario. It should, however, be mentioned that under the principle of technological neutrality enshrined in the eIDAS Regulation, standards would not be compulsory to reach compliance with the requirements of the Regulation. Standards would continue to provide a valuable reference to prove compliance with the provisions of the Regulation, without however excluding other methods to meet the regulatory requirements. The lack of relevant standards has already affected the mutual recognition of eIDs particularly in relation to the levels of assurance of mobile eID schemes, which has led to disagreements in the past. (e.g. the notification of a scheme at level "high" while the Cooperation Network adopted an opinion at level "substantial").

It is therefore expected that the underlying problems linked to the current mutual recognition based system to subsist and even amplify. As reflected by the problem definition, the current deficiencies linked to electronic identification go beyond mere implementation issues. As the implementing acts referenced in the eID part of the Regulation have been already adopted, there is no further margin for improvement via legislative intervention.

Under the baseline, the scope of the legislation would remain limited to notified eID schemes, enabling access to online public services, however leaving the largest part of the digital identity related transactions outside the scope of eIDAS. Indeed, most of the demand for electronic identity and remote authentication stems from the private sector, particularly in areas such as finance, telecom or platform operators that are required by law to verify the identity of their customers.

The following inherent deficiencies of the current ecosystem are expected to subsist and even amplify:

- Member States would continue to notify national eID schemes on a voluntary basis. As the notification process is what ensures mutual recognition of eID schemes across the EU, only the citizens of those Member States that chose to notify a scheme would be able to use eID in a cross-border context, while citizens of Member States that have not notified would still be deprived of this possibility. Even in a scenario where all Member States notify, the systemic shortcomings of a mutual recognition-based system will persist and possibly grow in scale as the interoperability system gains complexity.
- The overall user experience and cross-border authentication through eIDAS under the baseline scenario is expected to remain unattractive for end users, who will continue to face difficulties when trying to access public services in another country. In addition, citizens will continue to face obstacles when trying to use their secure eIDs to access online services provided by the private sector.
- It is also likely that the number of public services connected to the eIDAS network will grow only slowly depending on Member States integrating eGovernment

178 In 2018, a research project on the compliance of reIDAS with the GDPR proposed a modification of the technical specifications of eIDAS in order to enable selective disclosure (e.g. sharing only the necessary attributes for the service) and pseudonymisation (e.g.

services on central platforms or gateways (as deployed, for instance, in Estonia) and addressing other blocking factors such as identity matching. Citizens' access to services will continue to depend on technical and architectural choices made by Member States on their national identity systems.

- The limited data-set of eIDAS would continue to be a barrier to supporting the specific needs of the private sector (e.g. health, banking, etc.) and to solving identity matching problems. As a result the possible use-cases under eIDAS would continue to be limited.
- Access of private sector service providers to trusted and secure eID is likely to remain limited. Even if all notifying Member States open their eIDAS nodes to private sector services cross-border, the diversity of national conditions for the use of eID infrastructures will still make it very difficult for service providers to build a sustainable business case. Private service provider access to notified eID schemes would likely continue to be scattered and remain mostly at domestic level.
- Overall in the light of these difficulties, it is expected that the number of cross-border authentications with trusted and secure eID will remain low, particularly when compared to the usage of eIDs at national level, and it is likely that private solutions will gradually replace public eID once they can offer similar assurance levels.

In general, it is expected that the rapid evolution of technologies will disrupt the current market for digital identity and authentication solutions. Single-Sign-On solutions and digital platforms and wallets able to manage a variety of identity data and credentials that can be easily stored and presented to service providers are likely to proliferate. The global COVID-19 pandemic will undoubtedly accelerate the trend for convenient and secure identification to essential public (eHealth) and private services (e.g. banking).

In relation to trust services, the inconsistent interpretation and application of rules for trust services could be alleviated by the adoption of the implementing acts currently referenced under the Regulation aiming to further harmonise the supervisory procedures in the Member States.

The adoption of implementing acts and referencing standards have the potential to reduce the current fragmentation in relation to the certification of qualified trust service providers and the supervision systems established in Member States. However, remedy measures to address the emergence of new services or the non-recognition of qualified website certificates (QWACs) by web-browsers would not be possible under the baseline scenario since they would require changes to the Regulation. The baseline would also not include an extension to new trust services (e.g. eArchiving).

Policy option 1: Improve the current legal framework for cross-border recognition of national eIDs and trust services

Under this option, a European Digital Identity would be created in the form of a strengthened legislative framework for national eIDs notified under eIDAS. It would require Member States to make eIDs available to all citizens and companies for cross-border use and improve the effectiveness and efficiency of mutual recognition. The use of national eIDs by private online service providers would be triggered and facilitated through harmonised cost and liability rules, extended data sets and access obligations. All these measures would be taken without extending the regulation scope nor affecting its underlying principles (e.g. applicable to eID solutions notified by Member States, mutual recognition and technological neutrality). Option 1 would be supported by the following core elements.

Measures to ensure all EU citizens and business can use trusted and secure eID means to access online public and private services

Measure 1.1: Establish an obligation for Member States to offer eIDs and to notify them under eIDAS, facilitated by a streamlined notification procedure

The measure would establish an obligation in the Regulation for the Member States both to provide their citizens and companies with electronic identification means (e.g. eID cards, mobile apps), and to notify them under national schemes in line with the eIDAS rules. The measure would also set clear timelines for the submission of notifications and for the peer reviews to be carried out on the notified schemes.

In addition, this measure would aim to facilitate the notification of the eID schemes by streamlining the current procedures under the Regulation linked, in particualr, to the time needed from the pre-notification of an eID scheme until its publication in the Official Journal of the EU or to the delay for the application of mutual recognition following such publication. The aim is to render the notification process smoother and shorter for the Member States and to make it faster for citizens and businesses to take advantage of cross-border authentication.

Measures to ensure a wide range of public and private online services is accessible using eID

Measure 1.2: Establish a requirement for Member States to allow private online service providers across the EU to rely on notified eIDs

This measure aims to increase private sector use of notified eIDs by establishing a requirement in the regulation for Member States to allow the use of the eIDAS network and of their notified eID schemes to online service providers179. For this to function in a cross-border context, prior agreement as regards the conditions for access to the eIDAS node will be necessary between the service provider and the identity provider in the concerned Member States.

Example: *A bank in Member State Y would be able to digitally register clients from Member State X via the national eID and the eIDAS node of Member State X. The eIDAS node would be by default open for cross-border use by private relying parties.*

Measure 1.3: Establish a harmonised cost-model and liability rules to facilitate private online service providers to rely on notified eIDs

This measure would provide a **commercial contract model** to be agreed by the Member States and tailored to the identification and authentication needs of the private sector and suitable to accommodate potential business interactions between the eIDAS identity providers and the private online service providers.[180]

179 Currently, Member States have full discretion to decide the approach in relation to the possibility for private service providers to rely on national eIDs. In Netherlands, for instance, Digi D is open only to organisations with a public mission. This might raise difficulties for the Member States to agree on a harmonized approach

180 The commercial model would clarify the nature of the identity–related products and services **("What")**, the different types of stakeholders involved in the ecosystem and their roles **("to whom")** and the way these identity products/services will be delivered, in terms of operating model, cost, pricing and billing strategy **("how")**.

The contract model would establish the costs for the private online service providers for access to the eIDAS network (the price)[181], the contractual conditions (service level agreements) between the requesting private company, and the identity providers in the eIDAS network, and also the security requirements to provide reassurance and trust in cross-border eIDs. The existing eIDAS eID technical specifications would need to be adapted accordingly to accommodate all these dimensions.

The commercial contract model would be complemented by additional **liability rules in the eIDAS Regulation** aiming to provide further clarity and possibly define a liability framework applicable to all parties participating in the ecosystem (e.g. the notifying Member State, the party issuing the electronic identification means, the party operating the authentication procedure) for possible damages due to failure in complying with the eIDAS rules.

Example: *A car rental company in country X would be able to rely on the notified eID of a customer in country Y to conclude a transaction since clear terms and conditions would be in place related to the eIDAS node the company would need to connect.*

Measure 1.4: Extend the person identification data recognised cross border

In order to support a larger ecosystem of use cases, particularly in the private sector, this measure would support the mandatory **design, definition and addition** to the current eIDAS minimum data-set (first name(s) and family name(s); place of birth; current address; gender, etc) of various other attributes and related data-sets suited to access certain sector-specific services. The measure would also facilitate the comparison/matching of various identities of the same person, issued in various contexts or by different Member States (**identity matching)**. The eIDAS technical specifications would be amended to support **additional services relying on these additional attributes**.

Example: *Personal attributes such as the current address (relevant, for instance, for the delivery of certain types of services) or nationality could be used by citizens in their online transactions once Member States agree on this data to become mandatory as part of the minimum data set.[182] An extension of the current minimum data set to data relevant for the provision and exchange of digital vaccination certificates could enable EU-wide secure access to such certificates for health or other purposes.*

Measures to ensure citizens are in control of their personal data and their security is assured

Measure 1.5: Strengthen security requirements for mutual recognition

181 Currently, relying on an eID system to access public services is free of charge. The conditions for private online service providers to access the eIDAS nodes, pricing and billing, are currently established only at national level and Member States' approaches vary (from free access to detailed charging models).

182 The notion of minimum data set is linked to GDPR requirements and obligations. Any additional data will have to be provided only whenever needed and with the explicit consent of the user. This mean that such additional data will have to be made available at the request of the owner of the eID means.

In order to build trust in the cross-border use of notified eID schemes, the notifying Member States need to demonstrate how the notified eID scheme fulfils the interoperability and security requirements provided by the eIDAS Regulation and relevant implementing acts.

One of the targeted actions would be to open the possibility in eIDAS to make use, in the notification processes, of **certification** schemes to be established at EU level – e.g. the future common criteria certification scheme (SOGIS), or a targeted certification for eID schemes under the Cybersecurity Act. The possibility to use certification schemes could be referenced as ways to prove compliance with security and interoperability requirements, such as the capacity of the eID schemes to resist against attackers with *high attack potential as set in* Implementing act 2015/1502.

In the notification process, objective security standards could reduce divergences between Member States, on the security-merits of certain solutions. This could particularly facilitate the deployment of mobile solutions and eID solutions based on remote on-boarding or biometric authentication where security features are often under debate linked to the absence of clear boundaries between levels "Substantial" and "High".

In addition, a **formal process** could be established to **monitor** and ensure that security functionalities and cryptographic algorithms of notified eID schemes are updated on a regular basis to uphold the security of the electronic identification means. This is already in place for trust services (audits, regular revisions of standards, etc).

Example: *certification of eID means at EU level could be used to prove compliance with the security requirements for a mobile eID scheme assessed against level "High" in respect to its capacity to resist against attackers with high attack potential.*

Measures to ensure equal access to the trust services market

Measure 1.6: Introducing new Trust Services

A **new trust service** for e-archiving[183] will be introduced defining requirements and standards for the preservation of electronic documents. This would avoid fragmentation at European level as several Member States have already defined such trust service at national level.

Measure 1.7: Harmonise the certification process for remote electronic signing

The measure would rely on the empowerment in the eIDAS Regulation to amend CID (UE) 2016/650 [184] with the inclusion of the available standards for qualified

183 Electronic archiving aims at ensuring that a document is stored in order to guarantee its integrity (and other legal features). The technology underpinning electronic archiving therefore targets the document. Under the current eIDAS, electronic archiving remains the competence of Member States, to be regulated as a trust service in the future.

[184] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal

electronic signature and seals creation devices allowing a qualified trust service provider to provide solutions that manage electronic signature creation data on behalf of their customers. The possibility to use remote electronic signatures became particularly salient in the COVID context.

Measure 1.8: Strengthening the Recognition of QWACs (Qualified Website Authentication Certificates)

In order to improve the transparency and security of websites, the eIDAS Regulation has created a voluntary possibility to authenticate websites by means of Qualified Website Authentication Certificates (QWACs). QWACs are also identified as one legal means of authenticating websites in the financial sector in the context of the Directive on Payment Services[185] ("PSD/2 Directive").

4.2 Policy option 2: Creating a market for the secure exchange of Data linked to Identity

Under this option, the private sector would support the delivery of a European digital identity ecosystem in the form of a new qualified trust service for the exchange of digital identity attributes, such as proof of age (e.g. for accessing age restricted social media), professional qualifications (e.g. lawyer, student, doctor), digital driving licences, vaccination certificates etc. across borders. The scope of eIDAS would be expanded to cover this new trust service. In this new ecosystem, identity data and attributes would, whenever required, be securely linked to the legal eID of the user, making the data trustworthy and legally enforceable across borders. National eIDs notified under eIDAS would continue to be the sole means to provide legal identity across borders when this is required (e.g. for public services, such as submitting a tax declaration online).

Option 2 extends the possibilities for the secure exchange of identity data, such as personal attributes and professional certificates with legal effect across borders by creating a new trust service linked to national eID. This new service could be used to enable EU-wide authentication to access a variety of online services e.g. in the financial sector, offered today at national level only186 and would also allow for the identification / authentication of IoT devices.

Measure 1 of option 2 supervision to common rules and standards, common liability rules and, last but not least, legal effect and enforceability of certificates and attributes cross-border. All measures under this option are directed at this qualified trust service created and its providers.

In line with the eIDAS rules on trust services, the revised regulation would create **a new qualified trust service** (QTS) for the secure exchange of data linked to identity provided by trusted sources (authentic sources).

It would also cover a **non-qualified trust service** covering the market players active in this area but not fulfilling the requirements set for the secure access to authentic

market. The Commission is currently engaged in an advanced dialogue with the Member States to amend the implementing decision.

[185] Directive (EU) 2015/2366

sources. In contrast to qualified providers of trust services, non-qualified providers would be subject to lighter supervision and only Measure 6: Legal requirements to ensure the protection of personal data) would (partially) apply to them. Other requirements on non-qualified trust service providers include the current technical and organisational measures to manage risks to the security of the services provided, reporting requirements, training requirements for staff, the use of trustworthy systems and products, security assessment schemes for relevant components, validation and authentication etc. Creating a market for secure exchange of data linked to identity in the form of a new qualified trust service under a revised eIDAS Regulation would therefore also bring larger market benefits by introducing minimum requirements for all other market participants ("non-qualified trust service providers") thereby increasing security, transparency and legal assurance for the user (see *"supervisory system"* under measure 1 below).

Option 2 includes the following specific measures:

Measures to ensure all EU citizens and businesses can use trusted and secure eID means to access online public and private services

Measure 2.1: Creating a new Qualified Trust Service for the secure exchange of data linked to identity

Within the framework for trust services created by the eIDAS Regulation, *qualified* trust services and *qualified* trust service providers must satisfy particularly strict criteria regarding security and liability against which they are accredited by national conformity assessment bodies. Qualified trust services are harmonised at EU level and carry legal effect across borders. A digital driving licence or vaccination certificate exchanged in the framework of this measure would therefore be recognised and legally enforceable across the EU.

Based on the current eIDAS framework for the provision of qualified trust services, this service would be subject to common rules, equally applicable in all Member States, in order to ensure security, transparency, auditability and recognition across borders. It would organise the provision and exchange of attributes related to identity, such as name, address and age, medical certificates or a digital driver's licence. These attributes would be asserted by credentials provided by public and private entities who hold the relevant data-sources or have access to them under a legal and technical framework. that ensures seamless exchange and recognition across borders in a secure and trusted way. To ensure the cross-border legal effect of these credentials and their trustworthiness, they would need to be linked to national eID / eID credentials provided by Member States for their citizens and residents, and verified by the provider of the attributes. The service would therefore be only available to citizens in those Member States that have notified national eIDs under eIDAS These credentials linked to national eID could then be used by physical and legal persons to identify or authenticate themselves online or to get an authorisation.

Use Cases: The following typical use cases linked to this new trust service for the secure exchange of data linked to identity can be identified:

- **Exchanging digital credentials:** By sharing a digital credential, a user may demonstrate ownership of a valid driving licence when renting a car, prove

his/her vaccination or confirm a medical degree. A qualified trust service provider with prior user consent will access the data source and provide these credentials to the user thus allowing their exchange.

- **Accessing finical services in another MS**. By proof of identity and delivery of a pre-existing KYC record a person could immediately open a financial relationship. This assumes harmonization of AML and regulatory approval of such processes.

Example: Upon vaccination, a person acquires a digital vaccination certificate which is securely linked to his/her notified national eID and therefore recognised at cross-border level.

- **Asserting specific attributes** (e.g. proof of age, proof of residence, proof of establishment in a country): a user wishes to confirm his/her place of residence or his/her age to access a specific online service, such as downloading age restricted content without having to release any other personal information such as name or birth-date[187]. At the request of the user, a qualified trust service provider provides credentials asserting these attributes based on data from relevant authentic sources, thus allowing the user to confirm personal characteristics in an anonymous trustworthy certified way.

Identity Verification of the User: As for other qualified trust services under eIDAS, qualified trust service providers offering secure exchange of data linked to identity will be obliged to verify the identity and attributes of the natural or legal person to whom the service is provided. In the case of secure exchange of data linked to identity, the qualified trust service provider will be obliged to rely on national eIDs notified by Member States.

Digital credentials shared under the sole control of the user can be used for purposes of identification or authentication / authorisation , including IoT devices. However, whenever the use of legal identities is required by law, for example to identify for an online service of a national tax authority, data linked to identity cannot substitute the legal identities issued by Member States for online identification188.

Supervisory System*:* In accordance with the rules already applicable to other qualified trust services under eIDAS, qualified providers of trust services for the secure exchange of data would benefit from a supervisory regime based on supervision, common rules for accreditation, security and liability underpinned by commonly agreed technical standards.

Measure 2.2: Require Member States to make available data stored in authentic sources for the secure exchange of data linked to identity

Member States would be required under full control of the user or data subject to allow access to the minimum set of identity data stored in authentic sources required

187 Age verification cross border can currently take place only by sharing the whole data set identifying a person: (a) current family name(s); (b) current first name(s); (c) date of birth; (d) a unique identifier.

188 unless the qualified trust service provider providing the data is also a legal identity provider notified by a Member State under the eIDAS Regulation

for the specific service[189]. This requires a technical and legal link between service providers and these national legal identities. Member States would need to allow access to data stored in authentic sources (public registers and databases). This would be a pre-requisite for the provision of services by qualified providers of trust services for the secure exchange of data linked to identity fulfilling the requirements of the Regulation. This would however not imply an obligation to offer qualified service providers online access to national registries but just to the minimum required data. Qualified service providers would only be allowed to query specific data from national registries via standardised Application programming Interfaces (APIs) with prior consent of and mandate from the user.190 Measures to ensure a wide range of public and private online services is accessible with eID

Measure 2.3: Setting security requirements and common technical standards for the secure exchange of data linked to identity

In order to ensure trust, security and a seamless exchange of data necessary for this service, common technical standards will be required. Technical references and / or standards will be needed to access data stored in authentic sources, the provision of verifiable credentials and for hardware and software enabling their secure storage on devices.

The revised regulation would define functional requirements that will be further specified in technical references or standards. To identify these technical references / standards, the Commission would carry out a gap assessment on available industry standards. A cooperation has been established with ETSI to identify existing standards and possible gaps.

In case further specifications or standards will be needed, these would be established in cooperation with Member States and stakeholders and with support from the appropriate standardisation organisation (e.g. ETSI). References to necessary technical requirements and relevant standards would finally be included in a specific implementing act to the revised eIDAS Regulation.

Measure 2.4: Define the legal effect of digital identity credentials

As is currently the case under eIDAS for qualified trust services, the revised regulation would establish the principle that a digital identity credential should not be denied legal effect because it is in an electronic format. Furthermore, requirements would be provided according to which qualified digital identity attributes and credentials should have the equivalent legal effect of the paper-based credentials they replace. This would provide legal certainty at the European level similarly to what is provided for other trust services. For example, under eIDAS, a qualified electronic signature has the same legal effect of a handwritten signature[191].

Measure 2.5: Regulated sectors such as energy or finance and the Public Sector would be required to rely on Qualified digital credentials

189 These legal identities are provided by Member States' accredited providers notified under eIDAS (see option 1).

190 This is similar to set-up of the technical infrastructure supporting the once only exchange of data under Article 14 of the Single Digital Gateway Regulation, see https://ec.europa.eu/growth/single-market/single-digital-gateway_en

191 See eIDAS Article 25 on the legal effects of electronic signatures and article 35 on the legal effects of electronic seals.

To further improve the cross-border use of qualified digital identity attributes and credentials, regulated sectors such as energy, health and finance would be legally required to rely on them providing the same legal value as paper based attestations of identity attributes (in addition to the public sector where this is already the case).

Measures to ensure citizens are in control of their personal data and their security is assured

Identity data is personal data, the processing of which is regulated by the General Data Protection Regulation applying as well to new trust services for the secure exchange of data linked to identity and to the providers of legal national eID.

The existing eIDAS framework for trust services provides relevant assurances. However, to effectively protect personal identity data in a new market where private actors provide authentication services and where identity data will considerably increase in volume, specific requirements are necessary to ensure that market actors implement the rules. For these reasons, we propose to strengthen the existing safeguards under eIDAS following on the proposals made by the Digital Market Act in order to ensure GDPR however without going beyond them.

Measure 2.6: Legal requirements to ensure the protection of personal data

An effective enforcement of data protection rules needs to consider the specificities of the market segment in question and its dominant actors. A key requirement considered for market actors in this context is 'Keep Identity Data Separate from other personal transactional /behavioural data'. The case for this requirement is pertinent to sectors of the digital economy relying entirely on the use of personal data raising concerns of unfair competition and the lack of level playing field.

The Digital Markets Act proposal, which lays down harmonised rules ensuring contestable and fair markets in the digital sector, forbids gatekeepers to combine personal data sourced from services such as user identification with other personal data.192 However, the challenge related to the secondary use of identity data is not limited to the use of large online platforms, although they increasingly act as private regulators setting the rules of the game on the market they control[193].

All Trust Service Providers:

192 Draft DMA regulation, Art 5 (a): "gatekeepers shall refrain from combining personal data sourced from these core platforms with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of Regulation (EU) 2016/679"

193 Yoti Age Scan: in April 2019, Yoti launched a new initiative and potential income stream for the company: Yoti Age Scan technology. This product estimates an individual's age based on their image and is used, for example, within the Yoti app for those who have not uploaded a verified ID document that contains their age; at self-service checkouts to see if an individual is old enough to buy alcohol; to access social media services aimed at teenagers.. Yoti charge businesses to estimate the age of a face. In the case of the use of Yoti outside of the app, a photo of the individual is analysed by Yoti with no other identifying information, and the algorithm decides whether this person is over a certain age threshold. The photo of the individual is deleted and not further stored. Data to train their algorithm is from three sources, including from Yoti users. At the point an individual has a verified ID document on their Yoti account, they are added to the training dataset even though not only the user has no need to use Age Scan within the App. The July 2019 Privacy Policy there was little clarity as to how the users' data was used as part of the Age Scan dataset. There was no accessible way for Yoti users to opt out of use of their data in the training dataset and no accessible way for Yoti App users to request that their data is deleted from the training set without stopping them being able to use the app altogether.

In order to ensure the protection of personal data, the revised eIDAS Regulation will consider imposing the following requirements to *all qualified and non-qualified* providers of trust services for the secure exchange of data linked to identity. These requirements would be set out in the revised eIDAS Regulation and specified as necessary in technical references and standards against which providers are accredited and audited by national supervisory authorities:

- Keep identity data functionally separate from other personal data;
- Observe transparency obligations as to the use of data;
- Offer easy to use opt-in option for every use of identity data for other purposes.

Qualified Trust Service Providers:

For *qualified* trust service providers for the exchange of data linked to identity additional measures should apply given the sensitivity of their access to trusted sources from public and private sectors. The following additional principles should apply for qualified providers of such services:

- Keep identity services structurally separate from other services;
- Apply the principle of privacy by design.

Structural separation would give users (people and businesses) sufficient assurance that their data is safe under all circumstances. It would create the necessary trust to ensure uptake and usage of the system by people and businesses. For corporate users, full data security is a commercial and competitive requirement and needs to be ensured particularly for data generated by IoT devices.

Privacy by design would allow users to limit the provision of digital identity attributes to what is required to receive a service in line with the general requirements of the Data Protection Regulation. This would mean that providers would need to allow for the selective disclosure of attributes and credentials. It would also mean that services providers relying on the acceptance of digital authentication services would be required to use Application Programming Interfaces (APIs) enabling the selective use of attributes.

All measures to qualified and non-qualified trust service providers would be set out in line with the rights conferred to citizens by the GDPR, which also provide individuals the right to withdraw consent for the processing of their data.

Measures from Policy Option 1

Creating a market for the secure exchange of data linked to identity would be supported by the following measures put forward under option 1:

- Establish an obligation for MS to offer eIDs and to notify them under the eIDAS **(measure 1)** – since the identity data and attributes would be securely linked to the legal eID of the user, notified eIDs are essential to make the data trustworthy and legally enforceable across borders.
- Extend the person identification data set recognised cross border (measure 4) – this would support the versatility of the eIDs to cover extensive use-cases in the private sector and implicitly the issuance of more trustworthy attributes under this option.

- Strengthen security requirements for mutual recognition (measure 5).

Measures to ensure equal access to the trust services market

In relation to **trust services**, option 2 relies on a similar set of measures as provided by under Option 1.

4.3 Policy option 3: Personal digital identity wallet (EUeID)

This option aims to ensure that a European Digital Identity personal Wallet App would be made available, on a voluntary basis, to all residents and companies in Europe.

The wallet would empower users to securely share data related to their identity to public and private online service providers through their mobile device and allow them to control their own personal data in a user-centric way. Further to legal requirements, common standards and/or technical references for the Wallet App would be developed in close dialogue with Member States and private sector stakeholders.

The Wallet App would allow the user to integrate a national eID (notified under option 1) and various credentials obtained from private and public providers (issued in accordance with the framework under option 2) and link them to specific identification and authentication services.

Hence, the measures establishing the European digital wallet ecosystem need to rely both on measures put forward under option 1 aiming to strengthen the framework for notified eIDs, indispensable for the trustworthiness of its cross-border use and on measures under Option 2 allowing the establishment of a trust service for attestation of attributes enabling a multitude of use cases, particularly in the private sector.

To guarantee a high level of trustworthiness, and therefore to ensure that the user can receive and exchange qualified attributes and credentials related to their identity, the provider of the European Digital Identity Wallet App would need to ensure that the Wallet App can be linked to a national eID or eID credentials.

Two sub-options are considered for the deployment of the wallet: (1) deployment by private qualified trust service providers under eIDAS and (2) deployment by governments, under their mandate or recognised by them, independently or as an extension to notified eID solutions. Policy option 3 sets-up an ambitious framework that would enhance the exercise by the European citizens of their citizenship rights (Article 20 TFEU) under common rules across the EU.

Measures to provide access to trusted and secure digital identities for all citizens and businesses cross borders

Measure 1 (sub-option 1): creating a new qualified trust service for the provision of a user-controlled secure European Digital Identity Wallet App

This measure only applies if sub-option 1 (deployment of the wallet by private trust service providers) is retained.

The current set of trust services under eIDAS would be complemented with a new qualified trust service for the provision of a user-controlled secure European Digital Identity Wallet

App. Accompanying provisions in the revised Regulation would establish implementation powers for the Commission to adopt implementing acts detailing the overarching standards needed to ensure interoperability and the functionality of the system.

The Regulation would set the conditions for private providers to develop, distribute, manage and maintain the European Digital Identity Wallet App. The requirements applicable to the Wallet would aim to ensure that it meets high security and privacy requirements (see below, measure 2).

Specific data protection measures (see Option 2, Measure 6) would apply also to qualified trust service providers from the private sector providing the European Digital Identity Wallet, notably the obligation to keep these qualified trust services structurally separate from other services provided .

Some provisions might need to be introduced as regards the costs. Thus, it could be foreseen that qualified trust Wallet service providers should cover the costs of development, distribution and maintenance of the wallet (with available support by European funds under the DIGITAL EUROPE programme). While it would be in principle up to the Wallet provider and other relevant actors to define their business model, it could be foreseen that the wallet is free of charge for the user while costs incurred by Member States providing access to national eID and costs by wallet providers could be covered by the fees obtained by the wallet provider from online service providers relying on the wallet/credentials. Other business models could be possible (see below Chapter 6) .

The general requirements for the conformity assessment/certification and supervision of qualified trust service providers laid down in the eIDAS Regulation would apply, including on liability, technical and organisational measures to manage risks, the security of the services provided, reporting requirements , training requirements for staff, the use of trustworthy systems and products, security assessment schemes for relevant components, validation and authentication, etc.

Measure 1 (sub-option 2): Mandatory extension of notified eID schemes, or mandatory provision of a user-controlled secure European Digital Identity WalletApp by Member States

This measure only applies if sub-option 2 (deployment of the wallet by Member States) is retained.

The eIDAS Regulation would be amended to add the provision of the European Digital Identity Wallet App by Member States. The wallet would be subject to the eIDAS rules on notification and mutual recognition of eID schemes. Expedited procedures could be established to facilitate mutual recognition between Member States wallets. Wallets could be notified either as extensions of their current notified eID schemes or as self-standing solutions. As for the provision of national eID, Member States could notify solutions provided by the private sector.

Some provisions would be introduced as regards the bearing of costs. They could foresee that Member States cover costs of development, distribution and maintenance of the wallet directly (European funds, would be available). The wallet could be free of charge for the user while costs incurred by Member States providing access to national eID could be covered by fees applicable to transactions managed by the wallet. Other business models could be possible (see below Chapter 6). Liability would be regulated along art. 11 of the eIDAS Regulation whereby Member States are liable for their eID schemes.

Measures from Policy Options 1 & 2

The establishment of the wallet ecosystem (irrespective if sub-option 1 or 2 is retained) would be supported by the following measures put forward under option 1 & 2:

- to establish an obligation for Member States to offer eIDs and to notify them under eIDAS **(option 1, measure 1)**. The link between the wallet and the notified eIDs will support the trustworthiness and the security of the wallet, particularly in the context of cross-border transactions.
- to simplify and improve the notification and peer review procedures **(option 1, measure 2)**. As the wallet will be part of the mutual recognition ecosystem, streamlining the notification and the peer-review procedures will facilitate the notification of the national eID schemes relying on a wallet.
- extend the person identification data set recognised cross border **(option 1, measure 5).** An extended minimum data-set will enhance the capacity of the user to rely on the wallet and engage in as many and diverse online transactions as possible.
- to create a new qualified trust service for the secure exchange of data linked to identity **(option 2, measure 1).** The attributes issued by the qualified trust services for the purposes of the wallet will offer flexibility to the users to accommodate specific use-cases not covered, for instance, by the minimum data-set.
- Measure 2.2: Require Member States to grant access to authentic data to qualified providers of the new trust service for the secure exchange of data linked to identity **(option 2, measure 2)**. This measure is needed to enable qualified trust services to issue attributes at a high level of assurance to be asserted via the wallet.
- setting security requirements and common technical standards for the secure exchange of data linked to identity **(option 2, measure 3).** In order to ensure trust, security and a seamless exchange of data necessary in the provision of the attributes to be asserted via the wallet, common technical standards need to be established.
- Measure 2.4: Define the legal effect of digital identity credentials **(option 2, measure 4)**. This measure is needed to empower users by guaranteeing the legal effect of their credentials asserted via the wallet at European level.
- Measure 2.5: Regulated sectors such as energy, health and finance would be required to rely on digital credentials provided by qualified trust service providers **(option 2, measure 5).** This measure is needed to facilitate the cross-border use of qualified digital identity attributes and credentials in relation to the transactions where the identity of the users needs to be ascertained with a high level of certainty.

Measures to make accessible a wide range of public and private online services relying on trusted and secure digital identity solutions cross border

Measure 2 (all sub-options): Defining common standards for a European Digital Identity Wallet app

The European Digital Identity Wallet App will offer a unique personal and mobile platform to exchange credentials and attributes under full control of the user. In order to guarantee interoperability with credential issuers and service providers and meet strict security and privacy levels, performance requirements and related technical standards would be defined. To ensure availability for all citizens, a desktop version of the Wallet App will also be developed.

Four dimensions are linked to the core performance requirements of the European Digital Identity Wallet App and define its business case:

- unique personal and mobile platform to exchange credentials and attributes under full control of the user;
- mobility and accessibility (the mobile character of the European Digital Wallet supports convenience but a desktop solution would be provided to ensure accessibility)
- coverage of all levels of assurance (scope ranging from simple log-on solutions to identification for eHealth applications etc.)
- personal data protection and privacy by design (the wallet will enable convenient discretional disclosure of data and guarantee by its design that personal data is private and cannot be seen by service providers, credential providers of wallet providers unless the user consents. This supports the implementation of the GDPR requirements and helps providers manage data security risks)

To define these four dimensions, the following functional requirements would be included in the technical reference framework :

- Security Requirements: Security requirements would ensure the App is protected against attackers with high attack potential, duplication and tampering by means of storing cryptographic keys in a secure hardware element inside the device. Not all issuers of certificates might require such high level of protection and it is possible the certificates can be stored on the hard drive of a mobile phone after having been encrypted to ensure confidentiality;
- Interfaces: Interfaces towards credential issuers and service providers would be defined as well as requirements for the interface toward the user (look/feel and universal accessibility);
- Functionalities: Requirements on basic functionality of the app would be similar to those of eID means or signature creation devices and existing wallets on the market. The purpose of the functionality is to support use cases such as:
    a) users are able to request identity credentials to the wallet from credential providers as described in policy options 1 and 2,
    b) notified eID providers or other digital identity providers (such as qualified trust service providers as described in Option 2) can issue credentials to the wallet,
    c) the holder of the wallet can see an overview of credentials in the wallet as well as latest transactions,
    d) the holder of the wallet is able to delete a credential or the wallet,
    e) the holder of the wallet is able to present identity credentials to service providers for the purposes of authentication and digital signatures etc.
    f) the wallet can be used for login purposes (i.e. subsequent connections after initial authentication, without the need to provide identity credentials again)
    g) the holder of the wallet can create self-credentials

Depending on the type of Secure Element used and support from service providers, the Wallet App should support presenting credentials online. Depending on the type of

credential, the user may also be able to visually (e.g. displayed on the mobile device screen, including e.g. a QR- or barcode) present the credential from the screen of the mobile phone, including a QR code or similar to retrieve a more complete record for online validation of the correctness of the visually presented data elements.

Measures to provide citizens full control of their personal data and assure their security when using digital identity solutions

Measure 3 (all sub-options): Security requirements

In order to build trust in the cross-border use of European Digital Wallet App, the provider will need to demonstrate how the wallet fulfils the interoperability and security requirements provided by the eIDAS Regulation and relevant implementing acts.

As a security measure, the European Digital Wallet App may be certified in a targeted certification scheme developed under the Cybersecurity Act . Certification would prove compliance with the applicable security and interoperability requirements and performance standards.

Measures from Policy Options 1 & 2

The measures linked to data protection and security of the wallet ecosystem would be supported by the following measures under option 1 & 2:

- Measure 1.5: Strengthen security requirements for mutual recognition. This measure is needed to ensure that components essential for the security of the wallet are certified at the highest level of assurance in line with the state-of-the-art standards for cybersecurity (e.g. against cybersecurity schemes set-up under the Cybersecurity Act).
- Measure 2.6: Legal requirements to ensure the protection of personal data. As the wallet should be designed from a user-centric and privacy-enhancing perspective, it is of utmost importance that the qualified and non-qualified trust services issuing the attributes to be asserted via the wallet follow strict requirements liked to the protection of personal data.

Measures to ensure equal access to the trust services market

In relation to **trust services**, option 3 relies on a similar set of measures as provided by under Options 1 & 2.

Options Discarded at an Early Stage

As part of Option 3, the following measure has been discarded given that the Commission does not have the necessary technical capacity to deliver and for reasons of liability.

Measure 1 (sub-option 3): Development, distribution, management and maintenance by the European Commission or as mandated by it

In this sub-option the wallet would be developed, distributed and maintained according to common European standards by the European Commission, an existing European agency or by private provider(s) mandated by the European Commission.

The Commission would decide in an implementing act on the governance framework for an own deployment of the wallet or agree terms of reference with Member States to mandate a (consortium of) private companies for a limited duration of time.

Liability would be regulated along Art. 11 of the eIDAS Regulation whereby Member States under certain conditions are liable for their eID schemes whereas the Commission would

remain liable for the functioning of the wallet. Commercial liability would apply in case a private operator would be mandated by the Commission to manage the wallet.

Table 1. Overview of policy options

Policy objectives	**POLICY OPTIONS**			
	PO 0 (baseline)	**PO1** (legislative) **Improve the current legal framework for cross-border recognition of national eIDs and trust services**	**PO2** (legislative) **Creating a market for the secure exchange of Data linked to Identity**	**PO3** (legislative) PREFERRED OPTION **Personal digital identity wallet (EUeID)**
O1: Provide access to trusted and secure digital identity solutions for all EU citizens and businesses that can be used cross borders, meeting user expectations and demand	No change in scope of eIDAS (eID + current set of trust services), requirements (mutual recognition, supervision) and obligations (voluntary notification)	**M1:1** Establish an obligation for MS to offer eIDs and to notify them under the eIDAS, facilitated by a streamlined notification procedure.	**M1:1** Establish an obligation for MS to offer eIDs and to notify them under the eIDAS, facilitated by a streamlined notification procedure. **M2:1** Create a new Qualified Trust service for the secure exchange of data linked to identity. **M2:2** Require MS to make available data stored in authentic sources for the secure exchange of data linked to identity.	**M1:1** Establish an obligation for MS to offer eIDs and to notify them under the eIDAS, facilitated by a streamlined notification procedure. **M2:1** Creating a new Qualified Trust service for secure exchange of data linked to identity. **M2:2** Require MS to make available data stored in authentic sources for the secure exchange of data linked to identity. **M3:1 (SUB-OPTION 1)**: Creating a new qualified trust service for the provision of a user-controlled secure European Digital Identity WalletApp. **M3:1 (SUB-OPTION 2):** Mandatory Extension of notified eID schemes or mandatory provision of a user-controlled secure European Digital Identity WalletApp by MS.
O2: Ensure that public and private services can rely on trusted and secure digital	Under the DMA, gatekeepers will be required, under certain circumstances, to offer access and	**M1:2** Establish a requirement for Member States to allow private online service providers across the EU to rely on notified eIDs	**M1:2** Establish a requirement for Member States to allow private online service providers across the EU to rely on notified eIDs	**M1:4** Extend the person identification data set recognised cross border

identity solutions cross border	interoperability with notified eIDs	**M1:3** Establish a harmonised cost-model and liability rules to facilitate private online service providers to rely on notified eIDs **M1:4** Extend the person identification data set recognised cross border	**M1:3** Establish a harmonised cost-model and liability rules to facilitate private online service providers to rely on notified eIDs **M1:4** Extend the person identification data set recognised cross border **M2:3** Setting security requirements and common technical standards for the secure exchange of data linked to identity. **M2:4** Define the legal effect of digital identity credentials **M2:5** Regulated sectors such as energy or finance and the Public Sector would be required to rely on Qualified digital credentials	**M2:3** Setting security requirements and common technical standards for the secure exchange of data linked to identity. **M2:4** Define the legal effect of digital identity credentials **M2:5** Regulated sectors such as energy or finance and the Public Sector would be required to rely on Qualified digital credentials **M3:2** Defining common standards for a European Digital Identity Wallet App **M3:3** Security requirements
O3: Provide citizens full control of their personal data and assure their security when using digital identity solutions	Require MS to limit identification data transmission to only the data necessary for a particular transaction.	**M1:5** Strengthen security requirements for mutual recognition	**M1:5** Strengthen security requirements for mutual recognition **M2:6** Legal requirements to ensure the protection of personal data	**M1:5** Strengthen security requirements for mutual recognition **M2:6** Legal requirements on trust service providers of data linked to identity to ensure the protection of personal data
O4: Ensure equal conditions for the provision of qualified trust services in the EU, and their acceptance	Harmonise Supervisory Procedures for Trust Services	**M1:6** Introducing a new trust service for eArchiving **M1:7** Harmonise the certification process for remote electronic signing **M1:8** Strengthening the recognition of Qualified Website Authentication Certificates (QWACS)	**M1:6** Introducing a new trust service for eArchiving **M1:7** Harmonise the certification process for remote electronic signing **M1:8** Strengthening the recognition of Qualified Website Authentication Certificates (QWACS)	**M1:6** Introducing a new trust service for eArchiving **M1:7** Harmonise the certification process for remote electronic signing **M1:8** Strengthening the recognition of Qualified Website Authentication Certificates (QWACS)

5 COST - BENEFIT ANALYSIS OF THE POLICY OPTIONS

This chapter presents the analysis of the cost and benefits identified for each policy option. Estimates included in this section should be regarded as indicative.

5.1 Option 0 – Baseline scenario

Policy option 0 represents the baseline scenario, in which the Commission would not propose any changes to the current legislation. The eIDAS Regulation and its framework would therefore remain in force. In this legislative context, three measures can be brought forward.

5.1.1 Measure 0.1: Require gatekeepers to offer access and interoperability with notified eIDs

5.1.1.1 Citizens and users

Benefits

This measure would enable citizens and companies to benefit from the possible use of trusted eIDs, whenever an identification or authentication step is needed to access gatekeeper platform services. The measure would positively impact on their security online, since the notified eIDs would provide the safety safeguards which cannot be currently offered by the platforms' authentication solutions (e.g. social login solutions). By regularly using their eIDs, citizens and companies (in particular SMEs) will be educated to understand the importance of security online as well as to demand for strong authentication for online value transactions.

5.1.2 Measure 0.2: Require Member States to limit identification data transmission to only the data necessary for a particular transaction

5.1.2.1 Public authorities

Costs

Technical adaptations are likely to create some limited costs.

5.1.2.2 Citizens and (end) users

Benefits

Once adapted, the future Interoperability Framework and the eIDAS technical specifications, would positively impact on the citizens' and companies' opportunities to share only the identity attributes required for the transaction at stake. Similarly, the private relying parties would not be able to request more data than needed for that specific transaction. The measures should also impact by empowering users to send anonymous credentials, without disclosing the identity of the person (I am over 18 years old) and pseudonymisation, thus avoiding profiling opportunities by the eID providers.

This measure will also have a positively impact on citizens and companies trust in public authorities. However, in the exchange of these attributes, citizens will need to rely on the Member States, as opposed to an approach where these attributes could be used in a self-

sovereign way. This measure will also contribute to make users - in particular citizens and SMEs - understand what it means to be Europeans and the values the EU promote.

Practicing data minimization can deliver a host of benefits as[194]:

- **Reduced exposure to data theft**: the average data breach involves more than 25,000 records, and the cost per breached record in the United States is about $242 — in the healthcare industry, the cost runs as high as $429 per record. Several major fines have been proposed under GDPR for data breaches (including fines of $99 million against Marriott and $230 million against British Airways). In this context, data minimisation practices limit the number of records that could be compromised.
- **Efficient data management**: the sum of the world's data is growing at a rate of 61 percent year-over-year. When systems manage less data, it's easier to make them available to organizations who need it, when they need it.
- **Prompt responses to data subject requests (DSRs):** GDPR grants individuals specific rights to request access to and deletion of their personal data (among other rights), and businesses are obliged to respond within a reasonable time frame (one month under GDPR). By limiting the data gathered on individuals starting with the first point of contact, organisations will have less information to track down when those requests do come in.
- **Improved trust**: when citizen and users know that organizations only gather as much personal data as is necessary to conduct business — and take concrete steps to ensure the data is handled responsibly — they are more likely to place their trust in it

5.1.3 Measure 0.3: Simplify and improve the notification and peer review procedures

5.1.3.1 Public authorities

Costs

The costs of streamlining the notification process are expected to be immaterial and **mainly borne by the EU Commission**, since this would mainly require amending the relevant implementing acts (e.g. Commission Implementing Decision (EU) 2015/296), updating guidance documents and facilitating dialogue within the Cooperation Network on the proposed reforms.

Benefits

This measure would address a key challenge highlighted by stakeholders consulted for the evaluation study of eIDAS, which relates to the disproportionate burden imposed by the peer review process on the Member States and a lack of clarity of the Cooperation Network's mandate.

Cooperation network feedback on the peer review process
In a consultation conducted in early January 2019 for *Evaluation study of eIDAS*[195]:

[194] https://www.logic2020.com/insight/data-minimization-always-good-idea#:~:text=Benefit%20%231%3A%20Reduced%20exposure%20to%20data%20theft&text=And%20should%20a%20breach%20occur,records%20that%20could%20be%20compromised.

[195] Deloitte, VVA, Spark Legal Network, Ecorys. (2020). Study to support the evaluation of eIDAS - Final Report. Unpublished.

- 39% of responding members of the Cooperation Network answered that the circumstances, formats and procedures for the pre-notification of eID schemes are not adequate.

- Member States criticise the tendency for some peer reviews to go beyond scope with regard to the level of security scrutiny, rather than focus on an overall assessment of the eID schemes with the requirements of the eIDAS Regulation and correct assessment of the Member State declared LoA of its pre-notified eID solution. On the contrary, the interoperability aspects (e.g. availability of the node) were overlooked.

Following a meeting of the Cooperation Network on June 2019, a specific subgroup was created to discuss the lessons learned of the concluded peer review and propose some improvements. The group identified key issues and gathered the opinion of the Member States on four topics: scope of the peer review, preparation of the peer review, execution of the peer review, and drafting of the peer review.

The measure is expected to generate monetary and non-monetary benefits for the Member States. On one side, assuming an average 10 days per review (based on stakeholder input) and 27 Member States participating on average in 7 peer reviews each per year, a 20% reduction in the time needed to complete the process would imply a collective saving of around €63,000 in the first year, and €220,000 per year afterwards.

On the other side, non-monetary benefits are expected as follows:

- Facilitating a common understanding of the process among Member States, which, as highlighted in the evaluation study, is current lacking especially on how to assess new types of innovative solutions (e.g. mobile, biometric or video solutions), what are the best practices or what kind of implementation practices or requirements are considered level of assurance "substantial" or "high"[196]. This is likely to support the efficiency and effectiveness of the peer reviews
- Freeing up resources for the Member State representatives on the Cooperation Network to participate in more peer reviews, spend more time on the other international cooperation activities covered by the Network's mandate and undertake an adequate follow-up of the action points identified during the peer reviews. The effectiveness of the Cooperation network in fulfilling its mandate will also benefit from this.
- Increasing trust, transparency and accountability. The lack of legal value from the opinion has caused concerns among the Member States, as it does not prevent the notifying Member State to notify the peer reviewed scheme at a higher level of assurance than the conclusion of the peer review, greatly undermining trust in the system[197]. Publishing the opinions (as envisaged by this measure) would also enhance transparency and accountability of the assessments made.
- Improving incentives for notification. Currently, an eID scheme only becomes effectively available under the eIDAS network after almost 2 years. This duration is very long compared to the speed at which the identity market is developing, and could deter private identity providers from entering such procedure[198]. Member States that have not yet notified a scheme under eIDAS (particularly the smallest

[196] Deloitte, VVA, Spark Legal Network, Ecorys. (2020). Study to support the evaluation of eIDAS - Final Report. Unpublished.

[197] ibid

[198] ibid

MS) also identify the length and complexity of the process as a key barrier to notification[199].

In addition, a more efficient peer review process would provide, as a recurring benefit, for Member States and their representatives in the Cooperation Network, a reduction in time and complexity (and therefore, the costs) of the notification process. This is estimated by stakeholders to cost, on average, around €40,000 to €100,000 per notification[200].

5.1.4 Measure 0.4: Harmonise Supervisory Procedures for Trust Services

5.1.4.1 Public authorities

Costs

Given the current divergence in approaches across Member States on issues such as remote identifications, significant standardisation work may be needed at the European level in order to develop the additional guidance. Based on consultations with stakeholders, we estimate this cost to be in the order of €300,000. Supervisory bodies will also incur familiarisation costs of a similar order of €315,000 (i.e. €12,000 per SB) according to our estimates[201].

Benefits

Benefits for this measure are experienced in the area of compliance. Similar benefits were already reported in the literature. The vast majority of SBs and CABs reported inconsistencies both in the CAB accreditation processes and in the conformity assessment procedures carried out by the CABs on Qualified Trust Service Providers (QTSPs). [202] For example, differences in CAB accreditation schemes in the Member States and the absence of a standardised Conformity Assessment Report are reported to be a challenge. In some Member States, audit report contain approx. 100 pages while in other Member States the number of pages was reported being 500 pages. [203] As a result, this situation may lead to a non-harmonised trust Service market and questions regarding "quality" of Trust Services in the European Union may raise.

Desk research activities, interviews and the preliminary results of the online survey highlight that the impact of harmonised conformity assessment reports is expected to be marginal for Supervisory Bodies. Pursuant to Article 20 of eIDAS, "Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body (…) Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation.(…)". SBs across the EU therefore engage, to varying extents, in the following:

[199] This view was expressed by Member States with a small population participating in the cooperation network survey conducted for this study

[200] The estimate corresponds to the range of expenditure provided by Member states participating in a survey conducted for the evaluation of the eIDAS Regulation. It is based on 5 data points. Additional data points were collected through the interviews conducted as part of this study, which are consistent with the range estimated.

[201] For further details please refer to Annex. Notes on calculations *1.1.2 Familiarisation costs for Supervisory Bodies and Conformity assessment Bodies*

[202] ENISA (2018), *eIDAS: Overview on the implementation and uptake of Trust Services*, https://www.enisa.europa.eu/publications/eidas-overview-on-the-implementation-and-uptake-of-trust-services

[203] ibid

- Re-auditing QTSPs that have already been audited by CABs or requesting that they are re-audited. This can occur when the SB believes some important requirements have not been sufficiently verified.
- Requesting changes to conformity assessment reports.
- Carrying out inspections or surveillance audits after 12 months (if they do not request audits to be carried out annually)

Clearer and more harmonised rules on audits are likely to reduce the need for Supervisory bodies to re-audit QTSPs that have already been audited by an accredited CAB, as well as reduce time spent reviewing and requesting changes to the conformity assessment reports. Based on a survey conducted for the evaluation of eIDAS, only 8 of 25 respondents (representing SBs, CABs, and accreditation bodies) agree that the conformity assessment reports received by Supervisory bodies for trust service providers are of consistent quality and adequate[204]. However, differences among countries would occur depending on how often the Supervisory Bodies engage in these activities at the moment. In some countries, this is common practice, while in others (e.g. Austria) it is done on an exceptional basis. Overall, evidence collected on the number of audits conducted every year by Supervisory Bodies suggests these may range between 0 and 10[205]. Assuming that the average cost of an audit ranges between €20,000 and €50,000[206], harmonising and standardising these procedures is expected to reduce considerably the number of audits carried out by SBs in the former group of countries and have a positive impact favouring the Member States with a higher frequency of audits.

Tackling the legal uncertainty across the EU triggered by the possibility opened by the eIDAS Regulation to leave to the discretion of Member States the assessment on the equivalence of **remote identification** methods with the physical presence would generate significant internal market benefits, driven by the speed and convenience and cross-border reach of the remote processes.

The common position put forward by the Forum of European Supervisory Authorities (FESA) on the review of eIDAS lends support to the strong consensus on the need for greater harmonisation on key trust services aspects of the Regulation. Only one country (AT) expressed a general concern with regard to the possible cost implications of these reforms for the national competent authorities.

5.1.4.2 Conformity Assessment Bodies

Costs

The cost associated with this policy measure is based on the work in standardisation committees, the adoption of new routines and the amount of money spent by each CAB to familiarise staff with the new implementation acts and procedures.

Assuming that (i) each CAB employs only one person to learn the administrative processes and this person is able to pass this on to colleagues, costs associated to familiarisation are estimated to be approximately €339,000 (around €12,000 per CAB)[207].

[204] Survey: eIDAS review | Supervisory Bodies, Conformity Assessment Bodies, Accreditation bodies, Accessed 7 September

[205] Survey: eIDAS review | Supervisory Bodies, Conformity Assessment Bodies, Accreditation bodies, Accessed 7 September (data collected from Austria, Germany, Italy, Spain).

[206] Figure based on data collected from the interviews and through consultation with experts. This particular figure refers to external audit costs only (it does not include the cost of internal staff time allocated to participating in the audit)

[207] For further details please refer to Annex on calculation *1.1.2 Familiarisation costs for Supervisory Bodies and Conformity assessment Bodies*

Another member from the Cooperation Network highlight that in his country, CABs are not established yet (they are currently in the design phase), so new implementing acts would not generate high one-off adjustment costs. The same point goes for auditing schemes and conformity assessment reports.

Benefits

Some limited savings are expected with regard to the accreditation procedures. Stakeholder interviews suggest that the amount of time requested to complete the accreditation process varies between 5 and 10 men-days per standard. Assuming that the harmonised standards would result in 20% less time to complete the accreditation, the total benefit of greater harmonisation of accreditation procedures across Europe would be estimated at between € 17,000 and € 35,000 per year across all conformity assessment bodies in the EU[208]Despite the lack of standardisation of audits and conformity assessment reports, it is unlikely that the development of implementing acts will generate substantial economic benefits. Potential benefits are linked to cost savings due to a clearer regulatory framework.

Cost savings associated to the audit system are expected but are likely to be limited. According to the interviews carried out with CABs and thematic experts, CABs already follow the ETSI standards on audit in a number of countries. The definition of an implementing act is not expected to save a relevant amount of cost. However, the definition of binding standards is reported to enhance the competition across countries. As already noted in the literature, the fact that no binding standards have been defined resulted in the production of audits that differ in terms of quality. As a result, CABs based in Member States where the rules are stricter, offer the same service at a higher price compared to CABs based in Member States where the rules are not particularly strict. This is confirmed by the interviews carried out with relevant stakeholders: no binding standards for all CABs across Europe limits the number of potential clients. As a result, the introduction of an implementation act is expected to increase their revenues.

As already reported by ENISA and highlighted in the eIDAS evaluation survey above mentioned, interviews conducted with CABs for this study, currently there is a clear gap in standardisation with regard to Conformity Assessment Reports (CAR). However, CABs interviewed highlight that benefits are expected mainly when carrying out a conformity assessment procedure of a trust service based in another Member States. In this case, once binding harmonized standards for all conformity assessment bodies across Europe are available, it is expected that the previous difficulties raised by **"forum shopping"** by QTSPs and **divergent approaches** in the severity of audits in Europe would be alleviated. It is also likely that the stable framework would foster an increase of conformity assessment bodies revenues, while the definition of a standard conformity assessment report is also likely to provide more clarity on the requirements to be assessed and to reduce the amount of time requested to complete the report.

5.1.4.3 Trust Service Providers

Benefits

The main benefit that would arise for TSPs (qualified and non-qualified) are essentially linked to:

[208] For further details please refer to Annex A. Notes on calculations *Costs of standardised accreditation procedures for Conformity Assessment Bodies*

- a clear regulatory framework, reducing incongruences in the qualification of TSPs in different countries and their qualified trust services and therefore supporting a level playing field in the European trust services market
- ensuring no ambiguity in the accreditation and conformity assessment processes, which should reduce the risk of these processes identifying non-conformities. The net benefits to QTSPs will thus be modest. However, the literature review highlights potential benefits if implementing acts ensuring that the eIDAS requirements are satisfied at the same time meet the requirements of other communities like the CA/Browser Forum, browser vendors and application providers.[209]

5.1.4.4 Citizens and (end) users

Benefits

Introducing harmonized requirements on remote identification and its equivalence to physical presence would support citizens to avoid the difficulties raised by practical situations such as the need to renew their certificates or to receive technical support which, under many national legislations, they are required to be physically present in the country of issuance. If this measure implemented, they will not be faced with the choice between having to travel to their home country or being left without an active solution until they can proceed so.

5.2 Option 1 - Improve the current legal framework for cross-border recognition of national eIDs and trust services

Under this option, a European Digital Identity would be created in the form of a strengthened legislative framework for national eIDs notified under eIDAS. All these measures would be taken without extending the regulation scope nor affecting its underlying principles (e.g. applicable to eID solutions notified by Member States, mutual recognition and technological neutrality). Option 1 would be supported by the following core elements.

Measures to ensure all EU citizens and business can use trusted and secure eID means to access online public and private services

- **Measure 1.1:** Establish an obligation for MS to offer eIDs and to notify them under the eIDAS, facilitated by a streamlined notification procedure**.**

Measures to ensure a wide range of public and private online services is accessible using eID

- **Measure 1.2:** Establish a requirement for Member States to allow private online service providers across the EU to rely on notified eIDs
- **Measure 1.3:** Establish a harmonised cost-model and liability rules to facilitate private online service providers to rely on notified eIDs
- **Measure 1.4:** Extend the person identification data recognised cross border

Measures to ensure citizens are in control of their personal data and their security is assured

- **Measure 1.5:** Strengthen security requirements for mutual recognition

[209] ENISA (2019), *Towards global acceptance of eIDAS audits*, https://www.enisa.europa.eu/publications/towards-global-acceptance-of-eidas-audits

Measures to improve the EU market for Trust Services

- **Measure 1.6:** Introducing new Trust Services
- **Measure 1.7:** Harmonise the certification process for remote electronic signing
- **Measure 1.8:** Strengthening the Recognition of QWACs (Qualified Website Authentication Certificates)

5.2.1 Measure 1.1: Establish an obligation for MS to offer eIDs and to notify them under the eIDAS, facilitated by a streamlined notification procedure.

5.2.1.1 Public authorities

Costs

At present,12 Member States have already notified at least one scheme under eIDAS and 2 further ones have a scheme at the peer review and pre-notification stage. Consequently, the costs of this measure will be borne by the 13 remaining Member States.

Stakeholder feedback suggests that the **costs of the notification process** of a single eID scheme range between €40,000 and €100,000[210] on a one-off basis. This adds up to an estimated cumulative cost of between €520,000 and €1.3 million across the 13 countries that would need to notify a scheme in order to comply with the obligation. These 13 Member States already deploy various types of eGovernment platforms (e.g. user-name, password based) or trusted and secure eID systems allowing their citizens access to public services. Accordingly, it should considered that the additional cost caused by the mandatory notification will be linked to the implementation of the eIDAS related obligations (interoperability, connection to the eIDAS network). Taking as proxy the average initial costs of complying with eIDAS estimated by the *Evaluation of eIDAS* (€750,000 per Member State including the set-up of the eIDAS nodes), the overall cost of this measure is estimated at €9.7 million for the 13 countries.

In addition, depending on the timeline set for complying with this obligation, the eID Cooperation Network may see a significant surge in the **administrative burden** triggered by peer reviews. Assuming 13 additional peer review processes of 10 days each[211] (with 7 in 2021 and 6 in 2022) and each Member State participating into 4 peer reviews a year[212], this would amount to an overall cost of around €1.2 million in the next two years.

Finally, the European Commission is also expected to experience additional pressure due to its supporting roles in the peer-reviews and notifications processes. However, such administrative costs are not new ones to Member States as they are inherently linked to the existing notification procedure under eIDAS.

Benefits

The mutual recognition principle would be reinforced and Member States would see their role as providers of primary and secure legal identities be fully recognised also in the context of online also in the context of online cross-border transactions. As the trust and

[210] The estimate corresponds to the range of expenditure provided by Member states participating in a survey conducted for the evaluation of the eIDAS Regulation. It is based on 5 data points. Additional data points were collected through the interviews conducted as part of this study, which are consistent with the range estimated.

[211] As reported by experts during interviews.

212 Since participation is voluntary.

convenience in using such eIDs on regular basis will increase, a rise in the use of public services both at national and European is expected. By resolving the disparity among EU citizens with regard to the possibility to rely on their eIDs in cross border transaction, this measure would have direct positive impacts on the supply and usage of secure eIDs for online access to services across the EU, thus enhancing trust on line, raising awareness on secure practices and freeing EU citizens from digital barriers.

5.2.1.2 Citizens and (end) users

Benefits

Mandatory notification would make citizens and companies of the 13 notifying countries the first direct beneficiaries of such a measure. The direct effect for them would be to see their digital freedoms expanding considerably, by being able to authenticate (at least) to public e-services provided in other EU Member States. Taking into account each of these countries' population, the measure would open up access to cross-border eID for an additional 185 million EU citizens, or 154 million if only the population aged 15 and older is considered[213].

5.2.1.3 eID Providers

Costs

The costs for public authorities to develop a fully-fledged eID scheme from scratch would be shaped by specific cost drivers linked to inherent country characteristics as well to the overall system design or technology chosen. To provide an indicative range of investments: around €40-60 million were invested for the Finnish eID scheme; €72 million expenditures over 3 years in the Netherlands[214], while 100 € million estimate was provided by Sweden. However, the 13 remaining Member States who have not yet notified an eID already deploy various types of eGovernment platforms or trusted and secure eID systems allowing their citizens access to public services.[215]

5.2.1.4 Citizens and (end) users

Benefits

A more harmonised and transparent approach would shorten the time for notification of eIDs by Member States and increase the uptake by strengthening the confidence of citizens and businesses in the legal framework regulating eID and empower them to make informed choices, based on a clear understanding of the quality or features of eIDAS solutions.

5.2.2 Measure 1.2: Establish a requirement for Member States to allow a private online service providers across the EU to rely on notified eIDs

5.2.2.1 Online service providers

Costs

Estimates developed as part of previous EU interoperability projects suggest that building software from scratch to connect to an eIDAS node would imply a one-off cost to online

[213] EUROSTAT. (2020). Population by age group, 2019. Last accessed on 15 December 2020

[214] Dutch Report: (2012) Rekenhof - De elektronische identiteitskaart (eID) Toegangssleutel voor de burger tot e-government: (eID) Finnish and Swedish data: collected during interviews.

215 Member States are still in the process of implementing eID systems, mostly smartcard-based: Bulgaria, Cyprus, Greece, Poland, Romania, Slovenia. To be noted that the future Regulation 2019/1157 on strengthening the security of ID cards and residence documents obliges Member States to have an identity card with the security features specified therein by August 2021. Member States could build on the new identity cards and notify them as eID means under the eIDAS Regulation.

service providers for putting in place the required infrastructure (the global cost for a relying party could amount to €42,000[216]).

Benefits

An upgraded interoperability framework that enables more cost-efficient, direct service provider connectivity with the eIDAS network is likely to increase private sector take-up. This would trigger savings for private sector relying parties that decide to adopt these schemes in their workflows when the needed attributes come with the national eID. A study conducted on large retail banks suggests that by streamlining processes and adding technology to eliminate paper, operating expenses can be reduced by as much as 25% (a reduction of between 60% and 70% of records management associated costs[217]). Relying on the extended set of attributes provided by the national eIDs would contribute to this process.

5.2.2.2 eID providers

Costs

Notified eIDs should be adapted to fit the use-cases in the private sector. This may require costs which could widely vary and cannot be quantified. For instance, only three[218] notified schemes provide sufficient attributes today required for onboarding of natural persons in the financial sector (i.e. to open a bank account) and none provide all attributes for legal persons.

5.2.2.3 Citizens and (end) users

Benefits

No comprehensive data is available on the number of service providers (relying parties) connected to the national eIDAS node, and the fact that a relying party is connected to the eIDAS Node does not necessarily means that a cross-border citizens will be able to initiate a cross-border authentication on the online service provider's website[219]. Nevertheless, since a requirement to enable access to the eIDAS Network by online service providers will likely increase the number of private online service providers connected, it will also increase to some degree the number of those that offer this possibility to their customers, as well as contributing to expand EU citizens' access to trusted and secure solutions for identifying themselves online.

5.2.2.4 Public authorities

Costs

The measure may entail familiarization and training costs falling in particular on SPOC, since these provide support and guidance to service providers wanting to connect to the network and would therefore need to tailor their services to private sector relying parties and publish bespoke guidance to help them comply with eIDAS Nodes specifications.

---

216 LEPS Project. (2018). *D7.2 Report on Cost Benefit Assessment*

217 Deloitte (2012). Is it time to go paperless?: *Records management: The cost of warehousing bad habits*.

218 Signicat (2017) The rise of digital identities: Plugging the 'digital gap' in financial services onboarding. Out of 13 schemes notified at the time of the research. The number has now increased to 19.

219 Deloitte, VVA, Spark Legal Network, Ecorys. (2020). *Study to support the evaluation of eIDAS - Final Report.* Unpublished.

In this circumstance, Member States would also be expected to work with the private service providers on the standardisation of additional domain specific attributes to support private sector use cases.

5.2.3 Measure 1.3: Establish a harmonised cost-model and liability rules to facilitate private online service providers to rely on notified eIDs

5.2.3.1 Online service providers

Benefits

The development of a comprehensive and balanced cost and liability framework model is expected to incentivise use of the national eIDs by the private online providers. The clearer the contractual conditions on liability and prices online service providers would be charged for accessing the eIDAS network, the better the chances are for them to see opportunities and adhere to such a system.

One way in which guidelines on cost and liability will support the creation of benefits is in terms of bringing clarity and unformity to the access conditions for potential private sector relying parties. Currently, Member States have widely different approaches to costing the service for private relying parties, with some providing it for free and others charging their counterparts in order to recover the costs of usage of this public infrastructure when used for commercial purpose (e.g. banks using notified eIDs to reduce their onboarding costs).[220] As noted in the evaluation of eIDAS, liability rules are also set by the notifying Member State and highly variable across Europe, creating a situation where one notified eID scheme might be operating with a €100 maximum liability for damages due to negligence, whereas another Member State might require the minimum to be €10,000 [221].

This measure would likely contribute to removing uncertainties and national differences over the terms and conditions applying to usage of a notified scheme, therefore reducing transaction costs and the risk of inadequate compensation for damages. Ultimately, this is expected to increase the propensity of private online service providers to take up eIDAS solutions. The measure is likely to be most effective if the guidance provided covered all of the aspects that have been identified and requiring more clarity and harmonisation, namely[222]:

- the commercial contracting structure and pricing;
- the liability and support structure;
- responsibility for billing and payments, credit risk management;
- dispute resolution mechanisms.

5.2.3.2 Public authorities

Costs

With regard to the guidelines on costing and liability, these would mainly entail technical committee work costs from developing harmonised provisions.

---

[220] Deloitte, VVA, Spark Legal Network, Ecorys. (2020). *Study to support the evaluation of eIDAS - Final Report.* Unpublished.

[221] Deloitte, VVA, Spark Legal Network, Ecorys. (2020). *Study to support the evaluation of eIDAS - Final Report.* Unpublished.

[222] GSMA. (2018). *Mobile Connect for Cross-Border Digital Services Lessons Learned from the eIDAS Pilot*. https://www.gsma.com/identity/wp-content/uploads/2018/02/MC-for-cross-border-digital-services_eIDAS_Feb2018-Final.pdf

Upgrading the eIDAS interoperability infrastructure and updating the technical specifications to support the use of national eIDs by private sector's online service providers will result in some costs for Member States. For instance, there will be costs related to upgrading the operational capacity of eIDAS Nodes - in particular with respect to likely additional security, reliability and data protection requirements - to efficiently and securely handle increased levels of traffic. Taking into account the average technical costs of running the eIDAS node for the Member States (including annual upgrades), the expected overall one-off cost of this measure would amount to €6.1 million across the EU 27 (an average €225,000 per Member State)[223]. This is in line with other relevant references for the possible costs of upgrading the infrastructure, such as the grants attributed by INEA (Innovation and Networks Executive Agency) to support the cost linked to the set-up and operation of national eIDAS-Nodes (approximately €200,000 per Member State)[224]

In addition, there will be costs associated to adapt the existing eIDAS interoperability infrastructure to implement a common costing model that, however, would be mostly associated to regular enhancement of the eIDAS interoperability infrastructure. It is likely that the diversity of rules applicable at national level to private sector's relying parties will make it challenging for the Member States to agree on common cost model and related managing the revenues generated by the network.

Benefits

As the trust and convenience in using such eIDs on regular basis will increase, a rise in their use in public services both at national and European is expected.

With an hypothetical increase in transaction volume within the eIDAS network between 20% and 33% per year over the 5 years following implementation, the increase in revenue from this growth in transactions can be estimated at between €17 million and €53 million (assuming revenue of €0.01 per transaction) and between €797 million and €2.5 billion (assuming revenue of €0.48 per transaction[225]. These costs will depend on, the cost model chosen by Member State (paid by user and / or by volume).

Since some Member States monetise the offer for national eIDs for private relying parties while others provide the service free, developing a common costing model for the use cross border of notified eIDs by the private sector would avoid unfair competition and fragmentation of the EU authentication and attribute exchange market within the eIDAS network and between Member States. Private relying parties would not be able to adopt a "cherry-picking" approach and connect to the network via the most advantageous (free) eIDAS-Node. Similarly, overloading of certain national infrastructures would be avoided.

5.2.4 Measure 1.4: Extend the person identification data set recognised cross border

5.2.4.1 Public authorities

Costs

Some stakeholders expect that no significant costs will arise given the fact that work on an extension of the list of attributes is already in progress within the eIDAS technical subgroup

[223] For further details on these calculations, please see Annex on Calculations, section *1.1.5 Overall costs of upgrading the eIDAS infrastructure and updating the technical specifications.*

224 INEA, eIdentification and eSignature project pages, see: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/projects-by-dsi/eidentification-and-esignature

[225] For further details on these calculations, please see Annex A. Notes on Calculations, section *1.1.6 Potential revenues for Member States due to the upgraded infrastructure*.

(€20,000 per Member State). However, as revealed by the current works of the eIDAS technical subgroup on the topic and as expressed by certain stakeholders during the public consultation[226], finding an agreement between Member States on the attributes and on their technical and semantic expression is challenging (e.g. the "nationality" attribute, currently discussed has different interpretations in various countries). This activity will certainly benefit from the effort made and the lists of attributes already defined in the Member States[227] or internationally[228] where the use of national eID by private sector service providers is facilitated and supported. Significant standardisation work will also be necessary and, based on stakeholder views, is likely to create one-off costs of around €300,000.

The connection to the eIDAS Node of the relevant national registers/systems that contain the required attributes at national level (for instance a patient identifier) might imply additional costs for the Member States, depending on how their eIDs are organised. The attributes enablement costs could be minimised by leveraging on dedicated EU funding schemes, building for instance on funding in the context of the Digital Europe Programme.

Similarly, the interoperability framework would need adjustments to allow direct integration by private sector relying parties. This would imply a one-off cost to adapt the current infrastructure used for the exchange of the data sets only in the context of public services, which can be estimated as part of the upgrade work discussed above (see *Costs* of Measure 3).

Benefits

The eIDAS Regulation, and in particular the Commission Implementing Regulation (EU) 2015/1501, currently allows the exchange of a minimum dataset of attributes for cross-border recognition (name, family name, date of birth and cross border identifier). Additional attributes outside the minimum dataset can be shared only on a voluntary basis.

This measure will provide a legal reference for the trustworthy exchange of additional attributes, which will benefit Member States by providing legal certainty and in particular by clarifying their liability in those circumstances, as well as facilitating the ID matching (eIDAS identifier - national identifier) process where applicable.

The extension of the list of attributes will address a weakness identified early on in the implementation of the eIDAS Regulation. As discussed in the problem definition section, the minimum dataset is perceived by many stakeholders as too limited to support a wide range of private sector use cases[229]. Further, over 70%[230] of Member States responding to a survey conducted for the evaluation of eIDAS (strongly) disagree that eIDAS minimum dataset allows to uniquely identify both natural and legal persons. Similarly, some Member States (BE, LU, NL) explicitly highlight the positive impact on extending the list of attributes to facilitate eID matching (increasing data accuracy) and better uphold the principle of data minimisation.

226 See for example FESA. (2020). Position Paper On the review of the eIDAS Regulation FESA's answer to the European Commission's consultation

227 See for example the list of attributes defined in Italy for SPID https://www.agid.gov.it/sites/default/files/repository_files/regole_tecniche/tabella_attributi_idp_v1_0.pdf

228 See for example the approach in the UK https://www.gov.uk/government/publications/attributes-in-the-uk-digital-identity-and-attributes-trust-framework

229 See for example FESA. (2020). Position Paper On the review of the eIDAS Regulation FESA's answer to the European Commission's consultation. http://www.fesa.eu/public-documents/FESA_Position_Paper_eIDAS_2020_Review.pdf

230 13 out of 18 non-blank responses

5.2.4.2 Citizens and (end) users

Benefits

Providing a legal reference for the exchange of subsets/supersets of the minimum dataset with an assigned level of assurance via the eIDAS network would reduce the need and associated administrative burden and costs for users to fetch and provide pre-defined authentic documents or attestations (e.g. birth certificate to prove the age) in a number of use cases and transaction with public and private sector service providers. This will therefore reduce unnecessary sharing and circulation of personal data, thus providing stronger protection for EU citizens' security and privacy. By raising their trust, users would feel more protected and comfortable on line as well as access an increased number of online service providers.

5.2.4.3 Online service providers

Benefits

Many service providers do not currently have opportunities for re-using notified schemes that meet essential needs for customer identification and due diligence. For instance, a previous analysis shows that only three[231] notified schemes provide all of the attributes required for onboarding natural persons and none provide all attributes for legal persons.[232]

This measure would help enable private sector to access solutions that go further in meeting their needs. As a result, there might be savings for private sector relying parties that decide to adopt these schemes in their workflows when needed attributes come with the eID.

A study conducted on large retail banks suggests that by streamlining processes and adding technology to eliminate paper, operating expenses can be reduced by as much as 25% (a reduction of between 60% and 70% of records management associated costs).[233]

5.2.4.4 Online service providers

Costs

As highlighted in the Impact Assessment for the DMA, compliance costs would be miniscule as compared to the gatekeepers revenues and could be absorbed by gatekeepers with little incentive for them to pass on costs to business users or to consumers, Indirect (other than compliance) costs may be higher, however, the impact of such changes is difficult to quantify.

Benefits

The measure requiring online gatekeepers not to discriminate and be interoperable with eIDs recognised cross-border would have direct benefits for the gatekeepers themselves. They could use the notified eIDs as ready-made tools to enrol users on the basis of verified identities, to quickly validate their identity, minimise security risks and, most importantly, reinforce their GDPR compliance.

Government-issued/recognised eID means interoperable with the gatekeepers' platforms would support them to contain the proliferation of fake news, fake reviews damaging for

[231] Out of 13 schemes notified at the time of the research. The number has now increased to 18 (plus 1 country with a scheme at the pre-notification stage)

[232] Signicat (2017) *The rise of digital identities: Plugging the 'digital gap' in financial services onboarding*

[233] Deloitte (2012). Is it time to go paperless?: *Records management: The cost of warehousing bad habits.* https://www2.deloitte.com/content/dam/Deloitte/za/Documents/financial-services/ZA_ItsTimeToGoPaperless_24042014.pdf

their business and other activities aiming to mislead citizens and consumers. Eurobarometer data reports that 80% of Europeans have come across information they believe was false or misleading several times a month and 85% of the respondents perceive this as a problem in their country[234].

5.2.5 Measure 1.5: Strengthen security requirements for mutual recognition

5.2.5.1 Public authorities

Costs

A number of countries already relies on ICT security certification for their eID means when they take the form of the electronic identity cards (e.g. France, Austria, Estonia, Italy, Spain, Poland, etc.). However, ICT security certification is not widely used for other type of eID means (e.g. SPID in IT, Itsme in BE, etc.). The MS that already require ICT security certification for their eID means will not incur significant additional costs. For other countries, the conformity assessment process may require more material changes to existing methodologies, possibly creating up-front costs. While these costs can widely differ among countries, and stakeholders consulted found it unfeasible to give a reasonable quantitative figure, it is estimated that the familiarisation costs could amount to an average € 9,000 per Supervisory Body, adding up to €228,000 across the EU 27.[235]

Benefits

Promoting ITC security certification of certain elements of eID means via EU certification schemes (as per the Cybersecurity Act) coupled with conformity assessment reports, would improve the security of the eID schemes by making it easier for the Member States' to prove the compliance of the notified eID schemes with the eIDAS security requirements (as defined in the relevant Implementing Acts)[236], thus contributing to the efficiency savings discussed above. Some of the Member States consulted (DE, FR, CZ, HR) expect a reduction of the costs and delays linked to a lack of a commonly agreed methodology and a reinforced role of eIDAS as a horizontal regulation for electronic identification.

Conformity assessment and ITC security certification would directly address the current difficulties raised by the lack of agreement between Member States on the criteria that make, for instance, mobile scheme resistant to high level security attacks. Generally, ITC security certification would result in increasing trust and security in the eID solutions. Such an approach coupling the reliance on conformity assessment report and ITC security certification would also ensure better alignment of the governance of the eID part of the Regulation with the set-up already in place for the trust services (audits, regular revisions of standards, etc.), which would improve the coherence of the overall eIDAS enforcement efforts.

5.2.5.2 Citizens and (end) users

Benefits

Citizens would benefit from an increased public trust in eID products, services or processes providing a certified level of cybersecurity. Promoting harmonised cybersecurity level in provisioning and using of eIDs will make users (in particular citizens

234 Flash Barometer (464) Fake news and disinformation online. See: https://data.europa.eu/euodp/data/dataset/S2183_464_ENG

235 For this calculation we used the same reasoning for Familiarisation costs (See *Annex A. Notes on Calculations 1.1.2 Familiarisation costs for Supervisory Bodies and Conformity assessment Bodies*) assuming that the 25% less man/days will be needed for such upfront changes

236 COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means

and SMEs) understand what it means to be European as well as the values and protection the EU guarantee.

5.2.5.3 eID providers

Costs

The main one-off costs envisaged for eID providers are:

- Certification, estimated at an average €60,000-€120,000[237] (including external audit and internal staff costs);
- Ex-post adjustment of the products and its documentation to a certification scheme.

Recurrent costs are considered moderate to high. Respondents experience frequent modifications of the eID scheme that would in principle require frequent re-certifications processes. The costs/fees of re-certifications are strongly dependent on the complexity of the eID mean and the certification scheme adopted: it is necessary to consider that actually there is a wide variety in certification schemes used by Conformity Assessment Bodies (CABs), both in audit effort and quality, which is reflected in Conformity Assessment Reports (CARs) received by Supervisory Bodies.

As highlighted by some stakeholders, there is a risk that certification may affect innovation if certification standards fall behind technological advances. This could however be prevented through effective standards review mechanisms and the coexistence of alternative means in absence of standards, as it is already provided in eIDAS for qualified creation devices. This potential negative effect may also be offset by the positive contribution of certification to interoperability (as has been the case for e-signatures), which may instead act as enabler for greater innovation. The reliance on conformity assessment report and ITC security certification are understood as a voluntary measure taken by Member States to simplify the peer review process.

Benefits

This category of stakeholders would mainly benefit from the introduction of a security certification. Stakeholder consultations suggest that it could be beneficial and reduce the cost of proving conformity, as well as create opportunities to certify for private providers that are unable to do so due to the lack of standardisation. 54% percent of public consultation responses received support the introduction of a certification.[238]

Overall, an alignment between the Levels Of Assurance, as defined by the eIDAS Regulation and the Cybersecurity Act, would solve the issue of fragmentation, hence simplifying certification for companies. Indeed, the cybersecurity certification framework will introduce new requirements, for example, different assurance levels (basic, substantial and high) to cover different risk analysis. It is very important to be able to certify products, solutions and services at a level that is consistent with risks to be mitigated, but also taking into account the market needs (cost, time and performance to be achieved). An alignment of the levels of assurance between the certification of eID means and the cybersecurity certification framework would also clearly demonstrate the security of eID schemes.[239]

Moreover, relying on a harmonized, well-functioning certification process would contribute to reducing costs and delays related to the lack of commonly agreed assessment

[237] Based on information gathered through interviews

[238] See Annex E.

[239] Eurosmart (2020) *Eurosmart's feedback on an EU Digital Identity scheme (EUid)*

methodology of security requirements[240]. The following points demonstrate the potential impacts of having an EU-wide certification:

- **Reduction of costs associated with multiple testing to obtain national certification;**
- **Reduction of adaptation costs to meet national standards/requirements.** Common EU standards reduce the need to produce variants adapted to meet different national specifications;
- **Reduction of the 'time-to-market' of eID means. Having obtained EU certification**, eID means may be introduced to the whole EU market without delays caused by the need to meet national requirements;
- **Enhanced transparency of performance requirements and standards/specifications**. Common EU performance requirements and conformity assessment protocols should enable ID providers to better develop eID means according to 'predetermined' criteria, reducing uncertainty of product conformity assessment outcomes;
- **Acceleration of development process**. A common regulatory framework with reference to defined eID means standards/specifications should make it easier for ID providers to direct their research and development efforts to meeting regulatory/market requirements.

Savings would be generated for the eID providers as a result of less extensive re-auditing of new components, relying on elements that have already been certified for use in other applications. Assuming that the average cost of an external audit ranges between €20,000 and €50,000 plus an equivalent amount to cover internal staff costs, bringing the overall cost to €60,000-€120,000[241], and assuming a 20% reduction in the costs triggered by the reutilisation of certification, the savings would be in the range of €12,000-24,000 per audit for each private eID service provider. Overall, stakeholders identify the benefit in terms of risk avoidance (i.e. reducing the risk that the audit will identify non-conformities) to be far more valuable than these savings.

5.2.6 Measure 1.6: Introducing new Trust Services

5.2.6.1 Public authorities

Costs

The introduction of a new qualified trust service for **e-archiving** would incur costs linked to familiarisation for supervisory bodies as well as enforcement and administrative costs. There might also be some interoperability costs which would be absorbed under Digital Europe Programme specific activity on e-archiving.

5.2.6.2 Trust service providers

Costs

TSPs wanting to enter the market for qualified preservation services would incur compliance costs similar to those applicable to qualification for other trust services currently covered by eIDAS. Based on consultations with stakeholders, these would include:

[240] As identified by the stakeholders consulted and the existing literature, the fact that the eIDAS Regulation and CIR 2015/1502 do not require a specific certification scheme for devices used within eID means for LoA High has brought a lack of consistency between security assessments of such devices.

[241] As estimated by stakeholders in interviews

- **One-off costs of initial qualified status.** Estimates for these costs varied significantly among the stakeholders consulted, due in part to the size of the provider, sector and number of services offered. The average administrative costs linked to qualification are €545,000[242].
- **Recurrent compliance costs.** Stakeholder estimates for these costs were also wide-ranging, with figures suggesting annual costs are on average €255,000[243].

Benefits

The creation of e-archiving as a trust service under eIDAS will enable TSPs (many of them are already providing this service) to enhance trust in their service offer by inclusion in the European trusted lists of this service, likely resulting in increased consumer awareness of and demand for the service. In addition, the possibility to provision such a service on the whole EU market will give opportunities for economy of scale both on the service being provided – thus becoming more economic and efficient – as well as on the usage by businesses (in particular SMEs) that have to rely diverging nationally services. For every additional 1% of EU businesses that purchase an electronic archiving solution every year, additional revenue of over €37 million a year would be generated for providers[244].

5.2.6.3 Citizens and (end) users

Benefits

Citizens can benefit from the introduction of a new trust service for e-archiving since it would complement the qualified preservation of qualified electronic signatures (a trust service already regulated under eIDAS), avoiding fragmentation at European level as several Member States have already defined such trust service at national level. Because of the EU market offered to trust service providers and the likely competition that will be stimulated, the end users will benefit from more competitive services and lower costs.

5.2.7 Measure 1.7: Harmonise the certification process for remote electronic signing

5.2.7.1 Citizens/end users

Benefits

Based on data gathered for the eIDAS Expert group, greater harmonisation in this area finds generally support among qualified signature creation device vendors and qualified trust service providers, who would be most directly impacted by it[245].

Standardisation of the certification process would support fair competition and increase the security of trust services for end users. A unified framework that makes reference to EU-wide standards would bring more coherence in remote signing, ensure greater transparency and compliance of solutions with the eIDAS Regulation and better guarantee the security

[242] This is the average cost of administrative expenses linked to achieving and maintaining the qualified status reported by respondents to the survey of TSPs conducted for the evaluation. The figure is based on 16 data points from QTSPs that are large private organisations, public organisations and micro-enterprises or SMEs.

[243] This is the average annual cost of administrative expenses linked to compliance with eIDAS reported by QTSPS responding to the survey of TSPs conducted for the evaluation of eIDAS. The figure is based on 12 data points from QTSPs that are large private organisations, public organisations and micro-enterprises or SMEs.

[244] For further details on this calculation please refer to Annex on calculations section *1.1.7 Increased revenues for Trust services related to the introduction of eArchiving*

[245] Based on 34 responses collected in 2019 for the second report to the sub-group of the eIDAS Expert group on electronic identification and trust services, available on request.

of sever signing systems. As a result of greater harmonisation, the acceptance of mobile trust services in the market would also be enhanced.

5.2.7.2 Trust service providers

Costs

In terms of costs, harmonised certification would require operators to adapt to new processes and requirements, which would likely imply additional resources in the short term. The switch to a Common Criteria (CC) certification in particular is seen as increasing costs because it would be time-consuming to develop, modify, integrate, certify the solution, certify and audit the service, and in particular to rapidly patch any identified security vulnerabilities and deploy updates; this carries a risk of creating an unfair advantage for the larger, better resourced providers in the market.

5.2.8 Measure 1.8: Strengthening the Recognition of QWACs (Qualified Website Authentication Certificates)

5.2.8.1 Public authorities

Costs

Increased use of QWACs by public authorities in Member States (e.g. by incorporating them in public sector websites) is expected to have positive effects in terms of raising awareness on the benefits of these tools, however their take-up is not expected to be guaranteed solely on these grounds. Since some Member States (e.g. Spain[246]) already require (according to national laws) all public administrations to use QWACs, this measure would require focused campaigns to promote use among those that are not subject to similar requirements. Based on stakeholder views and previous estimates of the costs of EU-wide awareness-raising campaigns[247], the costs of this measure (including setting up a marketing campaign for awareness raising) could be in the region of €200,000-€400,000 on a one-off basis.

5.2.8.2 Citizens and (end) users

Benefits

Qualified Web Authentication Certificates will increase trust and reduce fraud in the online environment. A high level of trust in who is behind a website is particularly important related to online service provided by public and private sectors, e.g. e-commerce, e-banking and e-health. The use of QWACs would also support the principle of transparency as set out in Article 13 and 14 of the General Data Protection Regulation and strengthen data protection

5.2.8.3 Online service providers

Costs

The measure to ensure that users can use QWACs will come with a cost of around €550 per year, which will need to be sustained by all online service providers required to use it.

While they are not service providers, please note that for **browsers**, recognition of QWACs may entail some impacts although costs are likely to be limited as these procedures are already carried out or are part of standing standard procedures.

---

[246] ENISA.2016. Security guidelines on the appropriate use of qualified website authentication certificates

[247] See for example DG CONNECT. (2017). Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

From the point of view of browsers, recognition of QWACs may entail costs, which are likely to be limited as these procedures are already carried out or part of standing standard procedures and may include:

- Baseline certificate checks: these would be carried out by browser to ensure the source is a valid domain, according to their internal policies. In order for a TLS certificate[248] to work within a given browser by default, the browsers must evaluate the TSP responsible for issuing that certificate, covering aspects such as technical interoperability and alignment with business, user, and product needs and policies. No additional cost is expected as these would remain part of the checks the vendors already undertake.
- Checks to ascertain that certificate(s) used ***to*** authenticate the web site and meet the EU requirements – including, for instance, checking the certificate against the EU Trusted List to confirm conformance to EU requirements for QWACs. At this point, some identity information would be displayed to the user which links the certificate to the natural or legal person behind the website, alongside an "EU Qualified Status" trust mark. A new standard may be required to set out to support this process. While the costs of these checks are not precisely quantifiable from the available information, stakeholder consultations suggest that checks against the EU Trusted List would not require major development efforts and examples have already been developed.[249]

Summary of main costs and benefits for Policy Option 1

Policy option 1 – summary of main costs and benefits		
Measure	**Cost**	**Related policy options**
Measure 1.1: Establish an obligation for MS to offer eIDs and to notify them under the eIDAS, facilitated by a streamlined notification procedure.	Compliance with eIDAS related obligation - €9.7 million for public authorities (envisaged only for 13 Member States)	1, 2, 3
	Increased administrative burden due to mandatory notification - €0.52 - €1.3 million for public authorities (envisaged only for 13 Member States)	1, 2, 3
	Increased administrative burden due to additional peer reviews - €1.2 million for public authorities (in the next two years, cumulative for all Member States)	1, 2, 3
Measure 1.2: Establish a requirement for Member States to allow private online service providers across the EU to rely on notified eIDs	Infrastructural cost to connect to an eIDAS €42,000 per each online service provider	1,
Measure 1.3: Establish a harmonised cost-model and liability rules to facilitate private online service providers to rely on notified eIDs	Upgrading eIDAS nodes infrastructure - € 6,1 million for public authorities	1
Measure 1.4: Extend the person identification data recognised cross border	Committee work needed for standardisation - €300,000 for public authorities	1, 2, 3
Measure 1.5: Strengthen security requirements for mutual recognition	Compliance costs due to certification - €228,000 for public authorities	1, 2, 3
Measure 1.6: Introducing new Trust Services	Compliance costs linked to the introduction of a new qualified trust service - €545,000 per each trust Service Provider (one-off) Compliance costs linked to the introduction of a new qualified trust service - €255,000 per each trust Service Provider (recurrent costs)	1, 2, 3

[248] TLS = Transport Layer Security

[249] See for instance: https://addons.mozilla.org/en-US/firefox/addon/eidas-qwac-validator/

Measure 1.7: Harmonise the certification process for remote electronic signing	Costs related to compliance with new certification process for Trust Service Providers	1, 2, 3
Measure 1.8: Strengthening the Recognition of QWACs (Qualified Website Authentication Certificates)	Awareness raising campaign - €200,000 to €400,000 for public authorities QWACs-related compliance costs - €550 per year, per each online service provider	1, 2, 3
Measure	**Benefit**	**Related policy options**
Measure 1.1: Establish an obligation for MS to offer eIDs and to notify them under the eIDAS, facilitated by a streamlined notification procedure.	Enhanced digital inclusion for citizens / end-users	1, 2, 3
	Increased personal data protection and online security for citizens / end-users	1, 2, 3
	Increased access to public services through secure eIDs for citizens / end-users	1, 2, 3
Measure 1.2: Establish a requirement for Member States to allow private online service providers across the EU to rely on notified eIDs	Costs savings in operating expenses up to 25% per year for online service providers	1, 2
Measure 1.3: Establish a harmonised cost-model and liability rules to facilitate private online service providers to rely on notified eIDs	Increase revenues from increased online transactions through eIDAS nodes - €17 million to €2,5 billion – for public authorities in the next 5 years	1, 2
Measure 1.4: Extend the person identification data recognised cross border	Increased personal data protection and online security for citizens / end-users	1, 2, 3
Measure 1.5: Strengthen security requirements for mutual recognition	Savings in compliance costs for public authorities	1, 2, 3
	Savings in compliance costs (related to security certifications, GDPR requirements) - €12,000 to €24,000 - for eID providers	1, 2, 3
	Increased personal data protection and online security for citizens / end-users	1, 2, 3
Measure 1.6: Introducing new Trust Services	Increased revenues due to the introduction of eArchiving - €37 million a year for every additional 1% of businesses purchasing an eArchiving solution - for Trust Service Providers.	1, 2, 3
	Enhanced offer in the Trust Services market for citizens / end-users	1, 2, 3
Measure 1.7: Harmonise the certification process for remote electronic signing	Increased competition and security of trust services and acceptance of mobile trust services for citizens / end-users	1, 2, 3
Measure 1.8: Strengthening the Recognition of QWACs (Qualified Website Authentication Certificates)	Cost savings from reduced damages related to cybercrimes for citizens / end-users	1, 2, 3
	Increased personal data protection and online security for citizens / end-users	1, 2, 3

5.3 Option 2 – Creating a market for the secure exchange of data linked to identity

In Option 2 involves the establishment of a market supporting the delivery of a European digital identity ecosystem in the form of a new qualified trust service for the exchange of digital identity attributes across borders, such as proof of age (e.g. for accessing age restricted social media), professional qualifications (e.g. lawyer, student, doctor), digital driving licences, medical test certificates etc. The scope of eIDAS would be expanded to cover this new trust service where identity data and attributes would be securely linked to the legal eID of the user, making the data trustworthy and legally enforceable across borders. Each specific measure is clustered according to different larger objective categories:

The measures to provide access to trusted and secure digital identity solutions for all **EU citizens and businesses** cross borders are the following:

- **Measure 2.1**: creating a new qualified trust service for the secure exchange of data linked to identity
- **Measure 2.2**: require MS to make available data stored in authentic sources for the secure exchange of data linked to identity

The measures to make accessible a wide range of **public and private online services** relying on trusted and secure digital identity solutions cross border are:

- **Measure 2.3**: setting security requirements and common technical standards for the secure exchange of data linked to identity
- **Measure 2.4**: define the legal effect of digital identity credentials
- **Measure 2.5**: regulated sectors such as energy or finance and the Public Sector would be required to rely on Qualified digital credentials

Measures to provide citizens full control of their personal data and assure their security when using digital identity solutions

- **Measure 2.6**: legal requirements to ensure the protection of personal data

As part of the CBA section of the PwC Support Study to the Impact Assessment there was a deliberate methodological choice of jointly appraising measure 1, measure 2, measure 3, measure 4 and measure 5. These measures from an impact assessment point of view share the same impacts to the stakeholders category. For the sake of clarity and readability these impact measures are all jointly assessed.

In contrast, measure 6 on the legal requirements to ensure the protection of personal data is assessed as a standalone measure.

5.3.1 Measure 2.1 to Measure 2.5 - Creating a new Trust Service for the secure exchange of data linked to identity

5.3.1.1 Public authorities

Costs

In the creation of a new trust service for the secure exchange of data linked to identity a series of costs will have to be sustained by public authorities at national level. These can be summed up with the following:

- **Technical costs** for developing API thus enabling the access to the authentic sources to trust service providers –Allowing qualified trust service providers access to data stored in authentic sources with prior consent of the user would require the development at EU level of standardised Application Programming Interfaces (APIs) enabling integration from target public administrations across Europe. The costs for developing the API would be of around €30.000[250]. The development does not include the costs for standards setting of the API itself. These shall be commissioned to standardisation bodies or organisation composed by trust service providers, academia and stakeholders with skills and experience in defining standards for API such as the Cloud Signature consortium. The work, however, will benefit from and build upon already existing relevant standards.

  Public authorities would incur in integration costs to the API of around €18,000 to €27,000[251], which is a cost linked to digitization of public services and not directly linked to the eIDAS Regulation. The recurrent costs related to annual infrastructure assessment and maintenance costs are expected to be around 7.000€ yearly. By leveraging on the compliance obligations of the European legislation on open data and re-use of public sector information, the public sector can recover the marginal costs incurred or the costs related to the processing of the request for re-use .There are considerable uncertainties around the total number of organisations in Member States that will have to connect their systems through API. It is unknown at which level organisations hold data linked to identity or whether multiple data providers use the same system or database. Yet a study focusing on public entities integration to Single Digital Gateway estimates 23.120 organisations as relevant. Therefore, the overall total costs for Member states for integration would be of around 625 M € while the recurrent costs are expected to be overall 162 M € per year . This will depend extensively on the depth and breadth of the type of identity data that will be considered in scope. By leveraging on the compliance obligations of the European legislation on open data and re-use of public sector information, the public sector can recover the marginal costs incurred or the costs related to the processing of the request for re-use .

- **Communication and awareness raising costs** for the onboarding of public authorities in enabling to access their authentic sources. An EU and national level communication campaign would underpin the effective take up of public entities data owners to enable trust service providers to access their authentic sources. Awareness raising activities are assumed to be cost 8.400.000 € targeting an audience of 23.120 administrations and all EU citizens at large.

[250] Refer to Annex A note on data and calculation of costs and benefits, Policy Option 2: “Costs of API development”.

[251] Refer to Annex A note on data and calculation of costs and benefits, Policy Option 2: “Technical Integration costs to the API”.

- Costs for public administration acting as supervisory bodies for the **correct oversight of the new trust service landscape**. This change may imply an increase in resources needed for supervisory duties, i.e. enforcement costs, at the national level. More specifically:
    - **One-off costs**. Set up costs mainly linked to familiarisation (entailing a one-off cost of familiarisation of around €12,000 on average per supervisory body), staff recruitment and training would also need to be considered.
    - **Recurring costs**. With eID becoming a trust service, additional staff resources may need to be allocated to cover increased supervision needs at the national level if the national competent authorities maintain their role in the supervisory system. According to the views collected for this study, this cost could be significant. We estimate the recurrent annual costs of enforcement for supervisory bodies to be on average €282,000[252] per supervisory body. In this scenario, a doubling of the workload for each supervisory body would increase costs of enforcement by the same amount, reaching a total of around €8 million across all Member States. This cost could be mitigated if efficiencies from harmonisation were achieved If instead, the role of national supervision was dramatically reduced or eliminated as a result of a European Supervisory Trust Authority, these costs could be significantly reduced.

- **Costs linked to developing technical standards**. EU Digital ID will require investments which will depend on the technical standards employed. If the existing eIDAS profile will be used, costs should be comparable to those estimated for the integration of notified MS eIDs. Standard-setting is a multi-stakeholder decision making process with costs ranging around €1-2 million for the definition of a technical standard[253]. However, ongoing international standardization activities are already well-advanced, so that the costs of completing this process would be reduced significantly. Based on our interview consultations, EU grants for standard definition – which rely on the voluntary work of experts – are quoted on average at around €200,000 for the definition of one standard.
- **Expenses in international coordination.** Data collected for the evaluation suggests that Member States spend between €25,000 and €90,000 a year on international cooperation activities[254]. This expenditure could be expected to increase moderately in response to this measure.

Benefits

The main benefit for public administrations is linked to the possibility to rely on digitial identity autentication attributes and credentials sourced from verified and trusted surces in other Member States, further supporting the application of the once only principle cross border. The purpose to add new trust services related to the secure exchange of data linked

[252] This is the average cost incurred by SBs for supervisory activities as reported by respondents to the survey of SBs conducted for the evaluation of eIDAS. The figure is based on 9 data points.

[253] This is mainly made by the cost of hiring highly specialised technical staff to work on developing the standards for a number of months, estimated in consultation with experts in standard development and negotiation at EU level.

to identity boil down to the benefits associated to the use of platforms, credentials, and services to authenticate and/or verify the identity of end-users

- **Reduced costs of internal processes involving customer identity verification.** Efficiency gains for the service provider would be generated as a result of the removal of data verification step and enhanced user/customer experience with less or no physical presence required, and the possibility to re-use existing processes. The magnitude and type of this potential benefit will differ across sectors, depending on the level of digitalisation and identification needs linked to the type of service provided. For example, banks implementing the privately issued solutions may see a reduction in the cost of onboarding clients and wider costs of compliance, while health providers may also reduce costs related to the administrative procedures to identify patients and gain efficiencies from the dematerialisation of documentation.

- **Reduced fraud costs**. Using trusted identity credentials would increase accuracy in establishing that the customer is who they say they are based on verifiable attributes/credentials, mitigating losses from fraud, errors and fines linked to inaccurate customer identification and verification of transactions. In a recent survey, 84% percent of businesses said that the burden of fraud risk mitigation would be reduced if they were certain about the identity of a customer (42% said significantly reduced).[255] Higher data accuracy and reliability due to the trusted input system, would result in a reduced probability of errors and fraud. Liability costs are also likely decrease as a result of clearer liability for the correctness of the data.

5.3.1.2 Trust Service Providers

Costs

TSPs would incur in compliance costs, which we assume to be similar to the costs incurred today by qualified and non-qualified trust service providers regulated under eIDAS. This would include:

- **One-off costs of initial qualified status.** Estimates for these costs varied significantly among the stakeholders consulted, due in part to the size of the provider, sector and number of services offered. The average administrative costs linked to qualification are €545,000[256].
- **Recurrent compliance costs.** Stakeholder estimates for these costs were also wide-ranging, with figures suggesting annual costs are on average €255,000[257].
- **Costs from required technical changes to deliver the new service solutions to the specifications.** Technical costs from the need to bring the attribute service up to the standards prescribed by the Regulation which cannot be estimated as they are entirely dependent on the technical standards which are not defined yet.

---

[255] Experian. (2018). *The 2018 Global Fraud and Identity Report* https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf

[256] This is the average cost of administrative expenses linked to achieving and maintaining the qualified status reported by respondents to the survey of TSPs conducted for the evaluation. The figure is based on 16 data points from QTSPs that are large private organisations, public organisations and micro-enterprises or SMEs.

[257] This is the average annual cost of administrative expenses linked to compliance with eIDAS reported by QTSPS responding to the survey of TSPs conducted for the evaluation of eIDAS. The figure is based on 12 data points from QTSPs that are large private organisations, public organisations and micro-enterprises or SMEs.

Benefits

Existing TSPs would be mainly attracted by the greater market opportunities available to trusted providers of data exchange services linked to identity. Overall, the creation of such new trust service is likely to result in a significant expansion of the potential user base for these schemes by several times over, due to a better ability by providers to internationalise[258]. For example, one stakeholder suggests a tenfold increase in the number of users that could be reached by such a scheme if it gained cross-border recognition under eIDAS. The expansion of the user base is likely to be further supported by a greater re-use of identity credentials under eIDAS. Bringing credentials verification under eIDAS is seen as creating more scalable models for cross-border eID recognition and therefore more effective in increasing adoption.

Increased usage by end users and increased legal certainty would have an expansionary effect on the market for EU TSPs, with more potential customers and less unpredictability about legal validity and liability. Moreover, the adoption of common technical standards would significantly help Trust Service Providers by making the trust services market harmonized at the EU level.

5.3.1.3 Online service providers

Costs

Costs incurred by online service providers are mainly related to IT integration to the API. Integration costs through an API limited to enabling a new way of authenticating are expected to be from €18,000 to €27,000[259]. The initial cost will vary depending on the level of integration sought, the specific use case and the number of standard components that can be used. Relying parties need to upgrade their portals and carry out adjustments to have a new system of verified credentials and attestations.

Costs will also depend on the business model. In the commonly used business model, the costs are borne by the service provider / relying party, although there may be cases where the user will need to pay (part of) the costs[260]. To have a scheme for the exchange of credentials which is widely adopted, there is a need for an economic model with clear monetization. The stakeholders consulted provided insights to the business model for the exchange of credentials. The key point is that it is not the “order” or the citizen that shall pay to earn the credentials, but rather the online service providers requesting the verification that would pay the trust service provider. In this scenario, the order is not restrained into making a request and the issuer is incentivized to release the credentials. The model should aim at monetizing the claims to the verifiers. In fact, the solution would compete with forms of verification that are typically free for the credential owner, which will not be adopted if a charge is suddenly introduced. This means that successful monetisation must be on a B2B basis and ultimately be carried out in a similar way to payment networks[261]. The company ITSME offering electronic identify services in Belgium charges €3.04/user/year, in addition to set-up costs, maintenance & support fees[262]. An indicative price list of Juru API query

[258] Compared to a scheme that is only recognised nationally

[259] Refer to Annex A note on data and calculation of costs and benefits, Policy Option 2: “Technical Integration costs to the API”.

[260] https://www.skidsolutions.eu/en/services/pricelist/smart-id/

262 See https://business.itsme.be/fr/

pricing model[263], indicates prices for credentials verification going from free (for 1000 attributes) up to 0.1 euros per attribute.[264]

Benefits

Creating a trust service for the secure exchange of data linked to identity would support secure exchange of this information in the context of a wide range of private service use cases, such as customer due diligence/evidential identity information in the banking sector, allowing the possibility of reusing parts of the very costly Customer Due Diligence processes but also those cases that do not have strong requirements for customer identity verification but still require proof of attributes (e.g. age) and attestations. While the costs savings for online service providers in relying on trust service providers for credentials and attribute verification would depend on the business model adopted and the indicated fees.

Creating a trust service for the secure exchange of data linked to identity would make it possible for online service providers to:

- **cut the costs of verification and storage of attributes and attestations** (e.g. because of substitution of paper attestations by their digital equivalents);
- **reduce operating costs**. Efficiency gains for the service provider would be generated as a result of the removal of the data verification step and enhanced user/customer experience with less or no physical presence required, and the possibility to re-use existing processes. The magnitude and type of this potential benefit will differ across sectors, depending on the level of digitalisation and identification needs linked to the type of service provided. The table below indicates a upper bound and lower bound potential efficiency savings according to different parameters in four sectors.

Table 2 reduction in operating costs per sector[265]

Sector	Source of efficiency savings	Potential efficiency savings per year – Lower bound adoption [266]	Potential efficiency savings per year – Upper bound adoption [267]
Financial Services (credit institutions)	(i) More efficient customer onboarding & (ii) reduced cost of KYC/CDD compliance	€0.41 billion – €0.81 billion	€0.68 billion – €1.36 billon
eCommerce	Reduced cost of fraud prevention	€0.24 billion	€0.47 billion
eHealth	Dematerialisation of documents, more streamlined patient identification and more e-delivery	€1.26 billion	€2.51 billion

[263] Juru is a Blockchain start-up: https://www.chaineurope.org/blockchain-startups/juru/

[264] See Annex 6, Section 1.

[265] Please refer to Annex A, Policy Option 2 "Reduced costs of internal processes involving customer identity verification"

[266] As described in the paragraph introducing the tables, the range of adoption assumed is between 20% (lower bound) and 33% (upper bound) for the Financial services sector and between 5% and 10% for the other three sectors considered.

[267] As described in the paragraph introducing the tables, the range of adoption assumed is between 20% (lower bound) and 33% (upper bound) for the Financial services sector and between 5% and 10% for the other three sectors considered.

Aviation	Fewer repetitive traveller identity checks[268], reduced risk of fines and other costs from inaccurate passenger identification	€30 million	€60 million

- **increase data accuracy and trustworthiness, which reduces risk of costly errors and fraud**[269]. Using trusted eIDs would increase accuracy in establishing that the customer is who they say they are, mitigating losses from fraud, errors and fines linked to inaccurate customer identification and verification of transactions. In a recent survey, 84% percent of businesses said that the burden of fraud risk mitigation would be reduced if they were certain about the identity of a customer (42% said significantly reduced). Higher data accuracy and reliability due to the trusted input system, would result in a reduced probability of errors and fraud. Liability costs are also likely decrease as a result of clearer liability for the correctness of the data.

Table 3 - Estimated sectoral savings from reduced fraud[270]

Sector	Potential reduction in fraud losses per year - Lower bound adoption scenario[271]	Potential reduction in fraud losses per year - Upper bound adoption scenario[272]
Financial Services (credit institutions)	€0.85 billion	€1.4 billion
eHealth	€0.3 billion	€0.6 billion
Aviation	€3.5 million	€7 million
eCommerce	€0.13 billion	€0.26 billion

- **offer more personalized services**, as services providers would be able to acquire more relevant information about their users in a cost-efficient way thanks to more **effective** exchange of attributes;

5.3.1.4 Citizens and users

Costs

No costs are identitfied for citizens as part o of the implementation of measure 1 to 5. In fact the set-up, maintenance and transaction cost would normally be sustained by the service providers requesting the payment, or in this case the service provider requesting or

[268] Figures assume the proportion of passengers subject to repetitive identity checks could be reduced from the current 5% to 10%, based on IATA (2016) Document verification travel trouble https://airlines.iata.org/analysis/document-verification-travel-trouble

269 Experian. (2018). *The 2018 Global Fraud and Identity Report*

[270] Please refer to Annex A, Policy Option 2 "Estimated sectoral savings from reduced fraud"

[271] As described above, the range of adoption assumed is between 20% (lower bound) and 33% (upper bound) for the Financial services sector and between 5% and 10% for the other three sectors considered.

[272] As described above, the range of adoption assumed is between 20% (lower bound) and 33% (upper bound) for the Financial services sector and between 5% and 10% for the other three sectors considered.

relying on the qualified electronic attribute/credential. This is based on comparable business models such as those applicable to the use of payment cards in consumer transactions and for the provision of electronic identity services by private providers in European markets.

This means that normally the citizen will not pay for the service. In specific cases where the value of the credential benefits mostly the user, it may happen that the trust service provider requests a fee from the user rather than or in addition to the online service provider. This measure will contribute to make end users, in particular citizens and SMEs, feel the importance of being Europeans in particular with regard to the values and protection the EU promotes to build a European citizenship.

Benefits

The creation of attributes as a trust service will provide more possibilities for the **user to actively manage attributes, credentials and attestations** (e.g. gender, age, professional qualifications etc.), increasing user control of data related to his/her digital identity and enabling personalised online services in a trusted environment where online privacy can be ensured, and data is protected[273]. This measure would also improve trust in how attributes, credential ad attestations are handled by service providers.

Increased access to **secure and convenient digital identity authentication services for citizens** based on trustworthy digital identity attributes issued and guaranteed by Member States would also encourage greater access to services, lead to more digital identification enabled online transactions cross border and reducing the administrative burden associated with identifying digitally for access to online services and providing verifiable proofs and evidences when required either by private or public institutions saving on average 20 hours per year[274]. For citizens, administrative burden savings are estimated between 350 million and 400 million per year. Measures 1 to 5 would also support the more effective access to online public services cross border and other efforts at the European level to make the exchange of digital attributes and attestations possible[275].

Citizens will also benefit from the possibility of using digital identity credentials in legal proceedings across all Member States, preventing discrimination of credentials in electronic form. This would likely have wide-ranging positive impacts on the value and legal validity of identity credentials for cross-border transactions.

5.3.2 Measure 6 - Legal requirements to ensure the protection of personal data

5.3.2.1 Public authorities

Costs

This change may imply an increase in resources needed for supervisory duties as it requires ex-post supervision in a form to be further detailed. In addition, the incidence of such costs will change depending on whether and how the proposals regarding the governance framework are implemented. If no intervention in made on this aspect, the costs would fall on the national competent authorities; assuming 0.5 additional full-time member of staff is allocated to these supervisory activities, at the average wage costs would amount to €22,000 a year on average per Member State.

[273] European Commission. (2020). Inception impact assessment.

[274] McKinsey & Company. (2019). Digital identification: A key to inclusive growth

[275] See Article 14 of the Single Digital Gateway Regulation facilitating the cross /border exchange of proofs between public administrations in the EU

5.3.2.2 Trust service providers

Costs

QTPs or identity providers acting as credential providers, would face additional **costs** from implementing the personnel and infrastructural changes required to comply with **the data protection provisions**, although these would very much depend from the existing structure and underlying business of the provider. For those companies that are already offering digital identity services on a stand-alone basis, there would not be significant costs.

Functional separation are considerably less resource intensive that structural separation (logical data segregation). For a logical segregation of data of a medium size infrastructure it came down to around 25.000 € to 30.000 €[276]. Also non-qualified providers would be subject to this data protection measure and will have to bare the same costs to functionally separate identity data from other data.

5.3.2.3 Online service providers

A significant proportion of respondents to the Deloitte / PwC survey (41%) were positive towards measures to strengthen data protection and privacy, perceiving their benefits to be greater than their cost.

Structural separation is already in place for banks that are also identity providers. For instance, in the case of the Nordic BankID scheme, identity services have been structurally separated from other banking operations. Structural separation should not apply to data generated by the trust service provider core business essential for the provision of this new trust service, but to data collected by aggregation or through third parties.

For the provision of qualified digital identity attributes qualified trust service providers would face costs from fulling the requirement of structural separation. These costs could be comparable to the costs incurred in regulated sector such as telecom and energy requiring structural separation (physical data segregation). Based on an evidence retrieved on IT costs relating to structural separation from the broadband sector in Australia, where the move cost an estimated one-off cost of €730,000 plus a recurrent annual cost of €30,000 for operational support, business, communications and accounts.

5.3.2.4 Online service providers (platforms acting as gatekeepers)

Costs

Online platform acting as gatekeepers would have to implement functional and structural separation of their database and have to sustain the same costs described for qualified and non-qualified trust service providers (section above: 5.3.2.2). However for this organisation type there would be specific compliance obligations requiring gatekeepers to offer access and interoperability with notified eIDs.

As highlighted in the Impact Assessment for the DMA, compliance costs would be miniscule as compared to the gatekeepers revenues and could be absorbed by gatekeepers with little incentive for them to pass on costs to business users or to consumers, Indirect (other than compliance) costs may be higher, however, the impact of such changes is difficult to quantify.

[276] Based on estimates from internal confidential PwC professional activities in cybersecurity field.

Benefits

The requirement for online gatekeepers not to discriminate and be interoperable with eIDs recognised cross-border would have direct benefits for the gatekeepers themselves. They could use the notified eIDs as ready-made tools to enrol users on the basis of verified identities, to quickly validate their identity, minimise security risks and, most importantly, reinforce their GDPR compliance.

Government-issued/recognised eID means interoperable with the gatekeepers' platforms would support them to contain the proliferation of fake news, fake reviews damaging for their business and other activities aiming to mislead citizens and consumers. Eurobarometer data reports that 80% of Europeans have come across information they believe was false or misleading several times a month and 85% of the respondents perceive this as a problem in their country. Additional costs may be generated for online service providers acting as ID providers by possible provisions to strengthen data security and privacy under Option 2.

5.3.2.5 Citizens and users

Benefits

The measure would help address a key point of concern with respect to data protection and privacy in private service provision, which relates to progressive profiling and to accumulation of personal data that are neither properly anonymized, nor sufficiently verifiable and accurate. As such, it is regarded as an important component of the extension of the framework to the private sector which ensures such extension is undertaken without compromising the protection of users' data.

The benefits for citizens and end users for this sub-option would thus mainly include positive effects of a non-monetizable nature on citizens' data security and privacy.

The extent of collection and use of digital identity data is not always known nor readily ascertainable by the user, particularly when authenticating into large online platforms or mobile applications. As a result, users are not fully in control of their digital identity. In these cases the exchange of data is often contractually set out by terms of use and privacy, which can be complex and opaque and allow different privacy settings and opt-outs that are difficult to understand for the user and not very meaningful.[277] It has been estimated that a user would require 244 hours per year to read the privacy statements of all the visited websites [278]. Most importantly, the users' decision to accept these terms and conditions is less of a genuine choice when authenticating into multi-sided platforms that have a dominant position in multi-sided markets. As a result, users are not actually in control of their digital identity to the extent that is implied by these contractual agreements.[279] By requiring more transparency and imposing the separation of identity and activity data:

- further privacy-preserving safeguards can be applied specifically on identity data, for instance on the secure storage of such data

[277] International Bar Association. (2016). *Digital identity: principles on collection and use of information*

[278] A.M. McDonald and L.F. Cranor (2008), *The Cost of Reading Privacy Policies*, in

Journ. of L. & Pol. Inform. Soc., Privacy Year Revew, p. 540-565

[279] International Bar Association. (2016). *Digital identity: principles on collection and use of information*

- more clarity of interpretation can be brought to what constitutes identity data on large platforms and its relation to GDPR, strengthening the legal basis for protection of digital identity data
- user control can be enhanced through more transparent terms and conditions of use and more confidence that identity and activity data will not be linked unless they have expressly given their consent for such linkage
- the potential for unfair competition from online platforms in the ID market would be diminished, ensuring the are less able to exert undue influence on market outcomes. This would preserve user choice.

For what concerns digital identity safeguarded it is expected an increase in trust in transacting online and to a reduced likelihood of identity theft. The use of eID allows users to check the audit log of the use of their eID and authorise a revocation of the authentication certificates of the stolen document, making it unusable in the future and thus limiting the negative economic, legal and emotional consequences of the identity theft. This is a growing issue in Europe, with about one in five European citizens falling victim to fraud and scams (of which one third experienced identity theft) over the last two years . With regard to identity theft, we estimate based on EU-wide survey data that 25 million European citizens have fallen victim to ID theft over the same period. The same survey suggests that in 2% of cases, citizens incurred a financial loss above €500. Taking this lower bound estimate, measure 2.6 could help protect nearly 250,000 European citizens a year from ID theft and reduce the related financial losses by at least €125 million if it resulted in a halving of the percentage of citizens exposed to ID theft-related financial losses.

Greater trustworthy and secure exchange of digital identity attributes will also increase **data security for IoT devices** which are increasingly part of EU citizens and consumers in the digital space. In 2021, the market will increase to nearly 11.6 billion IoT devices; by 2025 it is estimated that there will be more than to 21 billion IoT devices[280]. Trust Services can intervene at a first level to certify the identity of the interconnected objects, guaranteeing their reliability from a technological point of view and providing additional security safeguards on the data provided by end users. These measures are necessary considering that attacks on IoT devices increased by more than 300% in the first half of 2019 and the risk of IoT devices being used as intermediaries is expected to increase[281].

Summary of main costs and benefits for Policy Option 2

280 Norton. (2020). *The future of IoT: 10 predictions about the Internet of Things*

281 Collard, A. (2019). *Large-Scale IoT Attack Coming*. Gadget. 6 December 2019. https://gadget.co.za/large-scale-iot-attack-coming/

Policy option 2 – summary of main costs and benefits		
Measure	**Cost**	**Related policy options**
Measure 1.1: Establish an obligation for Member States to offer eIDs and to notify them under eIDAS	Compliance with eIDAS related obligation - €9.7 million for public authorities (envisaged only for 13 Member States)	1, 2, 3
	Increased administrative burden due to mandatory notification - €0.52 - €1.3 million for public authorities (envisaged only for 13 Member States)	1, 2, 3
	Increased administrative burden due to additional peer reviews - €1.2 million for public authorities (in the next two years, cumulative for all Member States)	1, 2, 3
Measure 2.1: creating a new qualified trust service for the secure exchange of data linked to identity	Familiarisation with new procedures and standards - €315,000 for public authorities (one-off) Enforcement and administrative costs due to the introduction of new trust services - €8 million for public authorities per year (recurrent costs) Cross-border cooperation activities on trust services - €25,000 to €90,000 for public authorities	2,3
	Compliance costs linked to the introduction of a new qualified trust service - €545,000 per each trust Service Provider (one-off) Compliance costs linked to the introduction of a new qualified trust service - €255,000 per each trust Service Provider (recurrent costs)	2,3
	Familiarisation with new procedures and standards - €339,000 for Conformity Assessment Bodies	2,3
Measure 2.2: require MS to make available data stored in authentic sources for the secure exchange of data linked to identity.	€625 million for public authorities for accessing authentic sources (one-off) €162 million per year for public authorities related to certification (recurrent costs) €18,000 to €27,000 related to integration cost per each online service provider	2,3
Measure 1.2: Establish a requirement for Member States to allow private online service providers across the EU to rely on notified eIDs	Infrastructural cost to connect to an eIDAS €42,000 per each online service provider	1, 2
Measure 1.3: Establish a harmonised cost-model and liability rules to facilitate private online service providers to rely on notified eIDs	Upgrading eIDAS nodes infrastructure - € 6,1 million for public authorities	1, 2
Measure 1.4: Extend the person identification data recognised cross border	Committee work needed for standardisation - €300,000 for public authorities	1, 2, 3
Measure 2.3: setting security requirements and common technical standards for the secure exchange of data linked to identity	Committee work needed for setting technical requirements and standards - €1 to €2 million – for public authorities	2,3
Measure 2.4: define the legal effect of digital identity credentials	Costs for amending the eIDAS regulation in order to modify existing provisions and/or include new ones, for public authorities	2,3
Measure 2.5: regulated sectors such as energy or finance and the Public Sector would be required to rely on Qualified digital credentials		2,3
Measure 1.5: Strengthen security requirements for mutual recognition	Compliance costs due to certification - €228,000 for public authorities	1, 2, 3
Measure 2.6: legal requirements to ensure the protection of personal data	Technical costs related to functional separation of €25.000 to €30.000 per each Trust Service provider	2,3
	Technical costs related to structural separation of €730,000 (one-off) and €30,000 per year (recurrent) per Qualified trust service providers	2,3
Measure 1.6: Introducing new Trust Services	Compliance costs linked to the introduction of a new qualified trust service - €545,000 per each trust Service Provider (one-off)	1, 2, 3

	Compliance costs linked to the introduction of a new qualified trust service - €255,000 per each trust Service Provider (recurrent costs)	
Measure 1.7: Harmonise the certification process for remote electronic signing	Costs related to compliance with new certification process for Trust Service Providers	1, 2, 3
Measure 1.8: Strengthening the Recognition of QWACs (Qualified Website Authentication Certificates)	Awareness raising campaign - €200,000 to €400,000 for public authorities QWACs-related compliance costs - €550 per year, per each online service provider	1, 2, 3
Measure	**Benefit**	**Related policy options**
Measure 1.1: Establish an obligation for Member States to offer eIDs and to notify them under eIDAS	Enhanced digital inclusion for citizens / end-users	1, 2, 3
	Increased personal data protection and online security for citizens / end-users	1, 2, 3
	Increased access to public services through secure eIDs for citizens / end-users	1, 2, 3
Measure 2.1: creating a new qualified trust service for the secure exchange of data linked to identity	Cost savings due to reduced operational expenditures in identification procedures • €0.68 billion to €1.36 billion - for online service providers in the financial services sector per year • €1.26 billion to €2.51 billion - for online service providers in the eHealth sector per year • € 30 million to €60 million - for online service providers in the aviation sector per year • €0,24 billion to €0.47 billion - for online service providers in the eCommerce sector per year	2,3
	Cost savings due to reduced expenditures or damages related to cybercrimes • €0.85 billion to €1.4 billion - for online service providers in the financial services sector per year • €0.3 billion to €0.6 billion - for online service providers in the eHealth sector per year • € 3.5 million to €7 million - for online service providers in the aviation sector per year • €0.13 billion to €0.26 billion - for online service providers in the eCommerce sector per year	2,3
	Increased business opportunities for trust service providers	2,3
	Cost savings - €350 to €400 million per year - from reduced administrative burden for citizens / end-users	2,3
Measure 2.2: require member states to make available data stored in authentic sources for the secure exchange of data linked to identity	Cost savings from reduced administrative burden and increased cross-border data exchange for public authorities	2,3
Measure 1.2: Establish a requirement for Member States to allow private online service providers across the EU to rely on notified eIDs	Costs savings in operating expenses up to 25% per year for online service providers	1, 2
Measure 1.3: Establish a harmonised cost-model and liability rules to facilitate private online service providers to rely on notified eIDs	Increase revenues from increased online transactions through eIDAS nodes - €17 million to €2,5 billion – for public authorities in the next 5 years	1, 2
Measure 1.4: Extend the person identification data recognised cross border	Increased personal data protection and online security for citizens / end-users	1, 2, 3
Measure 2.3: setting security requirements and common technical standards for the secure exchange of data linked to identity	Enhanced harmonization in the trust service market for Trust Service providers Increased security in the exchange of cross-border data for online service providers	2,3
Measure 2.4: define the legal effect of digital identity credentials	Increased recognition of digital identity credentials for accessing public and private services in different Member States for citizens /end-users	2,3

	Reduction in the costs of verification and storage of attributes and attestations for online service providers Increased legal certainty for Trust Service Providers	
Measure 2.5: regulated sectors such as energy or finance and the Public Sector would be required to rely on Qualified digital credentials	-	2,3
Measure 1.5: Strengthen security requirements for mutual recognition	Savings in compliance costs for public authorities	1, 2, 3
	Savings in compliance costs (related to security certifications, GDPR requirements) - €12,000 to €24,000 - for eID providers	1, 2, 3
	Increased personal data protection and online security for citizens / end-users	1, 2, 3
Measure 2.6: legal requirements to ensure the protection of personal data	Increased personal data protection and online security for citizens / end-users	2,3
Measure 1.6: Introducing new Trust Services	Increased revenues due to the introduction of eArchiving - €37 million a year for every additional 1% of businesses purchasing an eArchiving solution - for Trust Service Providers.	1, 2, 3
	Enhanced offer in the Trust Services market for citizens / end-users	1, 2, 3
Measure 1.7: Harmonise the certification process for remote electronic signing	Increased competition and security of trust services and acceptance of mobile trust services for citizens / end-users	1, 2, 3
Measure 1.8: Strengthening the Recognition of QWACs (Qualified Website Authentication Certificates)	Cost savings from reduced damages related to cybercrimes for citizens / end-users	1, 2, 3
	Increased personal data protection and online security for citizens / end-users	1, 2, 3

5.4 Option 3 – Personal digital identity wallet

Option 3 aims to define a legal and technical framework for the deployment of the European Digital Identity as a user-controlled digital Wallet App.

Two possibilities are considered for the deployment of the wallet[282]:

- **Sub-option 3.1:** deployment by private qualified trust service providers under eIDAS,
- **Sub-option 3.2:** deployment governments as an extension to notified eID solutions

Further, each specific measure is clustered according to different objectives of the review and the sub-options that they support.

The measures to provide **access to trusted and secure digital identities for all citizens and businesses cross borders** are as follows:

- **Measure 3.1 (sub-option 1):** creating a new qualified trust service for the provision of a user-controlled secure European Digital Identity Wallet App
- **Measure 3.1 (sub-option 2):** Mandatory extension of notified eID schemes, or mandatory provision of a user-controlled secure European Digital Identity WalletApp by Member States

Option 3 further sets out measures to make accessible a wide range of public and private online services relying on trusted and secure digital identity solutions cross border (which are applicable to all sub-options). These are:

- **Measure 2 (all sub-options):** Defining common standards for a European Digital Identity Wallet app
- **Measure 3 (all sub-options):** (Introducing) Security requirements

The costs and benefits affecting different stakeholder groups are considered together for all sub-options under option 3; comments on the specific impacts of different sub-options are included wherever necessary to highlight differences. Equally, since the measures under option 3 are mutually dependent (i.e. none can be sensibly implemented in isolation from others) we also include for all sub-options a combined assessment for all three measures.

5.4.1 Measure 3.1(All sub-options)

5.4.1.1 Online service providers

Costs

Costs will depend on the business model (see below under impacts on Wallet providers). In the commonly used business model, the costs are borne by the service provider / relying party.

As mentioned for Option 2, IT integration costs will be necessary to have a new system of verified credentials and they will vary. Relying parties need to upgrade their portals and carry out adjustments to have a new system of verified credentials and attestations. Integration costs through an API limited to enabling a new way of authenticating are expected to be from €18,000 to €27,000. The initial cost will vary depending on the level of integration sought, the specific use case and the number of standard components that can

[282] A third possibility, Sub-option 3.3: the Commission (directly, via an existing agency or through procurement), has been discarded at an early stage (see relevant section)

be used. The availability of CEF building blocks in this case is expected to help reduce the costs of initial integration for online service providers.

In scenarios where service providers consume identity attributes on the spot from the user's mobile device screen (by verifying the authenticity of the credential through a QR code, barcode, NFC etc), service providers may need to acquire devices such as mobile phones, tablets etc to be able to verify the authenticity of the presented credential.

Benefits

The economic benefits for online service providers relying parties of the EU eID system depend on the economic model that shall be adopted. In the most commonly used business model today, the costs are borne by the service provider / relying party. Potential benefits include:

- **Costs savings related to credentials issuance/verification:** Where governments offer secure eID-s for use also in the private sector, it can be regarded as a public service and therefore allowing for substantial cost savings compared to Member States where the private sector has to cover the cost for themselves. McKinsey forecasts the ID verification as a service market size to be 16-20 billion globally by 2022.[283] Later customer interactions cost on average 4$ for a branch visit and 0,1$ for an online interaction[284]. Belgian itsme and Estonian Mobiil-ID price lists confirm similar numbers[285]. The European Digital Identity WalletApp would have to be competitive in this regard, either in terms of price, coverage among potential customers and ease in onboarding in order to generate substantial cost savings. The Wallet App provider's sales and marketing savvy is therefore a critical component of the success of option 3.
- **Better customer experience.** There is evidence suggesting that eID solutions that streamline online interactions between users and service providers would promote customer acquisition and retention. For instance, in the eCommerce sector it is documented that on average there is around 69% abandonment rate[286] when users get to the online shopping cart. Twenty-eight per cent of respondents mentioned as the second most important reason for dropping out the fact that the site requests them to use a specific account. Equally, in the financial sector, institutions face very high abandonment rates in their customer onboarding processes - 63% according to recent research, with over a quarter of customers that find them difficult or longer than expected[287].
- **Reduced costs due to fraud** can be another type of benefit for some service providers. Accurately establishing the customers to be who they say they are, mitigates losses from fraud, errors and fines linked to inaccurate customer identification and verification of transactions, if high level of assurance eID schemes are not yet used by the organizations. Moreover, identity theft is rapidly expanding, causing substantial financial loss to millions of people all around the world. This invisible crime is also widespread across the European countries, where the growing number of consumers is targeted by sophisticated fraudulent scams each year, both

[283] https://s3.amazonaws.com/fgt-c39f079198f6-prod-cms-media/wp-content/uploads/2019/03/20033501/The-Next-20-Billion-Digital-Market.pdf

[284] https://www.fintechfutures.com/files/2018/10/Backbase_The-ROI-of-Omni-channel_Whitepaper-2.pdf

[285] https://www.skidsolutions.eu/en/services/pricelist/mobile-id-service/, https://partner-support.itsme.be/hc/en-us/articles/360051689714-How-much-does-itsme-cost-

[286] This value is an average calculated based on these 41 different studies containing statistics on e-commerce shopping cart abandonment: https://baymard.com/lists/cart-abandonment-rate

[287] Signicat.2020. The Battle to Onboard 2020: The impact of COVID-19 and beyond https://resources.signicat.com/hubfs/Downloads/signicat_battle_to_onboard_2020.pdf?hsLang=en

offline and online. According to data gathered by Finanso.se, 56% of Europeans have experienced at least one type of fraud in the last two years. One-third of them became victims of identity theft, making it the second most-common type of fraud in Europe. The savings from reduced fraud could be substantial in a range of sectors requiring customer identification (see Option 2).

Overall, in Member States where eIDs are ubiquitous (e.g. Scandinavia, Baltic countries, Benelux), these benefits have been to an extent already realized thanks in part to existing eID means. The main value proposition of European Digital Identity wallet App lies where identity proofing and access management markets are not mature yet. According to Deloitte's 2020 digital banking maturity study, only 34% of banks offer fully digital account opening and 23% offer remote identification and verification. There is a substantial gap between the champions and latecomers for both opening a bank account through the mobile channel (55% vs 5%) and internet channel (58% vs 20%)[288]. The situation is similar with governments: more than 90% of citizens submitted forms to government online (a process that typically requires user identification and authentication) while for two countries the number is less than 40%[289].

5.4.1.2 Citizens/End Users

Benefits

Data from countries where digitalisation is most advanced suggests an increase in use-cases and market demand for trusted and secure digital identification. For example in Norway, BankID offers a trusted personal wallet space to manage e.g. a patient journal, vaccinations, doctor appointments, e-prescriptions, secure messages etc. the important uptake of BankID on high level of assurance (90% +[290]) has made it possible to provide digital e-Health services for almost all citizens.

The expected benefits for users of an EU eID Wallet App would be substantial in terms of the convenience and user-friendliness of the authenticating interface, because of the ease with which they would be able to manage their identity through the secure wallet on their mobile device (through the EU eID app) as well as desktop.[291] This "mobile first" design is likely to help create a consistent user experience and support accessibility. The EU eID Wallet App will deliver similar user experiences for end-users to e.g. Apple or Google Wallets, allowing e.g. for a visual representation of credentials. Connections may also be possible, to support additional use cases connecting physical and digital.

The measure also takes a more explicit privacy-by-design approach that could yield additional benefits in terms of data protection and privacy. The model proposed under this measure would reduce the need for intermediaries in the process, enabling the citizen to communicate directly with the service and credential providers.

Finally, some added value will likely be created for citizens and end users in terms of simplification of identity management, as the European Digital Identity Wallet would enable citizens to manage their own different identities and all associated credentials that they receive from various sources (e.g. education, employment, municipality, state, professional associations, leisure, etc.) anywhere in the EU.

Additionally, a universally issued EU eID to all European citizens based on a secure wallet trusted app, (provided upon citizens' request), could be expected to increase data security

[288] https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/financial-services/ce-digital-banking-maturity-2020.pdf

[289] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=67084

[290] CEPS. 2017. Europe's Digital Identification opportunity

[291] CEF eID SMO (July 2018) - Looking ahead - The user experience of eIDAS-based eID

and reduce the likelihood of identity theft, as the app's SSI functional design and strict requirements on security for providers would enable more secure sharing of the data than through other identity management systems, and the data architecture would make use of the secure element. Existing private sector solutions, including by online platforms cannot offer this. In addition, the possibility to protect personal data through a user-controlled privacy by design concept and impartiality towards service providers are advantages that are unique on the market.

The Wallet is likely to be made available free of charge (certainly under Sub-Option 2) although users might be charged for obtaining identity credentials in specific cases. Depending on market uptake and Government funding, having the wallet provided by multiple private providers (sub-Option 1) might result in reduced costs for the user and/or improved service due to competition between the providers. These aspects are covered under Option 2.

5.4.1.3 Conformity Assessment bodies

Costs

Assuming that (i) each conformity assessment body employs only one person to learn the administrative processes and this person is able to pass this on to colleagues, costs associated to familiarisation of the requirements related to the new trust service are estimated to be approximately €339,000 (around €12,000 per conformity assessment body). In any case these costs will be rolled over to Wallet Providers.

Benefits

Benefits: Similar to option 2, the benefit for conformity assessment bodies under sub-options 3.1 and 3.2 is more revenue opportunities. Member States may assess the conformity of their wallets with conformity assessment bodies in order to achieve greater conformity of implementation of standards. The number of wallets to be assessed by CABs is expected to be similar under the two sub-options.

5.4.1.4 Wallet App providers

Costs

Estimates for the key costs related to developing, launching and maintaining the Wallet App are provided below, broken down by the key features and activities that must be addressed for the implementation of the initiative.

Development and Maintenance Costs

The assessment by the European Commission included in Annex A could be the basis for a rough estimate.

To ensure continuity of operations, it is estimated that a permanent staff of 25-30 full-time employees will be needed (for any area of operation, at least 5 employees are required). The start of operations will require more investments into tools and system components, like test suites, app developments and the system test environment, while maintenance is of course lower.

In total about 10 m € could be assumed for the two years 2021/23. This cost has been estimated by the Commission on the basis of available data as a rough estimate for the first-time development of such an app. If developed libraries were provided to other wallet providers, their development and maintenance cost could be reduced. The budget for the DE Optimos 2.0 project that also included the development of a secure wallet was €5M.

In terms of providing readiness to deal with incidents and offer customer support, tasks related to help desks for end-users as well as ID providers and service providers and maintaining the security and functionality of the App are already considered in the table attached in annex 6, section 5. As reported there, service desk costs are estimated at €77,500 at the specification stage and € 310,000 at the roll-out and maintenance stages (with the latter representing a recurrent annual cost), while incident response will require an investment of € 310,000 at the roll-out stage and €155,000 per year for maintenance . Procuring an app from the private sector may offer substantial savings as the average cost to develop an app is reportedly below 100,000$, varying between around $40,000 and up to 500,000$ or higher, depending on features, complexity, UX etc. Nevertheless, there is still a need to maintain an organisation behind the app to maintain and further develop it as well as staff to work on business development, helpdesk, marketing and other functions.

In case the European Digital Identity WalletApp is secured by means of a SIM card, it would imply to sign agreements with relevant mobile network operators, which can be a substantial administrative undertaking, because of the need to organise legal, organisational and technical relationships with telecom companies. Developing a mobile application for each platform (Google Play Store, Apple App Store, Microsoft Store, Huawei AppGallery, other) can also mean considerable cost.

Certification Costs

The costs of possible certification of the WalletApp would be similar to currently incurred by trust service providers under eIDAS. As presented under other options, these consist of:

- One-off costs of initial qualified status. Estimates for these costs varied significantly among the stakeholders consulted, due in part to the size of the provider, sector and number of services offered. The average administrative costs linked to qualification are €545,000[292].
- Recurrent compliance costs. Stakeholder estimates for these costs were also wide-ranging, with figures suggesting annual costs are on average €255,000[293].

Security Costs

To secure the European Digital Identity WalletApp three conditions must be fulfilled:

- the mobile phone of the user must contain a so-called secure element (SE) for the secure storage of cryptographic codes. This secure element can either be an embedded hardware element in the device or a SIM-card (e-SIM, EUICC).
- this secure element must be accessible by the provider of the European Digital Identity WalletApp. In the case of embedded SE, the provider would have to request mobile device manufacturers/all relevant mobile network operators to provide access to the SE or eSIM, which can be difficult to obtain. Given the market potential and expected benefits/synergies with applications deployed by manufacturers it is likely that it can be achieved at little cost to the parties involved, which could be expected to be similar to the cost of negotiating a mid-complexity contract (see estimates above). However, some restraints were identitfied by interviewees. Apple, for instance, sells security solutions based on the SE to companies so some

[292] This is the average cost of administrative expenses linked to achieving and maintaining the qualified status reported by respondents to the survey of TSPs conducted for the evaluation. The figure is based on 16 data points from QTSPs that are large private organisations, public organisations and micro-enterprises or SMEs.

[293] This is the average annual cost of administrative expenses linked to compliance with eIDAS reported by QTSPS responding to the survey of TSPs conducted for the evaluation of eIDAS. The figure is based on 12 data points from QTSPs that are large private organisations, public organisations and micro-enterprises or SMEs.

resistance is expected if the two parties cannot come to a mutually advantageous agreement.

- standards for the secure operation of the SE and the WalletApp must be available.

The development and evaluation of an open SE-based ecosystem from scratch requires a substantial project organization that includes partners from all relevant areas.

Currently, about a third of mobile devices feature each of the SE options. Availability of devices with an eSIM is currently limited to high-end models, though their availability is expected to increase substantially in the medium term. Stakeholder interviews carried out by the Commission indicated that it can be expected that at least one of the required technical features will be supported by most mobile phones. (See overview in Annex 6, section 6)

Ongoing standardisation work is likely to speed up the development of this market. Of special interest is draft the ISO 23220 “Card and security devices for personal identification – Building blocks for identity management on mobile devices”, because of active involvement by (amongst others) American and global market players. GSMA is also working on a standard on Secure Applications for Mobile (SAM).

With the availability of these standards in the course of 2021/2022, it is likely that conditions 2 and 3 above will be fulfilled in the short / medium term. Once industry standards for the access and communication of a secure element in the identity environment are available it is likely that the associated hardware will be made accessible by all device manufacturers.

Onboarding Costs

To make the Wallet app usable the provider would need to have an active role in onboarding both credential providers and service providers to the ecosystem. There are over 11,000 identity providers in the public sector and about 13,400 in the private sector with the number of service providers being similar. To enable users to request identity credentials through the App, the App provider may agree with credential providers described in options 1 and 2 to build the necessary integrations and agree terms. Where Wallet App providers support provisioning of multiple kinds of identity credentials to a variety of service providers, it may be expected of it to facilitate billing between credential and service providers.

Marketing and Customer Support Costs

Even though the wallet will be used by end-users, its success depends on the uptake of service providers, which can help substantially with marketing and awareness raising. Due to the high requirements on security, the provider would need to maintain readiness to deal with incidents and offer customer support for credential providers, service providers and end-users (the estimated costs of which have been previously discussed and reported in full in the table in Annex A).

Benefits

Personal Wallets are developed by more and more ID providers from the public and the private sectors. In recent years, a number of banks have started to provide Wallet Apps, such as Rabobank in NL and Sparkassen in DE while there are also open Wallet Apps such as mTasku in EE or the Optimos 2.0 project in DE.

The business model for the wallet will depend on the sub-option for deployment chosen. While the business model would not be fully prescribed by the Regulation, under all sub-options the App provider would seek to cover costs by billing online service providers relying on the digital identity services and/or providers of digital identity services (trust services providers in Option 2).

Based on existing business models, it is unlikely that consumers would directly pay for the app. Considering a very rough cost of between €5 million and €8,3 million to get the Wallet App off the ground and a 0,1 eurocents revenue per transaction, roughly between 50 and 83 million transactions would be needed to cover the development and roll-out costs in one year.

For reference, BankID (7,9M users) was used 3,3bn times in Sweden in 2018 and Smart-ID (2,9M users) was used over 65M times in the Baltic countries in December 2020 . Under sub-option 2 and 3, part of the costs may be covered from public funds, but making revenue from provisioning of the wallet may be limited, depending on national approaches. Member States and the Commission would most likely hire contractors to develop the App and related solutions, potentially through a governmental/EU agency.

Existing Identity Providers that issue digital identity means to their users (such as governments, financial institutions, telcos etc.) may find developing of a European Digital Identity Wallet App (on their own or on behalf of governments depending on the Sub-Option) a financially sustainable alternative to existing means, especially if it offers revenue opportunities. In addition, mobile phone manufacturers (such as Apple, Samsung, Google, Huawei, Oppo etc.), app developers and Secure Element providers may find business opportunities in developing an European Digital Identity Wallet App or updating existing ones to meet security requirements.

European Digital Identity Wallet App providers may have an advantage compared to existing digital identity means providers although they can also act as platforms for the provision of their services. For chip manufacturers there are opportunities related to the likely increase in sales for secure elements (SE), general market development will also depend on the identification of devices.

5.4.1.5 Public authorities

Costs

The introduction of a framework for a European Self-sovereign digital identity scheme based on the issuance of verified electronic credentials is expected to create significant costs for the app provider (deriving from the development of the app and coordination structure and for the Commission and national competent authorities due to the need to set up new selection and supervision mechanisms for Wallet App providers. These are:

- **Cost of additional supervision activities**. If the first deployment option was chosen, the development of the legal framework would require resources to cover additional supervision activities as mentioned in Option 1 and 2. This would be needed to cover supervision for public/private Wallet App providers. Assuming that this would require the national competent authorities to allocate 1 FTE additional staff time at the average labour cost to cover these needs, the cost of additional supervision would be around €1.1 million per year across the EU (an average €44,000 a year per Supervisory Body).
- **Familiarisation costs.** For this sub-option, the cost of familiarisation is similar to the one reported for other options.

5.4.1.6 Trust Service providers

Costs

Regardless of the organisation providing the wallet, the costs for providers of identity credentials will vary depending on how the providers will adjust their business model and service offer, as their ability to increase volume of transactions and develop new services

may at least compensate for any loss of revenue linked to the need to share fees with the Wallet providers.

Benefits

As for Option 2, an EUeID Wallet will increase the economic feasibility of market opportunities for potentially all types of digital identity providers as they will have a platform giving them access to an increased number of users on both sides of the market (citizens and online service providers). Further market opportunities may stem from the incentive to design new services connected to the Wallet App. Specific areas where new services may emerge include identification and authentication of non-human entities: IDC estimates that there will be 41.6 billion connected IoT devices, generating 79.4 zettabytes (ZB) of data in 2025 . The time and costs of onboarding devices is seen today as a market barrier. The initiative would likely encourage providers to fill this market gap and invest in developing innovative services in this area.

5.4.2 Measure 3.2: Defining Common Standards for a European Digital Identity Wallet App

5.4.2.1 Public authorities

Costs

The development of a standardised SE-based ecosystem from scratch requires a substantial project organization that includes partners from all relevant areas. In order to set common standards, public authorities will face costs related to international cooperation activities which are estimated to be similar to those explained for Option 2 Measure 3, (namely an overall costs ranging between €1-2 million). However, also in this context, existing relevant standards and ongoing international standardization activities may significantly reduce the amount of effort needed.

5.4.2.2 Wallet app providers

Depending on the standards and technical requirements adopted, Wallet App providers are expected to face compliance costs. These are difficult to quantify before the definition of the above-mentioned technical requirements, but it could be reasonably assumed that would be mainly associated to ensuring a SE-based solution.

Ongoing standardisation work is likely to speed up the development of the SE market, as demonstrated by the global work on the ISO 23220 “Card and security devices for personal identification – Building blocks for identity management on mobile devices”.

Once industry standards for the access and communication of a secure element in the identity environment are available it is likely that the associated hardware will be made accessible by all device manufacturers.

Benefits

Wallet App providers would benefit from a harmonized level-playing field, without incurring in national legislative barriers. This could also ensure interoperability and an effective cross-border market for the App, positively affecting the Digital Single Market.

5.4.2.3 Citizens / end-users

Benefits

The definition of common development ad security standards with regards to the EU Digital Identity Wallet App will positively affect citizens and end-users as they could benefit from

a consistent user-experience and transparency about security requirements and functionalities included in the Wallet App, regardless of the provider.

5.4.3 Measure 3.3 (all sub-options): Security requirements

5.4.3.1 Wallet app providers

Costs

Since the measure consists in the introduction of a targeted certification scheme developed under the Cybersecurity Act[294], its costs would be similar to measure 6 under Option 1, which also envisages the introduction of EU-wide ICT security certification for eID means under the same act. The main costs would therefore stem from the need to get certified under the new scheme (also in the order of 80/100K€) which in this case would fall on Wallet App providers.

Benefits

The benefits of this measure would also match those reported for measure 6 under option 1. Firstly, by strengthening the security of the Wallet App and introducing more transparent criteria, certification would increase citizens/end users' trust in using the Wallet App. Secondly, despite the initial net cost of getting certified falling on the Wallet App providers, in the longer term the measure would prove an efficient way for providers to demonstrate compliance, as a clear and common assessment methodology and criteria would reduce the risks of delays in the process and unharmonized interpretation of security requirements across Member States.

5.4.3.2 Online service providers (platforms acting as gatekeepers)

Costs

This measure would create similar costs as Measure 1 under the option 0, as it would extent the same obligation envisaged there to the European Digital Wallet App. Consequently, the main costs would be the compliance costs borne by the gatekeepers to enable users to use the Wallet App for identification/authentication into their services, which is expected to be immaterial as a proportion of platforms' revenues and unlikely to be passed on to consumers.

Benefits

The gatekeepers would benefit from this measure as the Wallet App provides a ready-made tool to identify and authenticate customers securely and on the basis of a verified identity, facilitating security risk and reputational risk management as well as legal compliance (e.g. with GDPR and consumer protection legislation).

5.4.3.3 Public authorities

Costs

Some limited costs may also arise for public authorities to cover supervision of gatekeepers.

5.4.3.4 Citizens / end-users

Benefits

[294] REGULATION (EU) 2019/881 introduces a European cybersecurity certification scheme. Art 54(3) provides: "Where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act."

As for Measure 1 under option 0, the main beneficiaries of this measure would be citizens and end users (including companies). These would be enabled to use the Wallet App for accessing a wide range of popular services offered by the platforms, with clear benefits on their ability to identify and authenticate securely online compared with the current scenario, where they are often forced to use platforms' solutions that offer a lower level of assurance. Their awareness of the importance of security online would also be enhanced through regular use of a highly secure eID means.

Summary of main costs and benefits for Policy Option 3

Policy option 3 – summary of main costs and benefits		
Measure	**Cost**	**Related policy options**
Measure 1.1: Establish an obligation for Member States to offer eIDs and to notify them under eIDAS	Compliance with eIDAS related obligation - €9.7 million for public authorities (envisaged only for 13 Member States)	1, 2, 3
	Increased administrative burden due to mandatory notification - €0.52 - €1.3 million for public authorities (envisaged only for 13 Member States)	1, 2, 3
	Increased administrative burden due to additional peer reviews - €1.2 million for public authorities (in the next two years, cumulative for all Member States)	1, 2, 3
Measure 2.1: creating a new qualified trust service for the secure exchange of data linked to identity	Familiarisation with new procedures and standards - €315,000 for public authorities (one-off) Enforcement and administrative costs due to the introduction of new trust services - €8 million for public authorities per year (recurrent costs) Cross-border cooperation activities on trust services - €25,000 to €90,000 for public authorities	2,3
	Compliance costs linked to the introduction of a new qualified trust service - €545,000 per each trust Service Provider (one-off) Compliance costs linked to the introduction of a new qualified trust service - €255,000 per each trust Service Provider (recurrent costs)	2,3
	Familiarisation with new procedures and standards - €339,000 for Conformity Assessment Bodies	2,3
Measure 2.2: require member states to make available data stored in authentic sources for the secure exchange of data linked to identity	€625 million for public authorities for accessing authentic sources (one-off) €162 million per year for public authorities related to certification (recurrent costs) €18,000 to €27,000 related to integration cost per each online service provider	2,3
Measure 3.1 (sub-option 1): creating a new qualified trust service for the provision of a user-controlled secure European Digital Identity Wallet App	Costs of €339,000 linked to familiarisation with Wallet App conformity assessment procedures for Conformity Assessment Bodies Qualification costs of €545,000 (one-off) and €255,000 per year (recurrent) for Trust Wallet app providers Additional operational and marketing costs for Wallet app providers (not possible to quantify) Costs of onboarding both credential providers and service providers to the ecosystem. (not possible to quantify)	3
Measure 3.1 (sub-option 2): Mandatory extension of notified eID schemes, or mandatory provision of a user-controlled secure European Digital Identity WalletApp by Member States	-	3
Measure 1.4: Extend the person identification data recognised cross border	Committee work needed for standardisation - €300,000 for public authorities	1, 2, 3
Measure 2.3: setting security requirements and common technical standards for the secure exchange of data linked to identity	Committee work needed for setting technical requirements and standards - €1 to €2 million – for public authorities	2,3

Measure 2.4: define the legal effect of digital identity credentials	Costs for amending the eIDAS regulation in order to modify existing provisions and/or include new ones, for public authorities	2,3
Measure 2.5: regulated sectors such as energy or finance and the Public Sector would be required to rely on Qualified digital credentials		2,3
Measure 3.2 (all sub-options): Defining common standards for a European Digital Identity Wallet app	Committee work needed for setting technical requirements and standards - €1 to €2 million – for public authorities Compliance costs for Wallet app providers-	3
Measure 3.3 (all sub-options): (Introducing) Security requirements	Compliance costs with the new certification – €80,000 to €100,000 -for Wallet app providers	3
Measure 1.5: Strengthen security requirements for mutual recognition	Compliance costs due to certification - €228,000 for public authorities	1, 2, 3
Measure 2.6: legal requirements to ensure the protection of personal data	Technical costs related to functional separation of €25.000 to €30.000 per each Trust Service provider	2,3
	Technical costs related to structural separation of €730,000 (one-off) and €30,000 per year (recurrent) per Qualified trust service providers	2,3
Measure 167: Introducing new Trust Services	Compliance costs linked to the introduction of a new qualified trust service - €545,000 per each trust Service Provider (one-off) Compliance costs linked to the introduction of a new qualified trust service - €255,000 per each trust Service Provider (recurrent costs)	1, 2, 3
Measure 1.7: Harmonise the certification process for remote electronic signing	Costs related to compliance with new certification process for Trust Service Providers	1, 2, 3
Measure 1.8: Strengthening the Recognition of QWACs (Qualified Website Authentication Certificates)	Awareness raising campaign - €200,000 to €400,000 for public authorities QWACs-related compliance costs - €550 per year, per each online service provider	1, 2, 3
Measure	**Benefit**	**Related Policy options**
Measure 1.1: Establish an obligation for Member States to offer eIDs and to notify them under eIDAS	Enhanced digital inclusion for citizens / end-users	1, 2, 3
	Increased personal data protection and online security for citizens / end-users	1, 2, 3
	Increased access to public services through secure eIDs for citizens / end-users	1, 2, 3
Measure 2.1: creating a new qualified trust service for the secure exchange of data linked to identity	Cost savings due to reduced operational expenditures in identification procedures • €0.68 billion to €1.36 billion - for online service providers in the financial services sector per year • €1.26 billion to €2.51 billion - for online service providers in the eHealth sector per year • € 30 million to €60 million - for online service providers in the aviation sector per year €0,24 billion to €0.47 billion - for online service providers in the eCommerce sector per year	2,3
	Cost savings due to reduced expenditures or damages related to cybercrimes • €0.85 billion to €1.4 billion - for online service providers in the financial services sector per year • €0.3 billion to €0.6 billion - for online service providers in the eHealth sector per year • € 3.5 million to €7 million - for online service providers in the aviation sector per year €0.13 billion to €0.26 billion - for online service providers in the eCommerce sector per year	2,3

	Increased business opportunities for trust service providers	2,3
	Cost savings - €350 to €400 million per year - from reduced administrative burden for citizens / end-users	2,3
Measure 2.2: require member states to make available data stored in authentic sources for the secure exchange of data linked to identity	Cost savings from reduced administrative burden and increased cross-border data exchange for public authorities	2,3
Measure 3.1 (sub-option 1): creating a new qualified trust service for the provision of a user-controlled secure European Digital Identity Wallet App	Increased business opportunities for Wallet app providers	3
	Increased personal data protection and online security for citizens / end-users	3
	Increased access to public services for eID providers and citizens / end-users	3
Measure 3.1 (sub-option 2): Mandatory extension of notified eID schemes, or mandatory provision of a user-controlled secure European Digital Identity WalletApp by Member States		3
Measure 1.4: Extend the person identification data recognised cross border	Increased personal data protection and online security for citizens / end-users	1, 2, 3
Measure 2.3: setting security requirements and common technical standards for the secure exchange of data linked to identity	Enhanced harmonization in the trust service market for Trust Service providers Increased security in the exchange of cross-border data for online service providers-	2,3
Measure 2.4: define the legal effect of digital identity credentials	Increased recognition of digital identity credentials for accessing public and private services in different Member States for citizens /end-users Reduction in the costs of verification and storage of attributes and attestations for online service providers Increased legal certainty for Trust Service Providers-	2,3
Measure 2.5: regulated sectors such as energy or finance and the public sector would be required to rely on qualified digital credentials	-	2,3
Measure 3.2 (all sub-options): Defining common standards for a European Digital Identity Wallet app	More consistent user experience and transparency about security requirements and functionalities for citizens / end-users-	3
Measure 3.3 (all sub-options): (Introducing) Security requirements	Reduced the risks of delays in the process and unharmonized interpretation of security requirements for Wallet app providers-	3
Measure 1.5: Strengthen security requirements for mutual recognition	Savings in compliance costs for public authorities	1, 2, 3
	Savings in compliance costs (related to security certifications, GDPR requirements) - €12,000 to €24,000 - for eID providers	1, 2, 3
	Increased personal data protection and online security for citizens / end-users	1, 2, 3
Measure 2.6: legal requirements to ensure the protection of personal data	Increased personal data protection and online security for citizens / end-users	2,3
Measure 1.6: Introducing new Trust Services	Increased revenues due to the introduction of eArchiving - €37 million a year for every additional 1% of businesses purchasing an eArchiving solution - for Trust Service Providers.	1, 2, 3
	Enhanced offer in the Trust Services market for citizens / end-users	1, 2, 3
Measure 1.7: Harmonise the certification process for remote electronic signing	Increased competition and security of trust services and acceptance of mobile trust services for citizens / end-users	1, 2, 3
Measure 1.8: Strengthening the Recognition of QWACs (Qualified Website Authentication Certificates)	Cost savings from reduced damages related to cybercrimes for citizens / end-users	1, 2, 3
	Increased personal data protection and online security for citizens / end-users	1, 2, 3

5.5 Wider impacts

This section presents an overview of main economic, social and technological impacts associated with each Policy Option. No relevant environmental impacts could be identified.

The analysis is based mainly on results of a dedicated external study. Where quantification was possible, numbers and values are sometimes presented as broad ranges. This reflects uncertainties about existing data, as well as outcomes of sensitivity analysis and ranges of assumptions applied (e.g. on economic growth and number of jobs created).

Economic impacts

Option 1

The measures aiming to enable the use of public eIDs by the private sector will create additional **market opportunities** for online service providers who will be able to digitally expand their customer base at EU level. Similarly, the measures aiming to expand the number of private sector use cases that can be supported in the eIDAS network are expected to lead to greater adoption of the notified schemes for private uses, thus increasing the number of **private sector transactions.** The size effect would depend on the extent of private sector adoption and on the choices for use-cases to be technically enabled.

Greater harmonisation brought by **certification and references to standards** are expected to help mitigate the national implementation differences currently responsible for some of the frictions in the market for eID and trust services. The measures aiming to harmonize the operation of conformity assessment bodies will facilitate their **cross-border operation,** thus increasing development opportunities from performing certifications in more Member States. Trust service providers as well as online service providers that want to re-use notified schemes in other Member States would see new segments of the market open and their **transaction costs** from operating across the EU reduced.

Option 1 as a whole is likely to generate a very limited positive impact on **economic growth**. The macroeconomic benefits are estimated at €127 million added value generated over 10 years following implementation, of which almost 50% expected already in the first year.

Option 2

A stronger and wider European framework for the provision of trusted electronic identity authentication services underpinned by legal identities provided by Member States can boost global trade and support competitive advantage of EU-based enterprises. From this perspective, Option 2 could be beneficial as it facilitates:

- The creation of a world-class digital identity attribute autheticaion system that promotes Europe's leadership in this field
- The competitive advantage of European businesses globally, through greater digitalization (and thus, efficiency and effectiveness) of their service offering

Option 2 may also have a postitve effect on **International cooperation**. An improved and extended framework for the provision of identity and autheticaiton servcies can increase opportunities for mutual cooperation with other parts of the world, which would benefit European businesses. Imitation effects may also ensue in the long-time if the new framework delivers on its intended results, so that the EU's regulatory approach informs the development of legal frameworks for digital identity in other jurisdictions across the globe.

The table below reports the results in terms of **economic growth** obtained by a dedicated external study. These figures only capture the value added created by any additional

investments that can be attributed to changes in the legislation. As such, it refers to indirect effects only and does not take into account the direct productivity benefits accruing to businesses because of cost efficiencies and an expansion of the market.

Additional investment triggered by legislative changes (€millions)	Value added generated (€millions, 2019 prices) - Total by level of adoption, over 5 and 10 years					
	20% adoption		33% adoption		67% adoption	
	5 years	10 years	5 years	10 years	5 years	10 years
€100	€127	€133	€182	€189	€244	€254
€500	€637	€662	€910	€946	€1,220	€1,268

Option 3

Provision of a standardized European Digital Identity WalletApp is expected to result in more significant impacts on **international trade and competitiveness.** Creating a unified, more easily recognisable EU approach internationally would make a positive difference to the EU's ability to raise its global profile in digital identity, foster the competitive advantage of European businesses globally (as the obligation around universal acceptance within the EU will provide a greater boost to digitalisation) and to cooperate with third countries.

In terms of **economic growth**, under this option, it is expected that the introduction of a standard-based system will reduce uncertainty for market actors. As for the previous options, the results are provided are based on an a dedicated external study. Also in this case figures only capture the value added created by any additional investments that can be attributed to changes in the legislation.

Additional investment triggered by legislative changes (€millions)	Value added generated (€millions, 2019 prices) - Total by level of adoption, over 5 and 10 years					
	20% adoption		33% adoption		67% adoption	
	5 years	10 years	5 years	10 years	5 years	10 years
€100	€130	€133	€186	€189	€249	€254
€500	€650	€662	€929	€946	€1,244	€1,268

Social impacts

Option 1

The social impact under this policy option is expected to be positive but limited impact on **employment growth**. Once implemented, this policy Option is estimated to generate between 1,5 thousand and 2,8 thousand additional jobs in 10 years across the economy, half of which likely to be created in the first year of implementation.

In addition, Option 1 has the potential to enhance the **digital inclusion** of citizens (and disadvantaged groups) since the obligation for Member States to notify at least one eID scheme would provide citizens with universal access to an eID both at national level and in a cross-border context (to be used at least to access public services in other EU country). Option 1 has no cost implications for citizens.

Option 2

A positive impact on **employment** is expected from this option via its contribution to the future expansion of online transactions and reduction of barriers in the Internal Market. Taking into account the results from a dedicated external study, the introduction of this policy option is expected to generate between 5 thousand and 26 thousand additional jobs over the 5 years following implementation, which could be extended to 6 thousand and 28 thousand additional jobs in 10 years, if an adoption rate of eID by European enterprises of 67% (i.e. around two thirds) is reached[295]. This means that indirect effects in terms of job creation will likely be minimal, even at relatively high adoption rates; at the same time, no significant employment loss is likely to occur in net terms despite the strong incentive provided by the option towards digitalization and automation of processes connected to digital identity.

Additional investment triggered by legislative changes (€millions)	Additional jobs generated (thousands) - Total by level of adoption, over 5 and 10 years					
	20% adoption		33% adoption		67% adoption	
	5 years	10 years	5 years	10 years	5 years	10 years
€100	3	3	4	4	5	6
€500	14	15	20	21	26	28

Option 3

Option 3 (all sub-options) is expected to generate a slightly positive impact in the employment sphere. As discussed with regard to the estimates for economic growth, the majority of the expected impact on job creation is going to be generated within the first five years following implementation. Based on the results of an external dedicated study, additional investments that could be attributed to a change in the legislation in line with Option 3, are expected to generate between 3 thousand and 27 thousand additional jobs over the 5 years following implementation, which could be extended to 6 thousand and 28 thousand additional jobs in 10 years if an adoption rate of eID by European enterprises of 67% (i.e. around two thirds) is reached[296]. This means that, despite the impact on employment can be considered minimal, no significant employment loss is likely to occur in net terms. An overview of the impacts is illustrated in the table below.

Additional investment triggered by legislative changes (€millions)	Additional jobs generated (thousands) - Total by level of adoption, over 5 and 10 years					
	20% adoption		33% adoption		67% adoption	
	5 years	10 years	5 years	10 years	5 years	10 years
€100	3	3	4	4	5	6
€500	14	15	20	21	27	28

295 These figures only capture the jobs created by any additional investments that can be attributed to changes in the legislation. As such, they refer to indirect effects only and do not take into account the direct productivity benefits accruing to businesses because of cost efficiencies and an expansion of the market (discussed in the previous section)

296 These figures only capture the jobs created by any additional investments that can be attributed to changes in the legislation. As such, they refer to indirect effects only and do not take into account the direct productivity benefits accruing to businesses because of cost efficiencies and an expansion of the market (discussed in the previous section)

The positive impact on employment could also be explained by the reduced costs for businesses to identify relevant and adequate candidates. In this regard, a pan-European digital ID is likely to facilitate employee authentication, in particular of workers involved in non-traditional jobs such as the gig economy. Thus, reducing the time requested by businesses to find the most appropriate employee for an open position. This is confirmed by the fact that the proportion of job applications undergoing background checks has increased considerably (across 15 percent of the average hiring cycle).[297]

A greater availability of eID means will also support digital inclusion of citizens at risk of exclusion, particularly those who transact less online. A wider use of digital identity is likely to generate a positive effect on lower-income people, as it would allow them to participate in the modern digital economy in many ways such as assert their rights over digital services they have contracted.[298]

Previous research[299] identifies people who lack any form of legally recognised identification as a group that could benefit from access to digital identity. For example, refugees, stateless and forcibly displaced persons who may have fled their home countries without formal identification. Access to digital identities can help these individuals and their families prove their identities for access to assistance and basic services (e.g. purchasing a SIM card)[300].

With regard to people with disabilities, the introduction of digital ID is expected to facilitate access to several services, especially for the public sector. However, its impact depends also on the level of web-accessibility of public sector bodies, which remains low.[301] In the Open Public Consultation, 36% of respondents report accessibility barriers for persons with disabilities as one of the factors that could limit the use of eID. In this context, the transposition of the European Directive on the accessibility of websites and mobile applications in national legislation is expected to reinforce the benefits associated to Option 3 for this category of people.

Older people are also a category of stakeholders potentially able to benefit from the introduction of a digital eID, as it would eager the ability to access digital services (e.g. social assistance and/or healthcare services). This group would be encouraged to make more extensive use of their identities if convenient and secure solutions were made available. However, benefits are expected to be mitigated by a number of barriers faced by older people: available evidence shows that often older persons do not fully benefit from the potential of ICTs, due to a number of barriers to access to technology, as well as the digital divide experienced by this group of people. As a result, older people that have no or limited access to websites could be forced to seek alternative and potentially more costly solutions, generating a negative impact.

In addition, wider availability of digital identity is regarded as promoting:

- Citizen engagement: more opportunities to engage with services and civic processes online with secure digital identities can encourage participation from citizens who would not otherwise engage with these. For example, in Estonia, 1 in

[297] Why is hiring taking longer? New insights from Glassdoor data, Glassdoor, June 2015

[298] Brookings (2015), Identity and inclusion: When do digital identities help the poor?

299 McKinsey & Company. (2019). Digital identification: A key to inclusive growth

300 UNHCR (2019) Global Virtual Summit on Digital Identity for Refugees, Concluding Workshop: Summary Conclusions and Recommendations

[301] This was first showed by the "Measuring progress of eAccessibility in Europe" (MeAC) study in 2007, and then confirmed by the subsequent studies MeAC 2 (2010) and MeAC3 (2012).

5 of the over 30% of individuals vote online say they would not vote at a physical polling place.[148]

- More inclusive access to public and private services linked to public goods such as education and health, to which some social groups currently face some barriers. For instance, citizens with disabilities or living in rural areas have lower access to services that normally require physical presence if not delivered locally. If greater availability of digital identity resulted in more services being accessible online, these groups would disproportionately benefit from the intervention.

Technological impacts

Option 1

European **certification schemes** are likely to have a positive impact by incentivising the creation of highly secure eID solutions and by strengthening enforcement of the EU regulatory frameworks in the eID field. Introducing European standards via EU wide certification schemes would also support EU's **technological autonomy**. Technological sovereignty would also be enhanced through greater harmonisation of the implementation of eIDAS, as regulatory consistency and enhanced seamless delivery of cross-border services constitute supporting factors[302].

Option 2

With regard to **innovation and technological competitiveness**, Option 2 is likely to have a positive impact on innovation, as far as it would:

- Bring to the market solutions that build on the more significant private sector knowledge, skills and previous investments. These assets can be leveraged to build more ambitious and cutting-edge eIDAS-compliant solutions in the future, as commercial providers have the resources, know-how and incentives to take on riskier R&D projects.
- Create a more competitive market with independent participation from commercial providers, which would strengthen the incentive to innovate. More competition would encourage providers to gain a competitive edge through value-based differentiation of their products, bringing with it a better ability to achieve a return on R&D investment. Combined with more regulatory certainty, this would have a positive effect on the exploitation of technologies.
- Expand to public procurement for electronic identity and authetication solutions, as the measures proposed provide an opportunity to boost technological development in the field through public procurement processes, particularly with regard to investments that private sector actors may be less well positioned or willing to make (e.g. because returns may be too long-term or not fully appropriable).

Option 3

Similarly to option 2, Option 3 (all sub-options) is expected to have a **positive impact on innovation.** Option 3 includes measures to promote interoperability, resulting in:

302 See OECD. 2011. "Communiqué on Principles for Internet Policy-Making." OECD High Level Meeting, The Internet Economy: Generating Innovation and Growth. June 29. p. 3. <http://www.oecd.org/internet/ innovation/48289796.pdf>. Such criteria have been used to assess impacts on technological sovereignty in other studies; for example, see Maurer, T et al. (2016). Technological Sovereignty: Missing the Point?. 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace https://www.ccdcoe.org/uploads/2018/10/Art-04-Technological-Sovereignty-Missing-the-Point.pdf

- A stronger effect on innovation, as interoperability can be a driver of innovation in its own right[303].
- A stronger influence on the type of investments demanded in the market. Given the trade-offs to be made between interoperability and technological neutrality, more of the former would mean a stronger signal to the market as to the investments that should be prioritized (i.e. those that are more aligned with the technologies referenced by interoperability frameworks).
- Boosting the presence and accessibility of secure elements in mobile devices, which in turn can enable advances in other identity applications and beyond.

In addition, creating an EUeID with wide usability will ensure that more market players have an incentive to invest or encourage investments in cutting-edge digitalisation technologies.

Impacts on fundamental rights

Option 1

Option 1 would have positive effects on EU citizens in terms of their **opportunities to live, work and access services** seamlessly across EU. These effects are particularly dependent on the successful implementation of the measures to allow private sector re-use of notified schemes and on the design of a commercial model supporting cross-border transactions implying private relying parties.

Option 2

This option promotes better compliance with the provisions of the Charter of Fundamental Rights of the European Union, supporting, in particular:

- Freedoms – the right to Protection of personal data, which would be more effectively upheld to greater availability of highly secure solutions and additional provisions to promote data privacy, security and transparency of processing of identity data.
- Equality – As outlines in more detail as part of the social impacts, increased access to private and public services online can promote the digital inclusion of groups with low digital literacy and/or who may experience significant barriers in accessing services in person, thus furthering, in some cases, the rights of the elderly and the integration of persons with disability, provided that those services comply with accessibility requirements for persons with disabilities.
- Solidarity – Access to services of general economic interest, environmental protection, consumer protection would all be promoted by greater access to services online through more secure and privacy-preserving digital identity authentication solutions.
- Citizens' rights - greater access to trusted and convenient means available to access public and private services cross-border support the right to freedom of movement and of residence, making essential transactions easier in particular for European citizens living and working in EU countries other than their own[304].

303 Although the relationship between the two is highly complex and fact-specific. See for example: Gasser, U. Palfrey, P. (2007) When and How ICT Interoperability Drives Innovation. The Berkman Center for Internet & Society, Harvard University

304 The free movement of workers is also a fundamental right guaranteed by the Treaty on the Functioning of the European Union (EU)

A positive impact on employment is expected from this option via its contribution to the future expansion of online transactions and reduction of barriers in the Internal Market (see above).

Option 3

Option 3 (all sub-options) promotes better compliance with the provisions of the Charter of Fundamental Rights of the European Union, in line with the positive impacts on Freedom, Equality, Solidarity and Citizens' Rights:

- Freedoms – the right to Protection of personal data, which would be more effectively upheld by a secure, that is designed according to the principles of privacy by design.
- Equality – simplified access to private and public services online can promote the digital inclusion of groups with low digital literacy. Digital access in general lowers barriers as compared to services in person, for persons with disabilities, provided that those services comply with accessibility requirements for persons with disabilities. These advantages are however partially offset by the relatively high requirements as regards necessary (safe but costly) equipment on the side of the user.
- Solidarity – Access to services of general economic interest, environmental protection, and consumer protection would all be facilitated through more secure and privacy-preserving digital identity solutions.
- Citizens' rights – The EU_eID as a trusted and convenient means to access public and private services cross-border supports the right to freedom of movement and of residence, making essential transactions easier in particular for European citizens living and working in EU countries other than their own.

In addition, this option is expected to generate positive impacts in terms of more democratic, private, secure, and competitive digital basis for personal data management. Compared to the concept of federated identity, which could lead to the accumulation of control into the hands of a few identity providers (IdPs), the European Digital Identity builds an identity framework where the citizen communicates directly with her/his communicating parties (credential providers, service providers). The absence of intermediaries is likely to generate a positive effect.

Environmental impacts

All policy options

The overall assessment of the environmental impacts of the three options vows for greener paper-less and simplified processes enabled by the new identity ecosystems; yet with some caveats. The positive environmental impact is expected to be greater according to the different levels of ambition of each Policy Option, with the first policy option having the most limited environmental effects while PO3, which is expected to improve to the maximum extent the take up and usability of eID would bring the greenest potential.

Already SWD 2012 (135) identified that the eIDAS regulation would have led to a simplification of administrative procedures as well as to a reduction of paper-based processes. Indeed, the enhancement of the current Regulation will foster even more the replacement of paper-based interactions by electronic interactions allows for savings to be realised at many different levels such as postage, printing costs, processing time, ease of reuse of information, reduced error rates in data processing, transportation costs, archiving costs. These aspects became even more apparent during the COVID-19 crisis, where the restrictive measures to activities in presence have forced citizens and businesses to rely on

online access to public and private services thus boosting the request and use of secure eID.

To provide an order of magnitude of the impacts in relation to public services we can cite the Italian example. The number of Italian digital identities (SPID) at the end of 2019 was ~5 million. Today, the active users are more than 18 million active with a steadily increase of ~1 million users[305] per month. [for example, the use of SPID went from ~55 million for the entire year 2019 to ~32,4 in the sole month of February 2021], bringing positive impacts on the emissions reduction related to public service delivery.

The paperless process of identity verification cut down on environmental costs also in relation to private sector services. For instance financial institutions incurs in high record management costs throughout the client engagement life-cycle due to the dependence on paper. The records management expenses across the value chain (from record creation at a branch to the point of warehousing the physical documents) can be broken down into several phases, with two of them having substantial environmental impacts; the origination process such as the paper documents associated to the opening of a new bank account, but also transport related to the submission of original documents from branches to headquarters[306].

On the other side the benefits just presented are partly offset by the increased reliance in both private and public services delivery on online interactions which requires electricity consumption for the full life cycle of data centres which consume high levels of energy to power the IT equipment contained within them. However in order to properly assess the environmental impacts it shall be noted that if the energy used by a computational process is renewable, the energy consumed by that process is limited.

Summary of wider impact

A summary of the main wider impacts expected per each policy option is given in the table below.

[305] https://avanzamentodigitale.italia.it/it/progetto/spid

[306] https://www2.deloitte.com/content/dam/Deloitte/za/Documents/financial-services/ZA_ItsTimeToGoPaperless_24042014.pdf

Table 4. Summary of wider impacts

Impact categories	PO 1	PO 2	PO 3
Economic impact	• Expansion of online transactions and reduction of barriers in the Internal Market • €127 million added value generated over 10 years	• Stronger and wider European framework for trusted eID means • €127m - €1268 m added value generated over 10 years	• Boost global trade and support competitive advantage of EU-based enterprises • €130m - €1268 m added value generated over 10 years
Social impact	• Positive impact on employment growth (between 1,5 thousand and 2,8 thousand additional jobs in 10 years across the economy) • Increased digital inclusion of citizens (disadvantaged groups)	• Positive impact on employment via expansion of online transactions and reduction of barriers in the Internal Market • Between 5 thousand and 26 thousand additional jobs in 5 years which could be extended to a range between 6 thousand and 28 thousand in 10 years if the adoption rate of eID by European enterprises reaches the 67%	• Positive impact on employment via expansion of online transactions and reduction of barriers in the Internal Market • Between 5 thousand and 27 thousand additional jobs in 5 years which could be extended to a range between 6 thousand and 28 thousand in 10 years if the adoption rate of eID by European enterprises reaches the 67% • Increased digital inclusion of citizens and more inclusive access to public and private online services linked to public goods
Technological impact	• Strengthened EU regulatory framework • Increased EU technological autonomy and sovereignty	• More investment in user-friendly, secure solutions building on innovative technologies • Innovation stimulus via public procurement	• More investment in user-friendly, secure solutions building on innovative technologies • Innovation stimulus via public procurement
Fundamental rights	• Increased opportunities to live, work and access services seamlessly across EU	• reduced risk of ID theft and greater access to trusted and convenient means available to access public and private services online • Increased equality through the removal of barriers to access to public and private online services • Increased access to services of general economic interest, environmental protection, and consumer protection through more secure and privacy-preserving digital identity solutions • Strengthen freedom of movement and of residence, by easing essential digital transactions	• reduced risk of ID theft and greater access to trusted and convenient means available to access public and private services online • Increased equality through the removal of barriers to access to public and private online services • Increased access to services of general economic interest, environmental protection, and consumer protection through more secure and privacy-preserving digital identity solutions • Strengthen freedom of movement and of residence, by easing essential digital transactions • Positive impacts in terms of more democratic, private, secure, and competitive digital basis for personal data management
Environmental impact	• Limited but positive environmental impact due to the extended substitution of paper-based procedures with digital procedures.		

5.6 Impacts on SMEs

In the context of the digital identity proposal, SMEs are going to be affected in their capacities as eID/trust service providers and as end users. Given the current market situation the large majority of trust service providers in the EU are SMEs some few are subsidiaries or departments of larger companies[307]. In a wider sense, all SMEs that make regular use of digital services for their business are expected to be impacted. The number of impacted SMEs in EFTA countries that use digital services amounts to about 5 million[308].

A recent survey of SMEs indicates that current uptake of eID (whether or not eIDAS-notified) and trust services is around 17%. In the same survey, around 30% of SMEs reported being in the process of implementing eID/trust services or interested in doing so. Removing commonly reported barriers to SME uptake of eID and trust service solutions, such as complexity and lack of information, is therefore likely to support an increase in uptake up to slightly under half of SMEs (47%), and enable an additional 3 in 10 SMEs to access the benefits estimated. The potential uptake could grow even further with effective awareness raising. About half of the SMEs responding to the survey reported interest in digitalising their business further; yet, 30% indicated that they were not interested in implementing eID/trust service solutions. Narrowing that gap could support an uptake beyond the levels that could be expected by just considering SMEs that currently show interest in adopting eID and trust services, potentially pushing uptake levels beyond 47%.[309]

Option 1

SMEs as ID/Trust service providers: SMEs would benefit from the measures of option 1 for a more consistent implementation of eIDAS provisions across Member States to facilitate their business. At the same time, compliance costs associated with policy changes such as security certification affect SMEs disproportionally but also deliver cost savings in the medium / long-term. An estimated saving of €360,000-€900,000 per year for SME ID/trust service providers from greater harmonisation of audits can be identified.

SMEs as end users: In their capacity as end users, an extension of eID to private service providers (e.g. measures on requirements, extension of data set, cost-liability schemes) could create significant savings for SMEs in online transactions with suppliers, partner businesses and public administrations. Estimates on wider use of eID by citizens in accessing public services online suggest, SMEs would save, on average, 20 hours per year[310]. Assuming that the same saving can be achieved on private service transactions (for a total of 40 hours saved), this average time saving amounts to nearly 200 million hours saved across all SMEs using digital services in EFTA countries, and an associated cumulative saving of €4.1 billion a year (around €800 per SME)[311].

Option 2

SMEs as ID/Trust service providers: The introduction of a new qualified trust service for the exchange of data linked to identity opens new business opportunities for existing trust

[307] Definition of SME ; Overview of trust service providers: https://webgate.ec.europa.eu/tl-browser/#/tl/DE/9

[308] According to OCED reports 20% of SMEs are engaged in sales through e-commerce.

[309] https://op.europa.eu/en/publication-detail/-/publication/712f9ce2-5042-11e9-a8ed-01aa75ed71a1/language-en

[310] McKinsey & Company. (2019). Digital identification: A key to inclusive growth

[311] The value of each hour saved is defined as the average hourly labour cost across Member States (source: Eurostat, Labour cost, wages and salaries, direct remuneration (excluding apprentices) by NACE Rev. 2 activity) - LCS surveys 2016 [lc_ncost_r2]

service providers / SMEs as they are established in the business and accustomed to the related regulatory compliance requirements.

There will be additional compliance costs for non-qualified providers which will however remain limited as compliance procedures are less demanding[312].

SMEs as end users: SMEs are likely to benefit from the possibility to identify or authenticate their customers which creates efficiency and simplification benefits; SMEs as end-users would benefit from opportunities to exchange enforceable certificates cross-border, thus reducing an important barrier in the market that disproportionately affects smaller providers. SMEs relying on eID/trust services for online service delivery would enjoy better access and a wider range of solutions to choose from. Estimates suggest the costs for identity verification / authentication in some sectors can be reduced by 90%[313]. Assuming that SMEs spend €40 for identity verification[314] and on-boarding of each user, a business on-boarding 500 users a year can save up to €18,000 in costs on an annual basis.

As end-users, SMEs have fewer resources to interact with public administrations and other businesses and would therefore see transaction costs go down more significantly than other types of businesses. As indicated in the previous option, savings from reduced time spent on these transactions would be up to €4.1 billion a year overall, or around €800 per SME[315]. The additional opportunities created by their ability to use a much wider range of attributes and attestations in transactions (because of M 2.4, which introduces QVCs as a trust service) is likely to expand the potential savings for SMEs beyond this figure.

Option 3

SMEs as ID/Trust service providers: Sub-option 3.1 foresees the deployment of the European Digital Identity Wallet as a trust service. This opens new business opportunities for SME ID/trust service providers, although development and certification costs are likely to act as an entry barrier. SMEs would need to identify a strong business case in order to deploy the necessary resources and develop the wallet and conclude agreements with other players in the Wallet ecosystem e.g. credential providers).

Sub-option 3.2 would offer potential opportunities for SMEs as contractors to implement the wallet on behalf of Member States of the Commission. Compared to the opportunities offered by option 2, these opportunities are however likely to remain more limited.

SMEs as end users: SMEs may be interested in adopting wallet services for the purposes of business transactions, while larger companies are likely to favour desktop based solutions based on automated processes (e.g. social security companies using dedicated platforms). Integrating the wallet through APIs to consume credentials / attributes and identify or authenticate customers creates costs to SMEs which are however likely to be offset by simplification and efficiency benefits, depending on the specific business case.

---

[312] Requirements for non-qualified trust service providers include the current technical and organisational measures to manage risks to the security of the services provided, reporting requirements, training requirements for staff, the use of trustworthy systems and products, security assessment schemes for relevant components, validation and authentication etc.

[313] McKinsey & Company. (2019). Digital identification: A key to inclusive growth

[314] Customer identification costs for onboarding have been estimated at €30-40 per user. We apply the upper bound estimate to account for the higher costs that SMEs are likely to sustain in these processes due to lower digitalisation.

[315] The value of each hour saved is defined as the average hourly labour cost across Member States (source: Eurostat, Labour cost, wages and salaries, direct remuneration (excluding apprentices) by NACE Rev. 2 activity) - LCS surveys 2016 [lc_ncost_r2]

6 COMPARISON OF THE OPTIONS

In order to compare the different policy options and sub-options, a multi-criteria analysis of possible scenarios is carried out using an approach consistent with the EU Commission's Better Regulation Toolbox (Tool #63). This analysis is carried out with respect to two sets of criteria:

- Effectiveness, Efficiency and Coherence with other EU policies, as recommended by the Better Regulation guidance. With respect to the third criterion, an internal dimension of coherence has also been included to provide a general assessment of the internal consistency of the measures proposed (in light of the complexity of the policy options
- The criterion of proportionality of the three policy options has also be added to provide a more comprehensive comparative assessment

A detailed comparison of the options against each criterion is provided below.

6.1 Effectiveness

In an ex-ante perspective, effectiveness describes the extent to which the proposals are expected to generate effects that are consistent with the policy objectives set. The section below assesses each policy option in terms of the four specific objectives defined for the revision of eIDAS (see Chapter 3), which are as follows:

- Specific objective 1: **Provide access to trusted and secure digital identity solutions for all eu citizens and businesses cross borders**
- Specific Objective 2: Make accessible a wide range of public and private online services relying on trusted and secure digital identity
- Specific Objective 3: Citizens are in control of their personal data and their security is assured
- Specific Objective 4: Ensure equal access to to the trust services market"

Specific objective 1: Provide access to trusted and secure eID means for all EU citizens and businesses cross borders

Option 1 is expected to achieve this specific objective, and to bring significant improvements compared to the baseline mainly for the public sector. If implemented by Member States in a coordinated manner, the measures would potentially lead to eIDs available to all EU citizens and companies. The shortcomings linked to the current design of the trust-building mechanisms under eIDAS and the barriers to notification would most likely be alleviated by streamlining the peer-reviews and the notifications processes. The mutual recognition principle would be strengthened, thus contributing to the fulfilment of this objective.

Compared to the baseline, **Option 2** is expected to provide a major contribution to this objective, without however achieving it. The new trust service for the provision of credentials is expected to provide a significant boost both to the EU citizens' access to trusted digital identities and to expand considerably their possibilities to engage in online transactions. Option 2 provides a more effective response to the issues identified with low private sector re-use of eIDAS schemes than Option 1. As a standalone option, the contribution to achieving this objective would be dependent on the number of Member States that have notified their eID schemes. Consequently, only citizens of Member States who notified would benefit from the cross-border legal effect allowed by the qualified digital identity attributes linked to these notified eIDs. Hence, assessment and the successful

implementation of option 2 is reliant on the strengthening of the notified eIDs system under eIDAS to be completed under Option 1.

Option 3 is expected to attain this objective, regardless of the implementation scenario chosen, and would mark a sharp improvement in both the availability of eIDs and of the related digital identity attributes to be used by European citizens cross-border. Due to the similar functionalities of the wallet and benefits for the user, all sub-options would be equally effective. However, specificities linked to the possible effects on the market or to the deployment speed of the wallet would be likely. Compared to Options 1&2, all sub-options under Option 3 would provide a more rapid and direct vehicle for universal access to widely usable and trusted eID means by European citizens. It is expected to deliver the greatest level of acceptance by public and private online service providers. The wallet will enable the availability and use of both primary identity data (notified eIDs under option 1) and of a wide spectrum of digital identity related attributes (qualified or non-qualified attributes, as developed under option 2) that can be unlocked only by the user. The wallet would act as a single sign-on for all the digital identity data of the users. These features will allow maximum flexibility in accessing and managing both qualified and non-qualified attributes and eID related data, which cannot be achieved under Options 1 & 2.

It should be noted that the assessment of Option 3 to fulfil this objective is dependent on a series of assumptions and external factors.

Firstly, Option 3 has some inherent limitations in terms of possible outreach to citizens and companies, which stem from the high level of security to be set for the wallet via standards. It is likely that the mobile device compatible with the wallet service needs a hardware element with enhanced security features - i.e. an embedded secure element (eSE) or an embedded SIM card (eSIM). However, it is likely that market developments and recent standardisation processes accelerate the full availability of secure devices.

Secondly, full achievement of this objective by Option 3 relies on the capacity of Option 2 to deliver a mature and diversified market for credentials, which would subsequently be used via the wallet.

Finally, similarly, the on-boarding to the wallet is dependent on the existence of national eIDs notified under option 1, although an alternative solutions is foreseen for situations where Member States have not yet notified their eIDs.

Despite these limitations, it is expected that during the next years, by the time of adoption of the proposal, the availability of such devices to grow exponentially and even become omnipresent[316], at some point, driven by the penetration of mobile demand for secure applications from the private sector. Moreover, innovation might drive wallet providers to build secure solution that rely on a different solution than a hardware element. Overall, if pursued, Option 3 has in itself potential to boost the demand for secure elements in mobile devices.

316 There are currently 5.9 billion people with access to mobile telephony (70% of which are smartphones). Moreover, according to Juniper Research, the growth in mobile digital identity solutions could exceed 800% over the next five years, with unique mobile identifier services likely to become the primary source of identification for over 3 billion people by 2024 (https://www.gsma.com/identity/news-flash-7-billion-opportunity-in-digital-identity-for-operators-by-2024-as-world-turns-to-mobile)

Objective 2: Make accessible a wide range of public and private online services relying on trusted and secure digital identity solutions cross border

Option 1 is expected to have a limited potential to improve cross-border and cross-sector use of electronic identities and to support a larger ecosystem of use cases.

The measure establishing a requirement for Member States to allow private online service providers across the EU to rely on notified eIDs would provide service providers the opportunity to integrate notified eIDs in their business models. There are limiting factors to the establishment of such an obligation which might hinder the success of the option, such as the diversity of national legislation regulating the relationship with the private service providers[317].

The proposed measures to address uncertainties over costing and liability are widely seen by stakeholders as potentially beneficial, to the extent that they provide a response to an issue that has been frequently described by stakeholders as key barriers to private sector re-use of eIDAS schemes. That said, the complexity of an accompanying commercial model (contract) tailored to the needs of the private sector would imply complex negotiations between the Member States on the harmonisation of national liability regimes, on the pricing and billing strategies on the general operating models or on the service level agreements. The same reasoning applies to the definition and addition of further sector-specific attributes to the current eIDAS minimum data-set, thus justifying the low score for this option. When compared to Options 2 & 3 (sub-option 1), Option 1 offers less flexibility, as opposed to the dynamism and innovative potential of the private sector in developing the sector-specific attributes. Option 1 relies on the definition of attributes based on a heavy intergovernmental decision-making mechanism, while option 2 is supported by the reactiveness and the innovation potential of the open market which is empowered to develop tailored made solutions mirroring specific demands.

Compared to the baseline, **Option 2** is expected to provide a major contribution to the achievement of this objective. Option 2 would contribute to this objective by unleashing the potential of the credentials shared cross-border. This marks an important progress when compared to the baseline since it would empower citizens and companies to make use of the widest possible diversity of credentials in their digital transactions. Option 2 will contribute to the creation of a genuine market for attributes and for their exchange cross-border. As in the case of the specific objective 1, the success of option 2 is dependent on access to the authentic sources provided by notified eIDs under option 1. As a stand-alone option, the impacts of the option would be limited since trust service providers would be able to issue qualified attributes relying only on the eIDs of the citizens who hold a notified eIDs.

Option 3 would fully address this specific objective. It has the highest potential to empower citizens to exercise their freedom of movement in any of the Member States. In practice, the European Wallet would provide easy and seamless access to the essential services provided by the public and private service providers, thus simplifying citizens' efforts to establish in other EU Member State or to start a business abroad.

An EU Digital Identity scheme and of a standard-based framework are the central tenets for achieving maximum harmonisation and an interoperability structure that can seamlessly support a diversity of eID solutions in the public and private sector. The implementation of such standard-based system clearly puts the potential positive impact of Option 3 on this objective well ahead of the effects that could be achieved through Option 1 and 2 alone, at least with regard to harmonisation of eID. Option 3 displays the largest possibilities to

317 In some Member States – e.g. the Netherlands - the reliance of private sector on the national eIDs is open only to the bodies with a public mission).

combine attributes in various ways, ranging from low levels of assurance (e.g. login to various platforms based on username/email and password) to high levels of assurance needed for specific transactions (e.g. banking, telecom, eHealth, diplomas or proofs of membership to a professional association, etc.). However its full potential will be achieved if Options 1 and 2 are implemented because the success and universal availability of the scheme depends on all Member States enabling access to eID to their citizens and on a healthy market for the secure exchange of data linked to identity.

Option 3 also outperforms others in terms of providing a convenient eID solution that is more likely to attract significant usage by citizens and therefore also wider acceptance across public and private online services. The evidence gathered on public views of digital identity (through the Commission consultation and the Eurobarometer survey previously discussed) indicateS a strong preference for convenient, widely usable eIDs, which flags the importance for eIDAS of delivering eID means with these characteristics to make life simpler for EU citizens, companies and public institutions. As part of the OPC, a majority of respondents mentioned that the use of eID contributes to saving time (77% of respondents), a simplification of the administrative procedure (74% of respondents), saving money (68% of respondents) and an increase in service quality (65% of respondents). This would suggest that Option 3 would be the most aligned with this objective, as it is expected to deliver universal access to EU citizens as well as the greatest level of interoperability and acceptance by public and private online service providers.

Option 3 (like Option 2) is more prone to encouraging innovation by stimulating the private sector to invest in the development of a wide range solutions linked to real-life use-case, in a much more flexible way than option 1. For instance, the current KYC providers or data brokers acting at national level, once accredited as qualified trust service providers, would easily expand their business to provide their services cross-border as qualified services under Option 2, to be asserted in the context of a European wallet.

Objective 3: Provide citizens full control of their personal data and assure their security when using digital identity solutions

Option 1 would bring a major contribution to the baseline without fully achieving the specific objective (++). The full alignment of the eIDAS Interoperability Framework with the level of data protection introduced by the GDPR would require substantial changes to the current model where the whole eIDAS minimum dataset is automatically shared with the online service provider. Such an evolution would require major adjustments to the current infrastructure to enable new privacy and data protection features such as selective disclosure, pseudonymisation or unlinkability. It is likely that such steps would require additional investments and complex negotiations between the Member States that might not be concluded on a short-medium term perspective. Introducing certification of eID means at EU level is also widely seen as helping reduce the current fragmentation in the EU in terms of security requirements for eIDs, another important driver behind market fragmentation and concerns regarding the data security and privacy of end users

Option 2 would attain the specific objective. The measures under this option have the potential to safeguard the data protection level required by GDPR to a larger extent than Option 1. The new trust service would support more robust data protection, privacy and user control. Besides the requirements on providers of trust services for the secure exchange of data linked to identity, Option 2 goes a step further and establishes strict requirements for qualified trust service providers to query data from trusted, authentic sources. Specific measures in Option 2, such as keeping identity data functionally or structurally separate from other personal data, are strong safeguards for trust between the trust service providers and users.

Option 3 would fully achieve this specific objective. Since the wallet providers will be future qualified trust service providers, the data protection safeguards under Option 2 are fully integrated and applicable under Option 3 also. The added value of the wallet when

compared to the solutions under Option 1 & 2, is that it will offer similar convenience compared to the social login solutions or to the password managers available on the market, doubled by a high security and new privacy friendly ways to manage identity data will provide a higher level of user satisfaction. The wallet will provide unique features when compared to Options 1 & 2, namely empowering the user to be in full control over which personal data are shared with whom, while the recipient service provider will be able to quickly verify the requested data, strictly limited to the purposes of that specific transaction.

Specific Objective 4: Ensure equal access to the trust services market

For the purposes of analysing objective 4, the measures and the options targeted to improve the current trust services ecosystem will be considered.

Option 1 would imply exclusively soft coordination and enhanced dialogue measures without relying on strong regulatory intervention, and therefore Option 1 is likely to have limited contribution towards the achievement of this objective.

Option 2 would fully attain this specific objective due to the solid regulatory intervention addressing the problems and drivers. The current divergent practices on remote identification and remote signing, as well as the lack of harmonisation in the supervision of trust services will be addressed via targeted amendments of the Regulation and implementing acts currently referenced under eIDAS. In particular, harmonising various aspects of the Regulation would help enhance coherence in the conformity assessment process and remote identification have been frequently mentioned by stakeholders as areas where achieving more consistency should be prioritised, because they are perceived as primary causes behind the market fragmentation seen today in eID and trust services.

As described in the baseline scenario, it is possible that some greater level of coherence and interoperability could be achieved without further intervention as the reforms pushed by eIDAS continue to bed in and Member States find their own way around implementation issues. Equally, on the issue of interoperability, we may expect some degree of natural convergence towards global standards. However, the evidence suggests that much of the legal certainty and coherence problems are underpinned by factors that go well beyond the mere implementation of the Regulation, such as national differences in legislation and in cultural approaches to eID and trust services (e.g. in areas such as remote identification). Most importantly, more legal certainty, coherence and interoperability would deliver its greatest benefits at the level of the EU Digital Single Market by reducing fragmentation, such that a rapid and significant convergence of approaches on all of the issues described above could not be realistically achieved without further EU-level intervention.

Nevertheless, this general assessment of effectiveness needs to be complemented by two considerations:

- Since the measures mostly entail soft policy interventions, it is possible that harmonisation efforts may take some time and be uneven across Member States
- Stakeholder consultations have identified further issues that call for greater legal coherence and certainty, such as the legal effect of e-signature. The effectiveness of this option may therefore be improved through consideration of additional issues to be the subject of further guidance, implementing acts or clarificatory legal amendments.

  Some stakeholders have also identified the potential for unintended consequences. This was often argued by participants in our study on the basis that unnecessarily inflexible, restrictive or complicated guidance and implementing acts may harm effectiveness (due to over-regulation) rather than promote it.

6.2 Efficiency

Efficiency considers the extent to which the proposals provide a reasonable balance between benefits and costs. This section assesses each policy option in terms of the (i) compliance and administrative burdens generated for eID providers and businesses and (ii) compliance and enforcement costs generated to public authorities.

6.2.1 Compliance and administrative burden for enterprises

Option 1 is designed to reinforce the current regulatory framework and address the inconsistencies highlighted in the problem definition. For this reason, the implementation of this option is likely to produce a modest reduction of administrative costs and burdens (due to the introduction of guidelines and harmonisation procedures), while on the other hand slightly increase costs for regulated businesses due to the certification of eID means. Allowing private online service providers to rely on notified eIDs can substantially decrease compliance costs for regulated sectors where national eIDs are not yet available for the private sector to use, and especially with regards cross-border users.

Option 2 (measures 1 and 6) and option 3 are likely to generate limited additional compliance costs for providers of identity credentials, comparable to those currently incurred by trust service providers. Additional requirements for transparency are expected to generate minimal costs, due to the significant investments already made in response to the entry into force of GDPR. Harmonisation of the legal framework helps trust service providers to cut compliance costs and also support cross border service provision. Measure 2.5 will create compliance cost of integrating identity credentials for regulated service providers. The cost overall is high, but since the subjects are relatively large businesses, the cost per organisation is relatively low. Beside the interfaces, service providers would probably have to cover the costs for Wallet and credential providers if they impose fees. Compared to the baseline, the immediate cost for implementing measure 2.5 substantially overweighs the benefits for service providers. These costs may be balanced with benefits later on, depending on how the market for digital credentials develops (in terms of the number of users, number of transactions etc.).

6.2.2 Compliance and enforcement costs for public authorities

In **Option 1**, national competent authorities would incur in limited additional costs for enforcement due to the need to familiarise with the new legislation, contribute and align with new standards and guidelines, upgrade the interoperability infrastructure to support greater exchange of attributes and greater public sector re-use and campaigning efforts. Enforcement costs are expected to vary significantly among Member States, based on their current situation: from being largely cost-neutral for countries that have already aligned with new requirements, while limited costs are expected in those countries requiring significant changes to their operating model. The requirement to upgrade eIDAS nodes to meet new expectations such as selective disclosure and changes to the dataset would require an overhaul of the national infrastructure both on the side of node provisioning and service providers.

In the case of **Option 2**, an extension of the scope of the regulation is expected to generate additional costs due to national level supervision, which requires resources to be invested by national competent authorities to cover additional ex post supervision duties due to new trust services. Measure 2.2 will incur high costs for Member States to make available authentic data. The mandatory set-up cost depends on the scope of data and the number of organisations affected, but quite certainly will exceed the benefits for public bodies themselves (the benefits would be on the side of end-users and trust service providers).

In **Option 3**, the provisioning of Wallet Apps as trust services under sub-option 1 will impose national level supervision, which requires resources to be invested by national competent authorities to cover additional ex post supervision duties linked to the data protection provisions due to a new type of trust service. Sub-option 3 will also require supervision activities, but these costs would be smaller due to shared responsibility among Member States. In this case the burden of developing a Wallet is on the Commission, making it possible for all Member States to share the development cost. Sub-option 2, will incur high costs for Member States that may be balanced out with revenues in some cases, especially in larger markets thanks to economies of scale.

6.3 Coherence

Coherence describes the extent to which the options support wider policy objectives consistently with treaty-based legislation. This has been assessed by considering how far the options align with wider strategies and pieces of legislation, as well as by considering the internal consistency of the measures included under the option with regard to the overall objectives sought. In assessing the external coherence of the current and evolving legislations, none of the options impedes the correct implementation of other policy initiatives. At a high strategic policy level, and in conformity with treaty-based principles, the policy options are coherent – yet with different degrees of ambition - with overarching EU policy objectives.

To the extent the current eIDAS framework only partially succeeded in providing wide-spread access to public and private cross-border digital services[318], Option 1 would provide further harmonisation of the market, protecting the investments made, through improving the current legal framework for cross-border recognition of legal/national electronic identities.

Option 2 and 3 take a strong stance on data protection and ensure consistency with the GDPR regulation. In fact, the obligation for digital identity providers to differentiate between users' identification data and other data, and for gatekeepers acting as qualified providers of digital identity attribute services, to structurally separate this service from other gatekeeper services, would be a cornerstone of additional privacy-enhancing measures of the eIDAS revision. These initiatives are consistent with the objectives of the Single Digital Market supporting a fairer competition.

By contrast, only Option 3 seems to achieve the objective of developing an EU-wide secure public electronic identification to provide people with control over their online identify and enable access to cross-border digital services.[319] In this respect, Option 3 is the only option that demonstrates full coherence with the political mandate provided by the Council and the President of the European Commission Ursula von der Leyen its State of the Union speech on the 16 of September 2020.

This option is also the most coherent with overarching EU priorities since it provides the widest range of policy interventions to meet those priorities comprehensively and provide the best fit for EU priorities linked to the digital economy as set out in the strategy Shaping Europe's Digital Future:

- technology that works for people: the proposals directly support the aim to protect people from cyber threats and ensure technologies such as AI are developed in a way that is effectively regulated and meets high ethical standards;
- a fair and competitive digital economy: the proposals promote innovation, fair competition and better safeguards for personal and sensitive data; and
- an open, democratic and sustainable society - the proposals promote more control to citizens over their online data.

All three options help to support implementation of GDPR under eIDAS. With the enforcement of the General Data Protection Regulation, the demands and requirements for the handling of sensitive personal information have greatly increased. Article 32 of the GDPR demands that organisations implement appropriate measures to ensure the security

318 Results from the evaluation

319 European Council Conclusions – 9 June 2020

of personal information, and the first example of a measure to achieve this is pseudonymisation.

Option 1 is generally coherent with the demands of GDPR, in that, for instance, allowing cross-border exchange of selective attributes, instead of the whole minimum data set would support better alignment with GDPR principles and provisions; selective disclosure enables the system to transmit only those attributes of the eID that are absolutely necessary for the needs of each service. Option 2 is similarly coherent. Pseudonymisation can be a key feature in helping citizens protect their privacy, and for this reason it is seen as a key aspect to the privacy by design principle laid down in the GDPR. Option 3 provides a very comprehensive match towards implementing GDPR principles and provisions:

- Data minimisation
- Personal control of the holder
- Verifiable security
- Supervised security
- Functional compatibility with GDPR

Transversal measures to the three policy options provide elements in addressing consistencies with other key regulations such as the new Cyber Security Act. PO 1 (but also PO 2 and PO 3) fulfils a high level of complementarity with the new Cybersecurity Act and its common cybersecurity certification schemes. The technical specifications and procedures for assurance levels of the Cybersecurity Act LoA “High” (penetration testing) substantial (conformity), basic (self-certification) could be formally linked with the LoA of the eIDAS regulation overhaul. Also the need for IoT unique identity from eIDAS ensure consistency with the Cybersecurity Act and the need to cover a broader range of actors on top of persons and companies such as machines, objects, suppliers and IoT devices. Again, the strongest alignment with the Cybersecurity Act is provided by the proposal under Option 3, as it is designed to reduce fragmentation in standards and requirements in a similar way as achieved by the Act in the EU security certification landscape. Alignment between the revised Cyber Security Act is also ensured, irrespective of the differences between three options in so far as it has been proposed to regulate the security requirements applicable to trust services providers within the revised Cyber Security Act deleting Article 19 of the eIDAS Regulation.

As is already the case under the current eIDAS framework[320], the revised eIDAS Regulatory framework will ensure, where feasible, accessibility for persons with disabilities.

Linked to the security aspects of the eIDAS Regulation and the requirements on Trust Service Providers and the security requirements applicable to them, coherence and alignment with the revised Directive on Security of Network and Information Systems have been ensured. According to the revised NIS 2 Directive as proposed, Article 19 of the eIDAS Regulation will be deleted and replaced by the common criteria according to the NIS 2 Directive, also applicable to eIDAS trust service providers.

The draft Digital Market Act has also proposed regulatory measures for gatekeeper that are relevant. Policy Option 1 require online platforms, including platforms, not to discriminate and be interoperable with legal electronic identities notified by Member States, building on

[320] See Article 15 of the eIDAS Regulation

Article 6(f) of the proposed Act. Policy Option 2,will introduce measures to further ensure the protection of personal data building on Article 5(a) of the draft Digital Market Act.

The Single Digital Gateway Regulation (SDGR) has also important touchpoints and is in line with the review of the eIDAS regulation. Its objective is to fully modernise public administrative services and facilitate online access to the information, administrative procedures and assistance services that citizens and businesses need when living or operating in another EU country. A key tenet of SDGR is the once-only principle, whereby EU citizens and businesses can request that an evidence for something asked for by an administration as part of an online procedure is exchanged directly between the administration requesting it and the administration holding the evidence in another Member States. SDGR also requires that more administrative procedures will be available online than at present, to both users in their own country and cross-border users. All three policy options are consistent and provide foundational elements to support the objectives of making the once only principle operational under the Single Digital Gateway. Policy Option 1 and Policy Option 2 support the SDGR in some respect by providing stronger incentives for adoption by private sector providers, which, if effective, would likely help streamline online transactions considerably (given that the bulk of these occur in the private sector). Yet, Policy Option 3 is the most impactful of the three options in supporting the objectives of the Single Digital Gateway regulation by putting the user in control.

In sum, while all policy options are generally coherent with wider objectives and complementary to regulations which are currently adopted or are in the pipeline only Option 3 provides a coherent and comprehensive approach towards data protection and acceptance of an electronic identity. As such, it is the only option that can succeed in providing full consistency with the objectives set forth by the overall strategic guidance of the European Commission.

All three options are also coherent with the European Strategy for Data and the proposed Regulation on European Data Governance[321], providing a framework to support data driven applications in cases when the transmission of personal identity data is required allowing users to be in control and fully anonymised. Re-use of attributes and verification based on data available in official registers held by the public sector covered by policy Option 2 and 3, is also consistent with the Open Data Directive and its charging framework.

Similarly, the three options are coherent and built on the current regime under the EU Anti-money laundering framework[322] to be revised in 2021 and will offer additional flexibility and solutions to allow identification of customers and the transfer of information, which are necessary to comply with the customer due diligence requirements. This will be supported by the measures ranging from the extension of the minimum data-set to the provision of framework for the exchange of specific credentials and attributes defined by the future AML framework.

All options, as far at the delivery of electronic identity and attributes rely on the use of mobile devices, will be coherent with the radio equipment directive and the measures adopted under this directive in order to ensure the protection of privacy, personal data and against fraud.

The revised eIDAS Regulation will provide a framework for the provision of electronic identity and electronic identity services in the EU, on which specific sectors can rely to fulfil

321 See, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN

[322] Directive 2018/843/EU of the European Parliament and of the Council of 30 May 2018 amending Directive 2015/849/EU on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156

sector specific legal requirements, for example related to digital travel documents, digital drivers licences etc.

Similarly, the future proposal is aligned with the objectives of the Regulation 2019/1157 which strengthens the security of ID cards and residence documents. Under this Regulation, Member States are obliged to implement new identity cards with the updated security features by August 2021. Once developed, Member States could upgrade the new identity cards so that they can be notified as eID schemes as defined under the IDAS Regulation.[323]

The future proposal will also contribute to the transformation of the customs domain into a paperless electronic environment in the context of the initiative for developing an EU Single Window environment for customs[324].

It should be also noted that the future proposal will contribute to the European mobility policies by facilitating the legal reporting requirements of the maritime operators set in the context of the European Maritime Single Window environment which will start applying form 15 August 2025.[325] The same goes for the articulation with Regulation on Electronic Freight Transport Information obliging Member States authorities to accept electronic freight information. The Regulation will apply starting from 21 August 2024 and is aligned with the eIDAS Regulation provisions on the electronic documents. eIDAS already contributed to the initiative on digital tools for inland waterway transport (IWT) which embraced the use of trust services in the cross-border transmission of documents.

The European Digital Identity WalletApp will also be able to handle the credentials related to drivers, vehicles and operations required by the EU legal framework in the field of road transport (e.g. digital driving licences / Directive 2006/126/EC). Specifications will be further developed in the context of this framework.

The future initiative could also contribute to the shaping of the future initiatives in the field of social coordination services, such as the development of a European Social Security Passport which could build on the trust anchors offered by the notified identities under eIDAS.

6.4 Proportionality

As regards the proportionality of the intervention, **Options 1, 2 and 3** do not go beyond what is necessary to meet the specific objectives satisfactorily. **Option 1** builds directly on the legal basis underpinning the current eIDAS Regulation, introducing elements designed to improve the implementation of the existing legal framework. It provides a clear contribution to the objectives of improving the functioning of the Digital Single Market through a more effective and harmonised legal framework, intervening on cross-border aspects where the added value of EU action can be clearly demonstrated.

Even if **Option 2** entails more substantial costs for compliance and enforcement **than Option 1**, the costs would likely be outweighed by the significant potential benefits to be reaped in terms of competition and market growth, as well as benefits for citizens and end users. Such benefits stem directly from an increase in cross-border recognition and

[323] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement

[324] On 28 October 2020, the European Commission proposed a new initiative that will make it easier for different authorities involved in goods clearance to exchange electronic information submitted by traders.

[325] European Maritime Single Window environment (EMSWe): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A4407248

acceptance of electronic identity and attribute services, which is a key objective of the revision of eIDAS and would be better supported by this option compared with Option 1 and consistent with the principle of proportionality. Option 2 is also designed to tackle the deficiencies of the current framework and provide a regulated environment for private identification services, creating legal certainty and enforceability of such services that cannot be achieved at the nation level. This includes the risk to data protection, as there is currently no guaranteed separation between identity data and operational data on a level commensurate with the level of assurance provided by the identity service provider and the other services it provides. The additional costs generated by this option are designed to support harmonisation and justified on the expectation that they will reduce administrative burden and compliance costs in the long run. The costs linked to the acceptance in regulated sectors of digital identity authentication attributes can also be regarded as necessary and proportionate as far as it supports the overall objective and provides the means by which regulated sectors can fulfil legal obligations to legally identify a user.

Option 3, building on the relevant measures under Option 1 and 2, is the best aligned option, providing the most appropriate instrument for setting the necessary interoperability structure for the creation of an EU Digital Identity ecosystem building on legal identities issued by Member States and the provision of qualified and non-qualified digital identity attributes. Taking into consideration the set objectives, Option 3 is also considered sufficiently proportionate and the costs likely to be commensurate to the potential benefits. The costs derived from creating and aligning to the new standards (trust service providers and online service providers) cannot be avoided if the objectives of usability and accessibility are to be achieved. Further, there is evidence that a standard-based approach has been used successfully in similar contexts (e.g. with ICAO's standards on travel documents). Option 3, as well as Option 2 have a clear intent to harness the investments already made by Member States. This matches the aspirations and expectations of stakeholders consulted for this study, the majority of whom noted the importance of harnessing the assets and resources that the eIDAS Regulation has already helped create and enhance since 2014.

6.4.1 Summary assessment

The table below summarises our comparison of the three policy options analysed in this study.

Given the diversity of impacts analysed, the symbols are used to grade qualitatively the values reflecting the performance of each option. The grading is based on the balanced assessment of the evidence collected for each assessment criteria. An overview of the grading is provided below.

Qualitative assessment of the impacts	
+++	Very strong positive impact
++	Strong positive impact
+	Moderate positive impact
0	No or limited impact

The qualitative assessment is based on the analysis carried out in the previous sections

Table 5. Summary assessment for each Option

	Effectiveness	Efficiency		Coherence	Proportionality
		Cost/ benefit for businesses	*Cost/ benefit for public sector*		
Option 1	+	--/+	--/+	++	✓
Option 2	+	--/++	--/++	+++	✓
Option 3	+++	--/+++	--/+++	+++	✓

7 CONCLUSIONS

Initial summary conclusions from the study are presented below. This work will be completed and submitted in the Final report.

The section sets out our overall findings on:

- The definition of the problem addressed by the revision of the eIDAS Regulation
- The justification for EU action underpinning the revision
- The definition of objectives of the revisions
- The conclusions on the preferred option(s)

7.1 Problem definition

The core problems addressed by the revision of eIDAS with respect to eID means are as follows:

Increased demand by public and private services for trusted identification and exchange of digital attributes not met (eID)

The eIDAS Regulation focuses on access to cross-border public sector services, and has been able to offer this access only for a limited number of them. However, given its inherent limitation to the public sector, it cannot address growing demands for secure and trusted identification and exchange of attributes for access to ***private services***. In particular, the complexity for online private providers to connect to the system, its insufficient availability in all Member States and its lack of flexibility to support a variety of use cases (see section on drivers) are significant limiting factors. Furthermore, identity solutions provided outside eIDAS by social media providers and other private service providers (such as banks) cannot seamlessly respond to these new market needs as they may not be available to external customers, lack a direct link to trusted and secure eID and/or they do not benefit from cross-border recognition, preventing such solutions from being scalable.

As regards the ***public services***, demand for cross-border access has also grown and evolved due to digitisation and increased mobility (about 30% of EU population travel yearly to another Member State). However, eIDAS focuses mainly in the needs of those EU citizens of working age residing in another EU Member State, which represents in number only around 3% of EU population[326]. Crucially, today many citizens do not even have access to trusted and secure government eID means allowing them to access services across border. Six years after the adoption of eIDAS, the eIDAS framework covers only about half of the EU population , leaving 41% of EU citizens without the possibility to use any trusted and secure eID scheme across borders.Even in those Member States which notified a national eID under eIDAS, substantial barriers to access public online services persist and the number of services connected to the national nodes is considerably smaller than the number of services declared as being accessible via the domestic eID scheme.

In relation to the ***market demand for credentials digitally proving attributes,*** such as medical certificates or professional qualifications, they are currently not covered by eIDAS and as a result, Member States and service providers have been forced to develop proprietary trust and interoperability frameworks to ensure the security of these services and/or their recognition across borders.

[326]https://ec.europa.eu/eurostat/statistics-explained/index.php/EU_citizens_living_in_another_Member_State_-_statistical_overview

Current user expectations for seamless and trusted solutions to identify and share attributes across borders not met (eID)

Users today expect seamless online journeys, mobile applications and single-sign-on solutions that can be used for online services in the public and private sector, covering all use cases for identification ranging from pseudonymous log-on to an online platform to secure identification for e-health or e-banking. Secure online identification and the exchange of attribute credentials is becoming more important as the number of identity-sensitive and personalised services increases. The ability to identify digitally will become an important factor of social inclusion and the provision of digital identity a strategic asset.

New technological solutions are adopted by the public and private sectors that aim to address the evolving needs of citizens and businesses, wuch as digital wallets which allow the user to manage and exchange their own identity-related information, attributes and credentials. Some Member States are moving into this direction, which, unless regulated at EU level, will further increase the disparity between national systems.

Alternative ***digital identification solutions by private providers*****,** not recognised by governments, do exist. However, as mentioned above they only address some private use cases not requiring high level of security. Other more secure solutions offered by private providers lack common frameworks or standards as regards for example, the levels of assurance that they provide. They can therefore not scale up and be recognised across borders for access to public or private services which require a certain level of trust.

Without access to seamless and trusted identity solutions recognised cross border, citizens and businesses will have to rely on solutions that are not linked to their legal identities issued by Member States and are therefore less secure. This contradicts the increasing user demand for a secure digital identity to access all online services in the EU that gives users control over the use of their personal data and allows for the exchange of personal data attributes and credentials.

Data control and security concerns insufficiently addressed by available digital identity solutions (eID)

The **security risks** involved in providing personal data online or in information systems for authentication purposes are significant and increasingly important as more citiens conduct transactions online on a frequent basis. However, neither public nor private offers fully respond to this demand. Existing eIDs under eIDAS are not sufficiently widely usable for identification in the private sector to represent a viable alternative and has inherent limitations to discretional data disclosure for the user. Despite offering a high level of security, they show limitations as regards the principle of **data minimisation**; For example, eIDAS does not support so called ***"zero-knowledge claims"*****.** In addition, identification provided by large online platforms often does not allow for the effective protection of personal data, as evidenced by major data breaches and enforcement actions over the last decade, but is used by service providers given the large market power and customer base of platforms. The general shift towards a more comprehensive identity ecosystem that integrates attributes and credentials, some of them carrying sensitive data such as in the health sector, makes it necessary to develop eID ecosystems that are able to effectively protect personal data and offer full user control.

Unequal Conditions for the Provision of Trust Services and insufficient Scope of the Regulation (Trust services)

Although the evaluation of the eIDAS Regulation concludes that the regulatory framework has successfully established legal certainty on liability, burden of proof, legal effect and international aspects of trust services, it also shows that there is room for improvement

regarding a harmonised application of ***supervisory procedures*** and ***processes for identity proofing***, in particular when these processes are carried out remotely.

In addition, there are national differences in the way the conformity assessment of qualified trust services providers is carried out, which requirements apply and which standards are used. As the eIDAS Regulation does not regulate these aspects, differences in the application of the rules for national supervision between Member States raise challenges regarding a comparable level of trust and security of the services provided and of a common level playing field.

The problems described for the provision of trust services are also linked to the absence of a common governance structure at EU level similar to that of the Cooperation Network for eIDs allowing Member States to jointly address them. In the evaluation, some supervisory authorities noted that the role of FESA[327] should be formalised to address the need of consistent application of eIDAS chapter on trust services in all Member States.

Risks of market barriers have also been identified for ***eArchiving services***. The eIDAS Regulation requires archiving the signatures of electronic documents but does not specify requirements and which standards to use, leading several Member States to develop competing national rules

There is also need for improvement concerning the efficiency of a particular trust service, the provision of ***Qualified Website Authentication Certificates (QWACs)***. Despite the introduction of these certificates by the eIDAS Regulation, web browsers refuse to include them in their root stores and to display them clearly, which makes these certificates unusable for traders and consumers. For websites run by intermediaries or trading companies[328] only QWACs can guarantee identity of the entity behind a website with a high level of assurance. The lack of recognition of QWACs by web-browsers may also conflict with the protection of fundamental rights of consumers as enshrined in articles 12, 101, 102, 114 and 169 of the Treaty on the Functioning of the European Union and with EU Consumer protection legislation, in particular Directive 2005/29/EC[329].

A range of drivers underpins these problems, namely:

- Market, societal and technological developments triggering new user and market needs
- Notification by Member States of eID schemes under eIDAS is voluntary and the process is long and complex
- Not all Member States notified national eID and opened them to the private sector for domestic reasons or for lack of incentives
- Private providers of digital identity attributes are not subject to a harmonised regulatory framework ensuring trust and security cross-border

[327] The Forum of European Supervisory Authorities (FESA) for trust service providers, is a forum open to national bodies responsible for supervision and/or trusted lists in accordance with the eIDAS Regulation. The scope of FESA is to support the cooperation, information and assistance among the members and to facilitate the exchange of views and agreement on good practices: http://www.fesa.eu/

[328] Following the definition of article 1 of the 2011/83/EU Directive on consumers rights.

[329] Directive 2005/29/EC concerning unfair business-to-consumer commercial practices, protecting the right of consumers to know the legal entities they are interacting with, their geographical location to the point that providing misleading/inaccurate information or no information at all on the true identity of the business/trader, amounts to misleading or aggressive commercial practice (and fall just short of consumer fraud).

- Diverse and ineffective conditions for private online service providers cannot rely on trusted and secure eIDs cross-border
- The set of identity data provided by eIDAS is too limited and rigid
- Inconsistent Interpretation, divergent application and lack of acceptance of the eIDAS Regulation in relation to QWACs

Evolution of the problem

Globally, an increase in demand for digital identity solutions is expected, with a predicted annual market growth ranging from 13% to 20% . Users' expectations with regard to control of personal identity data and effective technologies for fraud and identity theft prevention will increase. Continued growth in mobile penetration strengthens the demand for convenient and secure mobile-first platforms and solutions . In the light of these expected trends, a no change scenario for the eIDAS Regulation may continue preventing access by all EU citizens and businesses to a trusted and secure eID that can be used across sectors and borders; undermine the functioning of other EU legislation, such as the Single Digital Gateway Regulation (and the Once-Only Principle in particular); perpetuate market fragmentation; continue to prevent users from being in full control of their identity data; fail to mitigate increasing fraud risks from more pervasive use of IoT devices.

7.2 Justification for EU action

With regard to Option 3, the EU has competence to act in order to address the current hurdles to authentication, since this enables electronic identification in online services (which are inherently cross-border in nature). As such, the proposal to establish European Digital Identity finds its legal basis in:

- The 1992 Maastricht Treaty, as regards EU citizenship. Being able to effectively deploy electronic identification means in online services throughout Europe is supports this fundamental concept
- Article 21 TFEU, as regards the exercise of the freedom of movement of EU citizens, which would be facilitated by the measure

The proposal is also in line with the principles of subsidiarity and EU added value, as domestic action alone would not suffice for the fulfilment of the conclusions adopted by the Council on 9 June and 1-2 October 2020, calling for new proposals for further development of the current framework for cross-border identification and authentication based on the eIDAS Regulation towards a framework for a European Digital Identity. A decision to delay this objective in favour of individual Member State solutions, would, based on the current experience with eIDAS, lead to further fragmentation of the Single Market and encourage forum shopping by trust services providers, leading to unequal offering to the detriment of business opportunities, service offering and user experience. Further, none of the policy proposals included in this initiative impede Member States to recognize their own national e-ID schemes or recognize national trust services, other than those which would be included in the proposed Regulation.

Options 1 and 2 also provide a legitimate legal basis for the EU to act, as follows:

- Option 1 results from the ongoing review of the eIDAS Regulation, which is a regulatory obligation included in article 49 of the Regulation and also falls within the area of shared competence of the EU in accordance with Article 4 (2) (a) and Article 26 TFEU (internal market). The proposal further addresses the proper functioning of the internal market for which the required powers have been conferred to the EU on the basis of Article 114 TFEU (the same legal basis as the current eIDAS Regulation). The EU added value is clear from this initiative, as existing voluntary bilateral or multilateral Member States cooperation have not effectively addressed

gaps and weaknesses that negatively impact the development of the Digital Single Market. The initiative would better support these aims without precluding Member States' ability to use any (notified) e-ID notification schemes by the private sector or to recognize national trust services.

- EU intervention via Option 2 may be legally based on Article 114 TFEU (see above) and Article 16 TFEU on the grounds that person identification data is inherently personal data, and the initiative also aims to increase the level of trust when private digital identity providers would be using person identification data (including by adopting further layers of security & privacy measures, notably data separation and transparency) in an online environment inherently not designed with privacy in mind as well as to promote the free movement of such data. As was the case for Option 3, domestic action alone would not suffice for the fulfilment of the conclusions adopted by the Council on 9 June and 1-2 October 2020. The crucial nature of digital identity services in the enablement of the full potential of the Digital Single Market also requires the adoption of additional safeguards in terms of security and privacy at the EU level.

7.3 Definition of objectives

The key general objective for the revision of eIDAS is to foster the achievement of the Digital Single Market by removing barriers to the free movement of goods, services and persons. This general objective can be broken down into four specific objectives, of which three relate to digital identity and one (Objective 4) to trust services:

- Objective 1: Provide access to trusted and secure digital identity solutions for all EU citizens and businesses cross borders
- Objective 2: Make accessible a wide range of public and private online services relying on trusted and secure digital identity solutions cross border
- Objective 3: Provide citizens full control of their personal data and assure their security when using digital identity solutions
- Objective 4: Strengthen the EU market for trust services

7.4 Preferred option(s)

In the light of our analysis, ***Option 3 stands out as the preferred option***. However, this options can only reach its full potential if it builds on other measures put forward under Options 1 and 2.

Option 3 would establish a comprehensive framework providing users with a personal digital wallet to access public and private online services cross-border. In addition, users would be able to carry-out transactions online by storing and managing identity data and sharing electronic attestations of attributes securely in a wide range of use-cases.

Under the preferred option, the following measures would reach the objectives set:

- Establish a European Digital Identity personal Wallet App ecosystem by:
    - Entrusting Member States or qualified trust service providers to deploy it (Measure 1/PO3 Sub-Options 1 or 2);
    - Setting common standards for the European Digital Identity Wallet with the aim to ensure interoperability with credential issuers (QTSPs under Option 2) and service providers. In addition, reference standards would be required to ensure compliance with the security and functional requirements to be set in the revised Regulation (Measures 2&3/PO3).

- Enable the free flow and exchange of digital identity data across borders and a strong, trusted link between them and the Wallet App by:
    - Extending the scope of the Regulation with a new Qualified Trust Service for the secure exchange of data linked to identity ***(Measure 1/PO2***)
    - Requiring Member States to make available data stored in authentic sources, under the full control of the user, for the secure exchange of data linked to identity (***Measure 2/PO2***). This is a pre-requisite for the provision of attributes and credentials by qualified trust service providers.
    - Setting security requirements and common technical standards for the secure exchange of data linked to identity (***Measure 3/PO2***)
    - Defining the legal effect of digital identity ensuring that digital identity credentials are recognized across borders and are not denied legal effect (***Measure 4/PO2***)
    - Requiring regulated sectors to rely on qualified digital credentials in order to improve the cross-border use of qualified certificates (***Measure 5/PO2***)
    - Strengthening security requirements for mutual recognition (***Measure 5/PO1***) and ensure that components essential for the security of the wallet are certified in line with the state-of-the-art cybersecurity standards
    - Extending the person identification data set recognised cross border ***(option 1, measure 5***) to multiply the opportunities of the users to rely on the wallet (***Measure 5/PO1***)
- Ensure cross-border trustworthiness of the Wallet App by linking it to the eIDs notified by the Member States:
    - Establish an obligation for Member States to offer eIDs and to notify them under eIDAS, facilitated by a streamlined notification procedure (***measure 1/PO1***)
- Ensure data protection and full user control over identity data by:
    - Establishing legal requirements to ensure the protection of personal data (***Measure 6/PO2***) - the rules applicable to the issuers of qualified credentials would guarantee the user-centricity of the wallet and the protection of personal data.
    - Strengthening security requirements for mutual recognition (***Measure 5/PO1***) would ensure that the Wallet App is equipped with the highest level of security to cover online use-cases at all levels of assurance.

Measures 2 & 3 of Option 1 are not retained under the preferred option, as they would cause an unnecessary duplication with the resources needed to establish a standards-based interoperability framework to support the wallet and the cross-border exchange of credentials.

In relation to **trust services**, the measures retained under the preferred option have a similar level of ambition under all options, implying a robust regulatory intervention. They aim to establish a new trust service for eArchiving, to harmonise the certification processes for remote electronic signing and to strengthen the recognition of Qualified Website Authentication Certificates (QWACS).

The preferred option is in line with the **subsidiarity principle**, as in this area the EU Digital Single Market cannot be accomplished by Member States at national level. In particular, Option 3 would lead to a more comprehensive, effective and efficient framework in all areas of intervention of this initiative. It will:

- build on the joint efforts of the public and private sectors to provide EU citizens and businesses with an ecosystem of secure and trustworthy digital identity systems, ensuring harmonisation and universal availability of eID means in the EU. This ecosystem would rest on three pillars: the eIDAS notified national eID schemes, a qualified trust service for the secure exchange of data linked to identity and an EUeID wallet that together ensure universal availability, wide usability of eID means in the EU and user control of personal data.
- provide a common reference framework for trust and security and minimum obligations on service providers to support universal acceptance of eIDs in the EU;
- strengthen user control and privacy, allowing citizens to control the provision and use of identity data based on verifiable credentials issued by Member States.

The preferred option does not go beyond what is necessary to address the identified problems and is **proportionate** to achieving its objectives:

- the preferred option will build on the existing notified eID schemes and the existing role of Member States as supervisory authorities to ensure a high level of trust in line with a commonly agreed framework.
- The preferred option will neither restrict the role of Member States as issuers of verified identifiers nor propose measures affecting the level of assurance for access to online public services in the EU. The approaches to the use and provision of verified identity credentials, attestations and attributes seek to strike a balance between EU regulation and Member States' public policy interests.

The preferred option is considered future proof in so far as it is content and technology agnostic, providing citizens a portable digital identity solution supporting current trends towards more user centric digital identities available on secure and mobile platforms allowing users to prove who they say they are and verify claims in a multitude of cross border use cases. It accommodates the most recent market developments and embeds the most flexible approach available today to integrate trusted and secure eID provided by Member States and identity attributes provided by a potentially unlimited number of providers. In addition, the option is open to future changes in the technological and legal environment as measures are technologically neutral and leave room for joint implementation by means of a common set of technical references and standards agreed with Member States. By building on available industry standards, implementation time would be reduced and innovation friendliness and adaptation to changing needs assured. Review mechanisms will further mitigate the risk that technical references and standards fall behind technological advance.

8 MONITORING ARRANGEMENTS AND INDICATORS

Many of the proposed indicators are output indicators. Are there indicators that are collected already for other legislation or other purposes that could be relevant for this framework too? It might be worthwhile to check this given the considerable coherence challenge of the legislation with many other initiatives (see box 1).

The eIDAS framework is currently monitored through a limited number of available indicators and data sources at the EU level. Official eIDs notified to the Commission are regularly tracked and made publicly available, while the EU trusted list allows monitoring of qualified trust services available across the EU and their providers. Nevertheless, the bulk of monitoring data and evidence that could support robust performance tracking are not currently collected in a systematic manner across the EU. As a result, comprehensive and systematically collected monitoring data in connection to key objectives is often not available at the EU level.

The gaps identified are multiple and should be addressed in the future. Notably, robust EU-wide information is missing on key aspects addressed by the Regulation such as:

- Usage of eID and trust services by end-users for national transactions and international (cross-border) transactions, and by different categories of population
- Services accessible with notified eIDs in the public and private sector

Further, there is currently no official monitoring of the status of each eIDAS nodes, nor compliance check for Member States that do not have a node in production. Another important aspect to be monitored systematically in the future is the volume and type of service providers connected to the eIDAS nodes, which is currently missing.

More generally, the challenges in quantification noted as part of this impact assessment and the evaluation of eIDAS point to the need for a policy intervention capable of strengthening the monitoring of the implementation of eIDAS and ensuring higher data reliability. Specifically, the evaluation recommends that the Cooperation Network could set up a comprehensive central monitoring system covering a set of key indicators agreed among the Member States in order to track stakeholder costs, benefits, and outcomes.

According to the Better Regulation Guidelines Toolbox Tool #63, the monitoring framework should cover the following aspects of the Regulation:

- **Implementation**: Covers changes to the Regulation and adoption of measures that are necessary to enable the implementation of the selected policy measures.
- **Application:** Focuses on the actual changes observed as a result of the realisation of the policy and is closely linked with the specific and operational objectives. Together with the indicators for implementation, these can be used to monitor enforcement and compliance with respect to each policy measure
- **Contextual information,** if applicable: developments not intentionally related to the Regulation, although they are likely to influence it, such as economic growth, use of new technologies or new behavioural patterns.

The table below presents the indicators and data sources proposed.

Table 6. Monitoring Framework: indicators and sources

Monitoring and evaluation aspect and relevant objectives	Indicator	Responsibility for collection	Source(s)/proposed data collection arrangements[330]	Possible underlying measure (if already available)	Baseline
Implementation of adopted changes					

[330] "**Ongoing Monitoring and Evaluation (M&E)"** refers to indicator data that could be collected on an ongoing basis (ie as they are made available), rather than at fixed points in time. "**Annual Survey"** refers to indicator data that could be collected at fixed points in time via a bespoke annual survey of the relevant audiences. **"M&E data collected by NCAs"** refers to indicator data that is collected routinely by National Competent Authorities for supervision/other purposes, which could also be used to track performance of eIDAS across the Member States if gathered in a consistent manner.

Monitoring and evaluation aspect and relevant objectives	Indicator	Responsibility for collection	Source(s)/proposed data collection arrangements[330]	Possible underlying measure (if already available)	Baseline
Extent to which necessary changes have been implemented in line with the adopted measures	Extent to which the changes have been completed by a set date	European Commission	Periodic reports by EC/NCAs		
Implement necessary changes to relevant national systems	Number of Member States that have completed changes to the relevant system by a set date	European Commission and National Competent Authorities (NCA)	Periodic reports by NCAs		
Implement necessary changes to compliance obligations by the regulated entities	Number of regulated entities that have completed changes from new compliance obligations by a set date	European Commission and National Competent Authorities (NCA)	Periodic reports by NCAs		
Application					
Provide access to trusted and secure digital ID means for all EU citizens and businesses	Number of European citizens and businesses issued with notified eID-s and number of issued identity credentials b)Number of European citizens and businesses issued with EU eID-s and number of issued identity credentials	European Commission and National Competent Authorities (NCA)	Annual survey of NCAs to gatherM&E data collected by NCAs on their notified eIDs in a standard format Automated collection via EU Wallet App		

Monitoring and evaluation aspect and relevant objectives	Indicator	Responsibility for collection	Source(s)/proposed data collection arrangements[330]	Possible underlying measure (if already available)	Baseline
Provide access to trusted and secure digital ID means for all EU citizens and businesses	Number of European citizens and businesses actively using notified eID-s and identity credentials (total and by category) Number of European citizens and businesses actively using EU eID-s and identity credentials (total and by category)	European Commission and National Competent Authorities (NCA)	Annual survey of NCAs to gather M&E data collected by NCAs on their notified eIDs in a standard format Automated collection via EU Wallet App		
Make accessible a wide range of public and private online services relying on trusted and secure digital identity solutions cross border	Number of online service providers accepting notified eID-s and identity credentials Number of online service providers accepting EU eID and identity credentials	European Commission	Annual survey of NCAs to gather M&E data collected by NCAs on their notified eIDs in a standard format Automated collection via EU Wallet App		

Monitoring and evaluation aspect and relevant objectives	Indicator	Responsibility for collection	Source(s)/proposed data collection arrangements[330]	Possible underlying measure (if already available)	Baseline
Make accessible a wide range of public and private online services relying on trusted and secure digital identity solutions cross border	Number of online transactions madevia notified eIDs and identity credentials (total and cross-border) Number of online transactions made via EU eID and identity credentials (total and cross-border)	European Commission	Annual survey of NCAs to gather M&E data collected by NCAs on their notified eIDs in a standard format Automated collection via EU Wallet App		
Make accessible a wide range of public and private online services relying on trusted and secure digital identity solutions cross border	Number of providers issuing credentials within the EU Wallet App(	European Commission and National Competent Authorities (NCA)	Automated collection via EU Wallet App		
Contextual information					
Provide access to trusted and secure digital ID means for all EU citizens and businesses	Size of the market for digital identity and trust services	European Commission	Commissioned research on the eID and trust services market in the EU		
Provide access to trusted and secure digital ID means for all EU citizens and businesses	Public procurement expenditure linked to digital identity	European Commission and National Competent Authorities	Annual survey of NCAs		

Monitoring and evaluation aspect and relevant objectives	Indicator	Responsibility for collection	Source(s)/proposed data collection arrangements[330]	Possible underlying measure (if already available)	Baseline
Make accessible a wide range of public and private online services relying on trusted and secure digital identity solutions cross border	Share of businesses providing their services online	European Commission	Eurostat	a) Eurostat: Enterprises making e-sales and turnover from e-sales, EU-27, 2009-2018 (% of enterprises % of total turnover) b)Eurostat: Enterprises with e-commerce sales of at least 1% of turnover	a)2018: 20% of enterprises b)2020: 18% of enterprises
Make accessible a wide range of public and private online services relying on trusted and secure digital identity solutions cross border	Share of online transactions rrelying on eID (total)	European Commission	Baseline research on the eID and trust services market		

Monitoring and evaluation aspect and relevant objectives	Indicator	Responsibility for collection	Source(s)/proposed data collection arrangements[330]	Possible underlying measure (if already available)	Baseline
Provide access to trusted and secure digital ID means for all EU citizens and businesses	Share of EU citizens using online private and public services (total and cross-border)	European Commission	Eurostat	a)Eurostat: Individuals submitting completed forms to public authorities, over the internet, last 12 months b)European Commission: Digital public services for businesses c)European Commission: eGovernment Benchmark key indicators – 1. Cross-border mobility, Key enablers (see method paper or source data file) d)Eurostat: Individuals ordering goods or services online e)Eurostat: Individuals ordering goods or services online, from sellers from other EU countries	a)2019: 43% of individuals b)2019: 88.5 index score c1)2019 - Cross-border mobility: 9% of citizens and 36% of businesses able to access a service from another European country via their national eIDs c2) Key enablers: 57% of eGovernment services that require online identification can be accessed by users via their national eID d)2019: 72% of individuals e) 2019: 24% of individuals

9 ANNEXES

9.1 ANNEX A. Notes on Calculations

In the Cost Benefit Analysis (Chapter 6) quantitative findings are presented. In this annex, we present a detailed description of the data underpinning the calculations, and an explanation on the methods and assumptions that we relied upon.

Calculation for Policy Option 1

Cost of audits for Supervisory Bodies and Qualified Trust Service Providers

No public information exists on the exact costs a Supervisory Body should bear to perform an audit. The team relied on interviews and surveys and several assumptions to compute a reasonable estimate of the SBs annual costs related to audit.

One CAB claimed that the number and cost of audits can be highly differentiated among SBs. Data collected from the interviews and through consultation with experts gave the Team an estimated range of costs borne by a Supervisory Body in performing an audit, which varies between **€20.000 and €50.000 per audit**. This particular figure refers to external audit costs only i.e. it does not include the cost of internal staff time allocated to participating in the audit. Given the width of this range, we assume that it could be applied to all the Supervisory Bodies performing an audit and QTSPs undergoing an audit in the EU.

Total costs for QTSPs due to audits

In order to compute the total annual costs for QTSPs, we applied the following reasoning:

T (Total Costs) = C (Costs of each audit) x N (number of annual audits) X Q (Number of QTSPs in EU Member States)

With regards to *C,* we use the figure explained above, namely a range between **€20.000 and €50.000 per audit.**

With regards to Q, we relied on the published eIDAS Trusted lists[331], giving the precise number of QTSPs per country, as reported in table 1.

With regards to N, number of audits per each QTSPs can widely differ among countries and depends on different variables which can hardly be measured. It is assumed that N is based on two elements:

- (Ni) a **minimum number of audits,** as requested by the eIDAS Regulation;
- (Nii) **additional annual audits** held on average, which should be assumed.

With regards to the minimum number of audits, according to the eIDAS Regulation, each QTSPs should be audited at least once every two years (and therefore, we assume one audit per year per each QTSP). **With regards to the additional number of audits**, we assume that each QTSP undergoes each year an additional number of audits which equals the minimum number of audits prescribed in the regulation.

Thus, the number of total annual audits borne by QTSPs in each Member States can be reasonably estimated as in the following table.

[331] Available at: https://webgate.ec.europa.eu/tl-browser/#/. Consulted on September 2020.

Table 7. Total number of audits undergone by QTSPs per country, per year

COUNTRY	Number of QTSPs	Minimum total number of audits per year	Number of additional audits per year	Total number of audits per year
Austria	4	2	2	4
Belgium	10	5	5	10
Bulgaria	5	3	3	6
Croatia	3	2	2	4
Cyprus	1	1	1	2
Czech Republic	6	3	3	6
Denmark	0	0	0	0
Estonia	2	1	1	2
Finland	1	1	1	2
France	22	11	11	22
Germany	12	6	6	12
Greece	5	3	3	6
Hungary	4	2	2	4
Ireland	2	1	1	2
Italy	21	11	11	22
Latvia	1	1	1	2
Lithuania	4	2	2	4

Luxembourg	2	1	1	2
Malta	2	1	1	2
Netherlands	8	4	4	8
Poland	5	3	3	6
Portugal	6	3	3	6
Romania	5	3	3	6
Slovakia	6	3	3	6
Slovenia	8	4	4	8
Spain	33	17	17	34
Sweden	2	1	1	2

Accordingly, the total costs related to audits (T) estimated annually for QTSPs can be computed as the range between the lower bound being the product of the minimum estimated cost per audit (€ 20.000) multiplied by the total number of audits per year in one country, and the upper bound being the product of the maximum estimated cost per audit (€ 50.000) multiplied by the total number of audits per year in one country. Overall these costs range between €3.6 million and €9 million.

Savings

We assume that for the effect of measure 9, the annual additional audits (Nii) will be reduced by the 20% in each country. This would make EU QTSPs save from audits-related expenditures between €360.000 to €900.000 each year.

Familiarisation costs for Supervisory Bodies and Conformity assessment Bodies

Supervisory bodies

Data collection activities did not give specific indication on the costs supervisory authorities would bear for familiarising with new measures and standards.Therefore, a set of assumptions was made, based on available data and generic evidence gathered through data collection. The team estimated that overall **€315.000** shall be borne by Supervisory Bodies across Europe to familiarise with the new eIDAS regulation, or around **€12.000** by each Supervisory Body.

We estimated these costs uniquely considering the training costs needed to make a sufficient number of employees familiarising with new measures and standards, with the following calculation:

T (training costs in one country) = C (daily costs for trainings) X D (man/days needed for trainings) X N (number of supervisory bodies in one country)

With regards to C, we decided to measure these costs in each country as the average of the daily labour cost per country as given by Eurostat[332], and the estimated daily cost of an expert in charge of training employees as estimated in one interviewee with a national competent authority (i.e. €1000 per day). Final results per each country are provided in the table below.

Table 5. Daily labour costs per country (€)

COUNTRY	Average hourly labour cost (Eurostat, 2016)	Estimated daily labour cost (Eurostat, 2016)	Estimated daily labour costs (interview)	Estimated daily labour costs (final average)
Austria	33,18	265,44	1000	632,72
Belgium	38,61	308,88	1000	654,44
Bulgaria	4,45	35,6	1000	517,8
Croatia	9,55	76,4	1000	538,2
Cyprus	15,69	125,52	1000	562,76
Czechia	10,28	82,24	1000	541,12
Denmark	42,06	336,48	1000	668,24
Estonia	10,81	86,48	1000	543,24
Finland	33,74	269,92	1000	634,96
France	34,90	279,2	1000	639,6
Germany	33,83	270,64	1000	635,32
Greece	15,28	122,24	1000	561,12
Hungary	7,89	63,12	1000	531,56
Ireland	30,76	246,08	1000	623,04
Italy	27,91	223,28	1000	611,64
Latvia	7,66	61,28	1000	530,64
Lithuania	7,44	59,52	1000	529,76

[332] We used the latest estimated hourly labour cost per country in industry, construction and services, as reported by Eurostat (latest update in 2016, consulted in September 2020), assuming a 8-hours working day

COUNTRY	Average hourly labour cost (Eurostat, 2016)	Estimated daily labour cost (Eurostat, 2016)	Estimated daily labour costs (interview)	Estimated daily labour costs (final average)
Luxembourg	38,96	311,68	1000	655,84
Malta	14,21	113,68	1000	556,84
Netherlands	35,09	280,72	1000	640,36
Poland	8,73	69,84	1000	534,92
Portugal	13,66	109,28	1000	554,64
Romania	5,35	42,8	1000	521,4
Slovakia	10,21	81,68	1000	540,84
Slovenia	16,77	134,16	1000	567,08
Spain	21,19	169,52	1000	584,76
Sweden	37,66	301,28	1000	650,64

With regards to D, we assumed a total of 20 man/days as the average duration of trainings for the staff and with regards to S, we considered one Supervisory Body per Member State).

Accordingly, the total training costs for familiarisation for each country (T) is reported below, with the total EU costs and the average cost per country.

Table 6. Estimated total costs for familiarisation per country (€)

COUNTRY	Total training costs for familiarisation
Austria	12.654,40 €
Belgium	13.088,80 €
Bulgaria	10.356,00 €
Croatia	10.764,00 €
Cyprus	11.255,20 €
Czechia	10.822,40 €
Denmark	13.364,80 €
Estonia	10.864,80 €
Finland	12.699,20 €

COUNTRY	Total training costs for familiarisation
France	12.792,00 €
Germany	12.706,40 €
Greece	11.222,40 €
Hungary	10.631,20 €
Ireland	12.460,80 €
Italy	12.232,80 €
Latvia	10.612,80 €
Lithuania	10.595,20 €
Luxembourg	13.116,80 €
Malta	11.136,80 €
Netherlands	12.807,20 €
Poland	10.698,40 €
Portugal	11.092,80 €
Romania	10.428,00 €
Slovakia	10.816,80 €
Slovenia	11.341,60 €
Spain	11.695,20 €
Sweden	13.012,80 €
Total	**315.269,60 €**
Average	**11.676,65 €**

With regards to measure 5, we follow the same computation, assuming a reduction of the 25% in man/days needed to face the small material changes which may be required by the measure.

Conformity assessment bodies (CABs)

With regards to CABs, we assume the same reasoning and use the average training costs for familiarisation computed for Supervisory Bodies (€11.676,65) multiplied by the number of CABs accredited in Europe (29[333]), obtaining a total costs of around €339,000.

[333] Data from August 2020.

Costs of standardised accreditation procedures for Conformity Assessment Bodies (CABs)

No public data is available on the average costs borne by CABs for standardised accreditation procedures. A few stakeholders interviewed and experts consulted underlined that it may vary widely among countries, mainly depending on different guidelines given to accreditation bodies.

In order to compute the overall costs borne by CABs we relied on stakeholders and experts suggestions, publicly available data on CABs and a set of assumptions.

We compute the total costs in each country related to accreditation procedures by using the following reasoning:

Total costs (C) = number of CABs (N) X average costs per procedure (P)

In order to compute N, the study used the official list of accredited CABs[334]. We consider only countries having at least one officially accredited CAB.

In order to compute P, we used the daily labour cost per country as computed in Table 5 above and we consider a range of 5 to 10 man-days needed to complete the procedure, as estimated by stakeholders in interviews.

Assuming that each CAB is involved in the accreditation of one standard per year, the total costs per country would be as in the following table.

COUNTRY	Number of CABs	Total annual costs savings	
		Lower bound (5 man-days)	Upper bound (10 man-days)
Austria	2	6.327,20 €	12.654,40 €
Czech Republic	3	8.116,80 €	16.233,60 €
France	2	6.396,00 €	12.792,00 €
Germany	5	15.883,00 €	31.766,00 €
Italy	7	21.407,40 €	42.814,80 €
Netherlands	1	3.201,80 €	6.403,60 €

Available here: https://ec.europa.eu/futurium/en/system/files/ged/list_of_eidas_accredited_cabs-2020-09-30.pdf. Consulted on August 2020.

Portugal	1	2.773,20 €	5.546,40 €
Slovakia	2	5.408,40 €	10.816,80 €
Slovenia	2	5.670,80 €	11.341,60 €
Spain	4	11.695,20 €	23.390,40 €
Total	**29**	**86.879,80 €**	**173.759,60 €**

Impact of Policy Option 0 – baseline scenario, *Measure 0.4: Harmonise Supervisory Procedures for Trust Services*We consider that the direct benefit of this measure consists in cost savings achieved by CABs in performing accreditation procedures. We expect these savings can reach up to the 20% of total costs borne in each country. overall ranging between € 17,000 and € 35,000 per year.

Costs related to peer-review process for national member of the Cooperation Network

The team relied on data collection activities and a set of assumptions in order to calculate the annual cost borne by CN members in relation to peer review procedures and compute the potential savings related to the introduction of measure 0.3: *simplify and improve the notification and the peer-review procedure*.

We estimate that each Member State (via the Cooperation Network) faces an annual costs for peer review procedures according to the following calculation:

C (average annual costs due to peer reviews)

=

P (average cost per review) X Q (average number of peer reviews per year) X N (number of member States)

The average cost per review (P), is the multiplication between the average man/days needed to conduct a peer review, estimated by stakeholders consulted at 10 man/days, and the daily labour cost for each country (as computed in Table 5 above).

With regards to Q, we consider that, given the number of eID schemes notified or pre-notified since 2017 (year in which the first scheme was pre-notified), at the time of this Study[335] (20 schemes), 7 peer-reviews have been conducted every year in each Member State[336]. Accordingly, we estimated that the total annual costs borne for peer reviews by Member States' authorities is around €1.1. million for the EU 27.

[335] September 2020

[336] Assuming that each Member State will conduct a peer-review on each scheme

Impact of measure 2: simplify and improve the notification and the peer-review procedure.

With regards to the impact of measure 2 (simplify and improve the notification and the peer-review procedure), we assumed based on stakeholder consultation that the impact of the measure could reduce the effort needed for peer review procedures up to 20%.

However, we consider that some one-off training expenditures would be needed to learn the new standardise peer review procedures in the first year of application of the measure, given the following calculation:

S1 (total annual savings in the first year) = 20%C – T (training expenditures)

S2 (total annual savings in the years afterwards) = 20%C

With regards to T, **we decided to use for each country the estimated daily labour costs (final average) as computed in Table 5 above,** multiplied by the average man/days needed to conduct a peer review, estimated by stakeholders consulted at 10 man/days (namely P = T).

Accordingly, total annual savings would result €63.000 in the first year (savings reduced due to T) and around €221.000 per year afterwards.

Overall costs of upgrading the eIDAS infrastructure and updating the technical specifications

In the study we estimate an overall one-off cost of around €6.1 million at the EU level related to upgrading the national eIDAS infrastructures based on new technical specifications. The computation of this cost is based on currently available data and assumptions.

The estimation considered the total cost as the product of (i) the technical costs a Member State has to bear to update an eIDAS node multiplied by (ii) the number of EU Member States having a fully developed node or a node in production:

Total Costs = P (Technical costs of related to the eIDAS node) x Q (27 EU Member States)

With regards to P, the eIDAS evaluation study reports that the average recurrent technical costs affecting eIDAS node operators is €225,000 a year. We took this as a proxy for the cost of an upgrade of the eIDAS nodes following a change in the technical specifications. This is in line with the value of the grants allocated by INEA (Innovation and Networks Executive Agency) to support the cost linked to the set-up and operation of national eIDAS-Nodes (approximately. €200,000 per Member State) and therefore assessed as a broadly accurate and conservative reference for the cost we are seeking to assess.

Taking these estimates as the proxy measure for the average cost of the infrastructural upgrade for each Member State to the new specifications, we obtain an overall cost of around €6.1 million for the EU 27. This is to be considered as a one-off additional cost because we assume that technical specifications will not be changed again over the next 5 years.

Potential revenues for Member States due to the upgraded infrastructure

Commercial models currently adopted at the national level are not publicly available and the landscape is heterogeneous, ranging from Member States providing access to eIDAS node for free to Member States requiring an annual fee together with a transaction fee.

An harmonized commercial model, setting a fixed price for the access of online service providers to eIDAS nodes could provide increased business predictability and revenues for Member States for the next 5 years between €17 million and €53 million (assuming revenue of €0.01 per transaction) and between €797 million and €2.5 billion (assuming revenue of €0.48 per transaction).

The **revenue** was calculated on two variables: (i) **price** online services providers are asked to pay to enter the eIDAS network and (ii) the **volume of transactions passing through the eIDAS nodes**.

(i) Price

Based on desk research findings we compiled a range of prices per transaction that Member States ask to relying parties. Considering both identification-related and sign-related transactions, the minimum price available for transaction amounts at **0,01 €** per transaction and the maximum amounts at **0,48 €**. (see below further explanation on cost elements).

Data gathered online	PRICE (original currency)	Price in € (10.02.2021 exchange rate)				
Swedish BankID						
Identification: 0,2 SEK/transaction.	0.2	0.02				
Sign: 1 SEK/transaction.	1	0.10				
Norwegian BankID						
Identification: 1,49 NOK/transaction.(Source: assently.com)	1		0.10			
Identification: 0,45 - 1,00 NOK/authentication (Source: criipto.com)	0.45					
Sign: 4,90 NOK/transaction.(Source: assently.com)	4.9		0.48			
Sign: 2,90 - 10,00 NOK/transaction.(Source: criipto.com)	2.9					
Danish NemID						
Identification: 1,10 DKK/transaction. .(Source: assently.com)	1.1			0.15		
Sign: 1,10 DKK/transaction. (Source: assently.com)	1.1			0.15		
Finnish Bank eID (TUPAS)						

Identification: 0,20 EUR/transaction. (Source: assently.com)	0.2				0.20		
Sign: 0,20 EUR/transaction. (Source: assently.com)	0.2				0.20		
Finnish Mobile ID (Mobiilivarmenne)							
Identification: 0,09 EUR/transaction. .(Source: assently.com)	0.09				0.09		
Sign: 0,09 EUR/transaction. .(Source: assently.com)	0.09				0.09		
BAIN Report "Customer Loyalty in Retail Banking: Global Edition" 0,1$ (Source: *bain.com*)	0.1					0.08	
SMART-ID (Estonia, Latvia, Lithuania), price packages based on the number of monthly transactions, minimum 0.008€ - maximum 0.1€ (Source: https://www.skidsolutions.eu/en/services/pricelist/smart-id/)	0.008						0.01

(ii) Volume of transactions

The volume of transactions is expected to raise since the first year of implementation of PO1, given an higher number of online service providers connected.

By using the data provided in the eIDAS Evaluation on the number of yearly transactions using eID at domestic level in EU Member States, we estimate that online transactions passing through the eIDAS network amount at 3,8 annual transaction per citizen[337]. Considering that the European population using online services ranges annually between 297.8 million and 451.9 million[338] we estimate that overall annual transactions passing through the eIDAS network in the EU 27 + UK ranges between 1.117 million and 1.694 million.

Revenues increase expected in a 5-years scenario

Assuming the above-mentioned range for the pricing model (lower bound 0,01€ and upper bound at 0,48 €) will remain the same, we investigated two scenarios in which the overall transactions passing through the **eIDAS network increases within a range between 20% and 33% each year, in the next 5 years**. Accordingly, overall increase in revenues for Member States are expected to be as in the following table.

Assuming an yearly increase of transactions passing through the eIDAS network of 20%

[337] Data refer to 2019 transactions per inhabitant for the MSs analysed, removing outliers.

[338] For this estimated we elaborate on EUROSTAT (2019). Lower bound considers only individuals in the EU (27 + UK) using internet banking [isoc_ci_ac_i] while upper bound considers individuals having used internet in the last 12 months [isoc_ci_ifp_iu].

	Year 0 (today, without the measure	Year 1 (after the introduction of the measure)	Year 2	Year 3	Year 4	Year 5
Number of transaction passing through the eIDAS network (units)						
Lower Bound	1.116.800.895	1.340.161.074	1.608.193.289	1.929.831.947	2.315.798.336	2.778.958.004
Upper bound	1.694.456.531	2.033.347.837	2.440.017.404	2.928.020.885	3.513.625.062	4.216.350.075
Cumulative year-on-year increase in revenues (million €)						
With 0,01€/transaction						
Lower bound	-	2.2€	2.7€	3.2€	3.9 €	4.6 €
Upper bound	-	3.4€	4.1€	4.9 €	5.9 €	7 €
With 0,48€/transaction						
Lower bound	-	107.2 €	128.7€	154.4 €	185.3 €	222.3 €
Upper bound	-	162.7€	195.2€	234.2 €	281.1 €	337.3 €

Assuming an yearly increase of transactions passing through the eIDAS network of 33%

	Year 0 (today, without the measure	Year 1 (after the introduction of the measure)	Year 2	Year 3	Year 4	Year 5

Number of transaction passing through the eIDAS network (units)						
Lower Bound	1.116.800.895	1.485.345.191	1.975.509.104	2.627.427.108	3.494.478.054	4.647.655.811
Upper bound	1.694.456.531	2.253.627.186	2.997.324.157	3.986.441.129	5.301.966.702	7.051.615.714
Cumulative year-on-year increase in revenues (million €)						
With 0,01€/transaction						
Lower bound	-	3.9 €	4.9 €	6.5 €	8.7 €	11.5 €
Upper bound	-	5.6 €	7.4 €	9.9 €	13.2 €	17.5 €
With 0,48€/transaction						
Lower bound	-	176.9 €	235.3 €	312.9 €	416.1 €	553.5 €
Upper bound	-	268.4 €	357 €	474.7 €	631.5 €	839.8 €

Increased revenues for Trust services related to the introduction of eArchiving

In our Study we estimated that the creation of e-archiving as a trust service under eIDAS is expected to bring greater awareness of the benefits of this service, likely resulting in more businesses archiving savings from trusted e-archiving solutions. More specifically we estimated that if 1% of EU businesses purchased an electronic archiving solution every year, under conservative assumptions the potential cumulative savings from using this service could amount to over €18 million a year.

This calculation was based on data available online and a set of assumptions. We considered that *increased revenue* could be the result of the product of two variables, namely *cost of trusted* 5GB e-archiving service per year multiplied by the number of EU enterprises, as in the following formula.

R (increased revenue) =
C (cost of trusted 5GB e-archiving service per year)
X
Q (number off EU enterprises)

With regards to C, market prices for e-archiving services are not readily available, except for the service offered by Aruba which costs €25 excl. VAT (€30,5 incl. VAT) for 1GB, 2 document classes, 3 authorized users.[339] Every additional GB costs the same and we assumed that an average business will need a 5GB archive, amounting to a total price of €152 per year (incl. VAT).

With regards to Q, we assume that there will be an increase in demand resulting from the creation of e-archiving as a trust service. In the absence of reliable projections, we calculate the expected revenue for providers in a scenario where an additional 1% of EU businesses (around 244,000[340]) decide to purchase trusted e-archiving services from Trust Service Providers.

Calculations for Policy Option 2

Reduced costs of internal processes involving customer identity verifications

Personal identity data securely shared brings the potential to optimise internal processes and achieve remarkable savings. Four sectors where identity and attributes verification is key were being analysed: transport, financial services, health and eCommerce.

The savings calculation for these sectors are based on public data sources and some methodological assumptions. The table below presents the overall savings for each of the sectors as reported in the study. Afterwards calculations are explained per each sector.

Table 8. Savings in internal processes by sector

Sector	Source of efficiency savings	Potential efficiency savings per year - Lower bound adoption scenario[341]	Potential efficiency savings per year - Upper bound adoption scenario[342]
Financial Services (credit institutions)	(i) More efficient customer onboarding & (ii) reduced cost of KYC/CDD compliance	€0.41 billion – €0.81 billion	€0.68 billion – €1.36 billon

[339] https://www.aruba.it/en/digital-preservation-price-list.aspx

[340] This statistic is extracted from EUROSTAT Annual enterprise statistics by size class for special aggregates of activities (NACE Rev. 2) [sbs_sc_sca_r2].

[341] As described in the paragraph introducing the tables, the range of adoption assumed is between 20% (lower bound) and 33% (upper bound) for the Financial services sector and between 5% and 10% for the other three sectors considered.

[342] As described in the paragraph introducing the tables, the range of adoption assumed is between 20% (lower bound) and 33% (upper bound) for the Financial services sector and between 5% and 10% for the other three sectors considered.

eCommerce	Reduced cost of fraud prevention	€0.24 billion	€0.47 billion
eHealth	Dematerialisation of documents, more streamlined patient identification and more e-delivery	€1.26 billion	€2.51 billion
Aviation	Fewer repetitive traveler identity checks[343], reduced risk of fines and other costs from inaccurate passenger identification	€30 million	€60 million

Aviation sector

In the aviation sector two specific cost savings are expected as a result of Option 2 and Option 3 implementation: 1) more efficient ID verification during checks of passengers 2) avoided fines and repatriation costs thanks to accurate ID verification. For each of the two cost reductions, we computed the savings in two scenarios: a lower bound scenario assuming a 5% of air transport enterprises adopting the measures and an upper bound scenario assuming a 10% of air transport enterprises adopting the measures. The total amounts of these savings are summarised in the table below and detailed afterwards.

Table 9. Savings in internal processes in the aviation sector

Type of cost-savings	Amounts of savings (€)	
	Lower bound (5% of adoption) (€)	Upper bound (10% of adoption) (€)
More efficient ID verification during checks of passengers	€ 29.7 million	€ 59.3 million
Avoided fines and repatriation costs	€ 102.000	€ 205.000
TOTAL	**€ 29.8 million**	**€ 59.5 million**

[343] Figures assume the proportion of passengers subject to repetitive identity checks could be reduced from the current 5% to 10%, based on IATA (2016) Document verification travel trouble https://airlines.iata.org/analysis/document-verification-travel-trouble

Savings from more efficient ID verification during checks of passengers

In order to calculate these savings we relied on the following reasoning:

$$Z = (R_0 - R_1) = \text{Savings from more efficient ID verification during checks of passengers}$$

where

R_1 = *total costs of ID checks in the EU in the aviation sector after the introduction of PO2;*

R_0 = *total costs of ID checks in the EU in the aviation sector before the introduction of the measure (current stage);*

In order to compute the total costs (R), we relied on a mix of international data and assumptions, using the following calculation:

R (Total costs of ID checks in the EU in the aviation sector) =
[P (cost of document check per passenger) X Q (number of EU passengers) X S (% of EU passengers going through standard document checks]

+

[T (cost of in-depth document check per passenger) X Q (number of EU passengers) X U (% of EU passengers going through in-depth document checks]

With regards to Q, the annual number of air passengers in the EU is of 1.1 million[344]. IATA[345] estimates that international travellers typically subject to in-depth document checks (our variable U) accounts for the 10% of total air passengers[346]. Accordingly, passengers going though standard document checks (our variable *S*) can be considered as the 90% of total air passengers[347].

With regards to P, according to IATA data[348], the cost of document checks is $0,5 per passenger. We assume that the cost of more in-depth identity verification checks (our variable T) rises up to $1,5 per passenger.

Given these estimates, the total cost of ID checks in the EU aviation sector amounts at $663.6 million ($R_0$) .

With regards to total savings (Z), we assumed that after the introduction of the option the share of passengers needing in-depth checks (variable *U*) in the EU would be halved, going from 10% to 5% of total passengers per year. Accordingly, R_1 will go

[344] Source: Eurostat (2018). Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php/Air_transport_statistics. Consulted on September 2020

[345] *ibidem*

[346] IATA gives a global estimates, which we consider valid also for the EU level.

[347] *ibidem*

[348] Available at: https://airlines.iata.org/analysis/document-verification-travel-trouble. Consulted on September 2020.

down to $580.7 per year in the EU aviation sector and total savings in the EU aviation sector would amount at $83 million.

Savings

With a total number of air transport enterprises of 6829[349] in EFTA[350] countries, the savings per enterprise would be on average $97.000. In case only the 5% of enterprises were to adopt the measure, the total savings would be $33.2 million, namely €29.7 million[351], while with the 10% of adoption the total savings would be $66.4 million, namely €59.3 million[352].

Savings from avoided fines and repatriation costs

For this estimate we relied on international data and a set of assumptions. The formal calculation is the following reasoning:

C (total annual costs due to fines in the aviation sector)
=
P (average cost of fines per passenger) X Q (number of passengers in the EU found with incorrect ID information resulting in a fine for air transport enterprises)

With regards to P, the study considered international data on fines from IATA[353], estimating the average cost of fines per passenger at $3.500.

With regards to Q, data from IATA[354] estimate the annual number of passengers found globally with incorrect documentation resulting in a fine for airlines at 25.000. We assume that the share of EU passengers is of 26,3%[355], namely 6575.

Based on these estimates, the estimated overall expenditure (C) by EU airlines on fines linked to passengers with incorrect ID information amounts at $23 million.

Savings

With a total number of air transport enterprises of 6829 in EFTA[356] countries, the savings per enterprise would be on average $336. In case only the 5% of enterprises adopt the measure, the total savings would be around €102.734, while with the 10% of adoption the total savings would be around €205.500[357].

---

[349] Estimate based on Eurostat, Business demography by size class (2017 or latest), accessed on 8 August 2020.

[350] For these sectoral calculations, we took the number of enterprises at the EFTA level, since it is expected that they will also be affected by these measures.

[351] Considering a USD - EUR exchange rate of 1,12 as of 9 September 2020.

[352] Considering a USD - EUR exchange rate of 1,12 as of 9 September 2020.

[353] Available at: https://airlines.iata.org/analysis/document-verification-travel-trouble. Consulted on September 2020.

[354] *ibidem*

[355] We estimate that this is equal to the overall Europe's share of global air passengers as provided by ICAO (2018). Available at

https://www.icao.int/annual-report-2018/Pages/the-world-of-air-transport-in-2018.aspx. Consulted on September 2020.

[356] For these sectoral calculations, we took the number of enterprises at the EFTA level, since it is expected that they will also be affected by these measures.

[357] Considering a USD - EUR exchange rate of 1,12 as of 9 September 2020.

Financial services

The estimated benefits linked to the implementation of PO 2 and PO3 in the Financial services sector are related to two categories of cost savings 1) reduced costs of onboarding procedure, 2) reduced costs of wider CDD/KYC procedures. For each of the two cost reductions, we computed the savings in two scenarios: a lower bound scenario with one-fifth of banks adopting the measures and an upper bound scenario with a one-third of banks adopting the measures. Total amounts of these savings are summarised in the table below and detailed afterwards.

Table 10.Savings in internal processes in the financial services sector

Type of cost-savings	Amounts of savings (€)	
	Lower bound (20% of adoption) (€)	Upper bound (30% of adoption) (€)
Reduced costs of onboarding procedures	137 million - 274 million	228 million - 457 million
Reduced costs of wider CDD/KYC procedures	269 million - 538 million	448 million - 896 million
TOTAL	**0,41 billion – 0,81 billion**	**0,68 billion – 1.36 billion**

Reduced costs of onboarding procedures

International data[358] estimate the global spend on customer onboarding in the banking sector at $40 billion per year. The EU market share in the global banking sector amounts to 43%[359], so that the estimated annual expenses on customer identification for EU banks is $17.2 billion.

We estimated savings from more efficient onboarding procedures, assuming that eIDs and attribute services would have a similar streamlining effect as the introduction of LEIs on onboarding. Considering that the average saving on onboarding costs from introduction of LEIs ranges between 5% and 10% of the total spend[360], we estimate that savings from more efficient onboarding can range between $860 million and $1.7 billion per year.

[358]Source: GLEIF, available at https://www.gleif.org/en/lei-solutions/mckinsey-company-and-gleif-leis-and-client-lifecycle-management-in-banking-a-u-s-4-billion-beginning. Consulted on Septemebr 2020.

[359] See at: https://www.lucintel.com/banking-market-2017.aspx

[360] See Footnote 11

Savings:

With a total number of 6498 banks in EFTA[361] countries, the average saving per bank would range on average between $132.000 and $265.000. In case one-third of banks were adopting identity data solutions, total savings would range between €228.5 million and €457 million[362], while with the one-fifth of banks adopting the measure the total savings would be €137 million to €274 million[363].

Reduced costs of wider CDD/KYC procedures

International data[364] estimate the global cost of wider AML compliance in the banking sector at $110 billion per year. The EU market share of global banking amounts at 43%[365], so that the estimated annual spend on AML compliance in European banking sector amounts to $47.3 billion. However, AML compliance includes also onboarding costs. Therefore, by subtracting the current spend on onboarding estimated in the previous section ($17.2 billion) from the total AML compliance costs, we obtained the estimated annual wider compliance costs in the European Banking sector, namely $30.1 billion.

We estimated savings coming from more efficient wider CDD/KYC procedures assuming that private eIDs and attribute services would have a similar streamlining effect as the introduction of LEIs on onboarding. Considering that the average savings on onboarding spend from introduction of LEIs ranges between 5% and 10% of the total spend[366], we estimate that savings from more efficient wider CDD/KYC procedures can range between $1.5 billion and $3 billion per year.

Savings:

With a total number of 6498 banks in EFTA[367] countries, the average savings per bank would range on average between $231.000 and $463.000. In case one-third of banks adopts the measure, total savings can range between €448 million and €896 million[368], while with the one-fifth of banks adopting the measure the total savings would be €269 million to €538[369].

Health sector

[361] For these sectoral calculations, we took the number of enterprises at the EFTA level, since it is expected that they will also be affected by these measures.

[362] We considered a USD - EUR exchange rate of 1,12 as of 9 September 2020.

[363] We considered a USD - EUR exchange rate of 1,12 as of 9 September 2020.

[364]Accenture (2018) Intelligent Automation and Advanced Analytics To Power Financial Crime Compliance. Available at: https://www.accenture.com/_acnmedia/PDF-109/Accenture-Powering-Financial-Crime-Compliance.pdf

[365] See Footnote 12

[366] See Footnote 11

[367] For these sectoral calculations, we took the number of enterprises at the EFTA level, since it is expected that they will also be affected by these measures.

[368] Considering a USD - EUR exchange rate of 1,12 as of 9 September 2020.

[369] Considering a USD - EUR exchange rate of 1,12 as of 9 September 2020.

The Study considers that a benefit for the healthcare sector can derive mainly from increased savings in providing online health services, i.e. paperless data, online interaction, workflow/automation, patient self-care and patient self-service.

According to one report[370] studying the German healthcare sector, these kind of savings can amount to 10% of the total healthcare spend in the country. We considered this percentage as a reasonable proxy valid for all the Member States.

Accordingly, given that the healthcare expenditure in the EU amounts at €1.3 billion[371], savings from digitisation of healthcare services are estimated to allow for savings around €126 million.

In order to compute the overall benefit for the sector, we considered the number of human health activities enterprises in EFTA[372] countries, as given by Eurostat[373], namely 1.956.986. Thus, the average savings per enterprise amounts at € 64.138.

However, it seems reasonable to take into account only those enterprises providing health services online (at least one). Since no official data are available on the share out of total enterprises providing services online, we assume that this share is 20%.

In case the 10% of them adopt the measure, total savings are expected to be around €2.5 billion, while with the 5% of enterprises adopting the measure the total savings would be €1.3 billion.

eCommerce sector

The Study considers that a main benefit in the eCommerce sector can include efficiency effective gains in internal processes directed at fraud prevention.

Considering that the annual total sales for eCommerce sector in Europe are estimated to be around €621 billion[374], and that on average businesses with revenue of over 1 million spend on processes directed at fraud prevention the 7.6% of annual revenue[375] , we can reasonably estimate that the average spend on internal processes directed at fraud prevention peaks around €47.2 billion per year.

---

[370] See at: https://www.mckinsey.com/~/media/McKinsey/Industries/Healthcare%20Systems%20and%20Services/Our%20Insights/Digitizing%20healthcare%20opportunities%20for%20Germany/Digitizing-healthcare-opportunities-for-Germany.pdf

[371] Source: Eurostat, latest data available. See at:

https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Current_healthcare_expenditure,_2017_SPS20.png. Consulted on Spetember 2020.

[372] For these sectoral calculations, we took the number of enterprises at the EFTA level, since it is expected that they will also be affected by these measures.

[373] See at: Business demography by size class (from 2004 onwards, NACE Rev. 2) [bd_9bd_sz_cl_r2], human health activities

[374] Source available at:

https://ecommercenews.eu/ecommerce-in-europe/#:~:text=Ecommerce%20sales%20in%20Europe%20grew,total%20European%20online%20retail%20turnover. Consulted on September 2020.

[375] Javelin Strategy and Research LLC. (2016) The Financial Impact of Fraud. Available at: https://www.javelinstrategy.com/coverage-area/financial-impact-fraud

According to Eurostat data[376], retail enterprises selling online correspond to the 36% of total retail enterprises in EFTA[377] countries, around 1.4 million.

We assume that the 10% of the average expenditure devoted to fraud prevention processes is reduced thanks to the adoption of this measure. Assuming that each enterprise can save the same amount, the average savings per retail enterprises selling online is estimated to be around €3.300 per year. In case the 10% of them adopt the measure, total savings are expected to be around €471 million, while with the 5% of enterprises adopting the measure the total savings would be **€235 million.**

Estimated sectoral savings from reduced fraud

In the report, the following sectoral benefits were estimated with regards to measure of PO2. The savings calculation for these sectors are based on public data sources on fraud related to ID theft and some methodological assumptions. The table below presents the overall savings for each of the sectors as reported in the study[378]. Afterwards calculations are explained per each sector.

Table 11. Savings from reduced fraud by sector

Sector	Potential reduction in fraud losses per year - Lower bound adoption scenario[379]	Potential reduction in fraud losses per year - Upper bound adoption scenario[380]
Financial Services (credit institutions)	€0.85 billion	€1.4 billion
eHealth	€0.3 billion	€0.6 billion
Aviation	€3.5 million	€7 million
eCommerce	€0.13 billion	€0.26 billion

Financial services

[376] See at:

https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200420-1-. Consulted on September 2020.

[377] For these sectoral calculations, we took the number of enterprises at the EFTA level, since it is expected that they will also be affected by these measures.

[378] Figures used in the study reflects only the best-case scenario in which digital ID could prevent up to 40% of consumer identity-related fraud

[379] As described above, the range of adoption assumed is between 20% (lower bound) and 33% (upper bound) for the Financial services sector and between 5% and 10% for the other three sectors considered.

[380] As described above, the range of adoption assumed is between 20% (lower bound) and 33% (upper bound) for the Financial services sector and between 5% and 10% for the other three sectors considered.

Following the estimates of different international reports[381], we estimate that the proportion of credit losses due to ID fraud amounts at 20% of total credit losses. From international data on the banking sector[382] we estimated that the **annual cumulative credit losses for the banking sector** in the period 2017 - 2019 is around **€53.3 billion, resulting in €10.6 billion** of annual credit losses due to ID fraud.

According to McKinsey (2019)[383], digital ID could prevent up to 40% of consumer identity-related fraud. Using this estimated as the best-case scenario, and assuming a worst-case scenario in which only the 10% of fraud is prevented, overall savings from reduced fraud can potentially range savings in the EU financial sector may range between €1.1 billion and €4.3 billion.

With a total number of banks amounting at 6498 in EFTA[384] countries, the average savings per bank would range on average between €164.150 and €656.600. In case one-third of banks adopt the measure, total savings can range between ca. €0.35 billion and €1.4 billion, while with the one-fifth of banks adopting the measure the total savings would be between €0.21 billion and €0.8 billion.

eCommerce sector

According to a report of LexiNexis (2018)[385], the cost of fraud for online merchants amounts on average at the 1.8% of their annual total revenue. According to the same report, the percentage of fraud attributable to ID theft (as self-reported by merchants) amounts at 23% in two years.

Given a total volume of sales for eCommerce in Europe amounting at €621 billion[386], the eCommerce sector in Europe bears an annual cost due to ID-related fraud of €2.57 billion.

Considering that in the EFTA[387] countries 40% of the 1.429.496 retail enterprises selling online, the average cost of fraud per enterprise amounts at. €1798.5. Assuming that these costs, thanks to the measures, will be entirely offset for the 5%

[381] See World Bank (2018), available at: http://documents1.worldbank.org/curated/en/219201522848336907/Private-Sector-Economic-Impacts-from-Identification-Systems.pdf . and McKinsey & Company (2019) available at: https://www.mckinsey.com/business-functions/risk/our-insights/fighting-back-against-synthetic-identity-fraud

[382] See Oliver Wyman (2020). Available at: https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2020/jul/European-Banking-Outlook-2020.pdf. We assume the overall amount is equally distributed in the three years.

[383] See at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.pdf

[384] For these sectoral calculations, we took the number of enterprises at the EFTA level, since it is expected that they will also be affected by these measures.

[385] Available here: https://chargebacks911.com/lexisnexis-true-cost-of-fraud/

[386] Latest data available. See at:

https://ecommercenews.eu/ecommerce-in-europe/#:~:text=Ecommerce%20sales%20in%20Europe%20grew,total%20European%20online%20retail%20turnover.

[387] For these sectoral calculations, we took the number of enterprises at the EFTA level, since it is expected that they will also be affected by these measures.

enterprises selling online, overall savings would be around €0.13 billion, while for the 10% enterprises sectoral overall savings would be of €0.26 billion.

Aviation sector

Considering latest IATA (2016) data available, *payment fraud costs the industry an estimated $858 million annually, approximately $639 million of which is borne by airlines and the remainder by other participants in the travel value chain*[388].

No data is available on the percentage of fraud which is attributable to ID theft. Thus, we assume that the data available for the eCommerce sector[389] can be applied to the aviation sector as well, and amounts at the 23% of the total fraud, namely around $197 million.

According to McKinsey (2019)[390], digital ID could prevent up to 40% of consumer identity-related fraud. Using this estimated as the best-case scenario, and assuming a worst-case scenario in which only the 10% of fraud is prevented, overall savings from reduced fraud can potentially range between $19.7 million and $79 million.

With a total number of enterprises in air transport amounting at 6829 in EFTA[391] countries, the average savings per enterprise would range on average between $3.000 and $11.500. In case 5% of enterprises adopt the measure, total savings can range between ca. €0.9 million and €3.5 million[392], while with the 10% of enterprises adopting the measure the total savings would be between €1.8 million and €7 million[393].

Health sector

According to EUROSMART (2010)[394], the percentage of healthcare expenditure which is lost annually because of fraud ranged in 2010 between 6% and 10%. We assume it is a reasonable estimate to be applied every year and, given a current healthcare expenditure in the EU of €1286 billion[395], we estimate this lost ranging between €77.1 billion and €128.6 billion.

No data is available on the percentage of fraud which is attributable to ID theft. Thus, we assume that the data available for the eCommerce sector[396] can be applied to the health sector as well, and amounts at the 23% of the total fraud.

---

[388] See at: https://www.iata.org/en/pressroom/pr/2016-01-07-01/ . Consulted on September 2020.

[389] Available here: https://chargebacks911.com/lexisnexis-true-cost-of-fraud/

[390] See at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.pdf

[391] For these sectoral calculations, we took the number of enterprises at the EFTA level, since it is expected that they will also be affected by these measures.

[392] Considering a USD - EUR exchange rate of 1,12 as of 9 September 2020.

[393] Considering a USD - EUR exchange rate of 1,12 as of 9 September 2020.

[394] See the report "Understanding and measuring fraud in healthcare" (2010). Available at:

https://www.eurosmart.com/understanding-and-measuring-fraud-in-healthcare/

[395] Latest data available taken from Eurostat (2017). Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Current_healthcare_expenditure,_2017_SPS20.png . Consulted on September 2020.

[396] Available here: https://chargebacks911.com/lexisnexis-true-cost-of-fraud/

According to McKinsey (2019)[397], digital ID could prevent up to 40% of consumer identity-related fraud. Using this estimated as the best-case scenario, and assuming a worst-case scenario in which only the 10% of fraud is prevented, overall savings from reduced fraud can potentially range in the EU health sector between €7 billion and €29,6 billion.

Assuming that only the 20% of human health activities enterprises provides online services, for a total 1.956.986[398] enterprises, the average savings per enterprise would range on average between €3.600 and €15.100. In case 5% of enterprises adopt the measure, total savings can range between ca. €71 million and €296 million, while with the 10% of enterprises adopting the measure the total savings would be between €142 million and €592 million.

Costs of API development

In order to compute the costs of API development, the team relied on quotations from PwC past professional experience in API development to its clients. The costs breakdown is provided in the table below. These costs should be considered as one-off costs. They exclude the costs envisaged for the definition of standards.

In addition a recurring fee for annual maintenance of 25% of total costs should also be considered.

Table 12. One-off costs of API development

	Man/days	Unit price	Cost
Programming/code development	20	1.000 €	20.000 €
Documentation	2	800 €	1.600 €
Prototype and testing	4	800 €	3.200 €
Monitor and alerts time	3	1.000 €	3.000 €
Logging features	2	1.000 €	2.000 €
Testing package for implementation	4	800 €	3.200 €
Total			**29.800 €**

[397] See at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.pdf

[398] Latest, adjusted, data from eurostat, Business demography by size class (from 2004 onwards, NACE Rev. 2) [bd_9bd_sz_cl_r2], human health activities

Technical Integration costs to the API

The integration costs to the API that public organisation should pay for allowing Trust Service Providers access to their authentic sources or for private sectors to rely on TSP services are around € 18,000 to €27,000. The costs items such programming and testing largely depend on the complexity of the platform and explain the variance. The recurrent costs related to annual infrastructure assessment and maintenance costs are expected of 7.000€ yearly

		Lower bound estimate		Upper bound estimate	
	Unit price	Man/days	Cost	Man/days	Cost
Programming/code development	1.000 €	8	8.000 €	12,5	12.500 €
Documentation	800 €	2	1.600 €	4	3.200 €
Prototype and testing	800 €	5	4.000 €	8	6.400 €
Monitor and alerts time	1.000 €	3	3.000 €	3	3.000 €
Logging features	1.000 €	2	2.000 €	2	2.000 €
Testing package for implementation	800 €	4	3.200 €	4	3.200 €
Total		**18.600,00 €**			**27.100,00 €**

Costs linked to the development of technical standards

According to our consultations with experts and based on ETSI standards negotiations in the field of electronic identity, the definition of one technical standard from scratch would require between € 1 million and € 2 million. However, for the development of EUeID standards and SSI standards the cost could be as low as € 150.000 and € 200.000, which is the work of 1 to 2 experts FTE. In fact the costs linked to the development of technical standards heavily depend on two factors:

- Reusability of existing international standards. The higher a new standard can rely on previously defined standards, the lower its cost;
- Effort needed for negotiations with all the stakeholders affected by the standard. In this case, the longer the time needed to negotiate, the higher the costs.

Considered the above, SSI standards for EUeID could cost only € 150.000 to € 200.000. In fact stakeholders consulted during the study considered that SSI standard-related efforts could leverage on the advanced work done by (i) W3C on standards concerning verifiable credentials and Decentralised Identifiers (DID), (ii) ISO CEN-CENELEC and the (iii) Decentralised Identity Foundation. Also experts consulted assumed that the European Commission will have a more active role in

coordinating all organisations working on standards and could liaise with all the affected stakeholders by using the already established European forums on Digital Identity and SSI.

Costs of setting-up an eID scheme for public authorities

Figures on the total investment borne by one country for the implementation of a new eID scheme are based on the national eID schemes developed so far in Europe. However, data collected from the study team reveal very different estimates from country to country: € 40 million - € 60 million borne by the Finnish eID scheme [399], € 72 million expenditures over 3 years in the Netherlands[400], € 100 million estimate for Swedish scheme.

The variance can be explained by the cost elements which are considered in the overall estimate. We limit our estimate to the costs that can be predicted with more certainty, such as 1) human resources and (2) IT infrastructure which are roughly above € 10 million. Integration with legacy systems (3) and Information, Education, Communication (IEC) (4) have not been quantified as they are the most erratic variables affecting the total investments made by public authorities in one country for the full implementation of an eID scheme. They can explain the high variation in costs sustained in different European countries so far.

Given the lack of a standardised measure for the computation of costs implied in the setting-up of an eID scheme, we considered the following cost categories[401]:

1. **Human resources.** The personnel costs for the operational maintenance of a Digital Identity Scheme can be reasonably estimated, on average, as in the following table:

Type of staff needed	Units	Average salary	Total annual cost (FTE)
supervision	12	€ 90.000	€ 1.080.000
architecture	4	€ 120.000	€ 480.000
systems&network administrators	8	€ 80.000	€ 640.000
security	4	€ 120.000	€ 480.000
compliance	4	€ 70.000	€ 280.000

[399] As reported in OIX (2018) Digital Digital Identity in the UK: The cost of doing nothing. Innovate Identity. April

[400] Dutch Report: (2012) Rekenhof - De elektronische identiteitskaart (eID) Toegangssleutel voor de burger tot e-government: (eID) Finnish and Swedish data: collected during interviews.

[401] In line with the international benchmark set by the World Bank (2018). Understanding cost drivers of Identification Systems. World Bank Group. Available at: http://documents1.worldbank.org/curated/en/702641544730830097/pdf/Understanding-Cost-Drivers-of-Identification-Systems.pdf

operational	20	€ 60.000	€ 1.200.000
support	20	€ 60.000	€ 1.200.000
TOTAL			**€ 5.360.000,00**

2. **IT infrastructure.** Costs related to centralised IT systems and hardware to be developed are on average € 5 million for the set-up of a scheme[402];
3. **Integration with legacy systems**. Costs related to integrating a new eID scheme in the different landscapes and context where it can be used are estimated to highly vary depending on countries starting conditions from a technological and administrative point of views[403];
4. **Information, Education, Communication (IEC).** Costs related to trainings needed to adapt to the new scheme, communication and awareness campaign for the citizens etc. are estimated to highly vary depending on countries willingness and availability to invest in these elements.

Considering only cost categories 1 and 2, the total costs of setting up a new scheme can be above € 10 million and can widely increase by adding categories 3 and 4.

Cost to access authentic sources based

The costs that all EU public entities would have to pay in order to enable trust service providers to access their authentic sources is estimated at € 625 million for the one-off integration costs and €162 million for the recurring costs. The formal calculation is the following:

***B** (overall yearly cost to enable access to authentic sources)*

=

*[**P** (one-off integration costs to the API) X **Q** (# of public entities affected by the measure)]*

+

*[**O** (recurring costs) X **Q** (# of public entities affected by the measure)]*

[402] The figure is based on the Deloitte evaluation report.

[403] eIDAS-related costs were not considered since already estimated in the eIDAS Evaluation Study. It has assessed the eIDAS-related costs for an eID scheme at the national level. On average, the initial costs for the set-up of the scheme amounts at € 750.000, the recurrent administrative costs – namely notification process of eID schemes and IEC – amounts at €135.000 while the recurring technical costs amounts at € 225.000.

The one-off integration costs to the API (**P**) that each public entity is expected to pay is € 27.000[404]. (**Q**) are the 23.120[405] public entities which are affected by measure 2.2 (require member states to make available data stored in authentic sources) and are expected to become data providers. There are considerable uncertainties around the total number of organisations in Member states that will have to connect their IT systems through API. As indicated in the Single Digital Gateway cost assessment study[406], it is unknown at which level organisations hold data linked to identity or whether multiple data providers use the same system or database. Additionally, in some cases it is unclear whether or not they are lawfully issued in an electronic format. This explains the large variation between the lower bound estimates of 2.440[407] public entities data providers and upper bound estimates of 114.455[408].

The recurrent costs for each public entity data provider (**O**) is expected to be around € 7.000 yearly[409]. This includes:

- Infrastructure assessment (annual) to proof the compliance with the conditions imposed to be connected to the EUeID ecosystem
- Maintenance cost - 25% from the value of the software/licenses.

In order to compute the overall recurring costs for all EU public entities data providers across Europe the recurring costs were multiplied by (**Q**).

Lower bound and upper bound estimates

Given the uncertainty about the number of public entities that would be impacted we project the results of the overall one off integration costs and the overall recurring costs to (i) lower bound estimate of # of public entities; (ii) point estimate; (iii) upper bound estimate.

[404] Refer to Annex A note on data and calculation of costs and benefits, Policy Option 2: "Costs of API development". The expected integration costs to the API range from € 18.000 to € 27.000. Given the expected complexity of integration with public entities legacy system, for the calculation on cost to access authentic sources we take into account the estimated upper bound (€ 27.000).

[405] Deloitte - Final Report Study and analysis on the readiness of Member States to connect to and exchange data in accordance with Article 14 of the Single Digital Gateway and the Once Only Technical Infrastructure.

[406] As above.

[407] As above.

[408] As above.

[409] These estimates are based on PwC professional experience in these activities.

	Lower bound estimate	Point Estimate	Upper bound estimate
Data providers	2.440	23.120	114.455
One-off integration costs	Around € 66 million	Around € 625 million	Around € 3.090 million
Recurrent costs	Around € 17 million	Around € 162 million	Around € 800 million

Caveats

The cost assessment is limited to a scenario entailing a reduced set of data entries that were taken from the cost assessment study of the Single Digital Gateway Regulation[410] which can be used as a proxy for assessing the number of potential data providers. While the focus of the SDGR cost assessment study is on the procedures it is still relevant for the appraisal of the number of organisations that are expected to develop API-led Service Oriented Architecture. The elements taken into account are:

- Birth/Marriage/Divorce certificates
- commonly held evidence and procedures at University level
- Vocational qualification and vocational qualification supplement
- Certificate of completion of secondary education

The number and typologies of data providers are expected to be much higher and will vary according to the final scope of the regulation and based on the possible market take up and business uses of trust service providers.

Costs of a communication campaign

An EU and national communication campaign would go along with the implementation for both Policy Option 2 and Policy Option 3. In Option 2 the objective would be to raise awareness towards public entities data owners for them to enable trust service providers to access their authentic sources. Concerning Policy Option 3 the campaign would instead aim at the wide take up of the Wallet App solution. In both cases, communication activities are assumed to be carried out by the European Commission and by Member States. The overall estimate of the communication strategy, including both the EU level and the national level, is of € 8.400.000 targeting an audience of 23.120[411] administrations as well as EU citizens.

[410] Deloitte - Final Report Study and analysis on the readiness of Member States to connect to and exchange data in accordance with Article 14 of the Single Digital Gateway and the Once Only Technical Infrastructure

[411] Refer to Annex A note on data and calculation of costs and benefits, Policy Option 2: "Cost to access authentic sources".

This overall estimate has been calculated as the sum of the costs borne to run a communication campaign plus the costs borne to run one campaign in each country, namely:

***B** Costs of a communication campaign*

=

*[**Q** (Costs of National level communication campaign) X **(27** EU member states)]*

+

***R** (Costs of EU level communication campaign)*

To estimate the costs of national level communication campaign (**Q**), the team relied on figures from three PwC advisory projects to Italian public administrations targeting nation-wide communication campaign of similar nature. The three projects revealed expenses of around €300.000 for the design and implementation of communication activities according to the following professional fees breakdown:

Professional figures involved	Man/days	Total Costs per country
10% project management, 20% subject matter experts 45% communication experts, 25% web designers	1.500 man days	€ 300.000

For the European level (**R**), in order to compute these costs, the study team relied on a proxy figure given by the annual budget of the CEF eID of the 2012-2020 setting at € 300.000 € the expenses related to stakeholder management and communication[412]. This includes:

- Contribution to the maintenance of the CEF Digital web portal
- Organisation of events / webinars
- Production of news items and success stories
- Online community management

Calculation for Policy Option 3

A series of calculations which are relevant for PO3 can be found in previous calculation from PO1 and PO2 section. Namely:

[412] PwC professional work carried out for DG DIGIT as part of CEF eID project

- Reduced costs due to fraud
- IT integration costs
- benefit for conformity assessment bodies (additional revenues)
- costs of qualification of the WalletApp providers
- cost of additional supervision
- cost of familiarisation

The calculation which is specific to PO3 is the cost to develop a mobile Wallet application.

Cost to develop a mobile Wallet application

The following assessment by the European Commission could be the basis for a rough estimate:

A permanent staff of 25-30 full-time employees (for any area, at least 5 employees are required to ensure continuity of operations). The start of operations will require more investments into tools and system components, like test suites, app developments and the system test environment, while maintenance is of course lower.

In effect, in total about 10 m € could be assumed for the two years 2021/23 including specification & development, roll out and maintenance. Below is a conservative breakdown of costs[413].

Table 13. Costs to develop a mobile application: conservative breakdowns

	2021		2022		2023	
	Specification & Development		**Dev & Roll out**		**Maintenance**	
Technology Stack	FTEs	Cost	FTEs	Cost	FTE	Cost
Project Management	2	310,000 €	2	310,000 €	1	310,000 €
eID SWAPP	4	620,000 €	4	620.000 €	3	620.000 €
3rd party embedding	2	310.000 €	2	310,000 €	1	155,000 €
EU eID (Q)VCP integration	3	465.000 €	3	465,000 €	1	155,000 €
Service Provider integration	3	465,000 €	3	465,000 €	1	155,000 €
TOTAL		2,170,000 €		2,170,000 €		1,085,000 €

[413] Expected Average Cost by FTE : 155.000 EUR

EU_eID Support Services	FTEs	Cost	FTEs	Cost	FTE	Cost
Project Management	1	155,000 €	1	155,000 €	1	155,000 €
Service Desk	0.5	77,500 €	2	310,000 €	2	310,000 €
Risk& Security management	1	155,000 €				
Interoperability testing (incl. Test system)	0.5	77,500 €	3	465,000 €	2	310,000 €
Community Building Service (Stakeholder management)	2	310,000 €	3	465,000 €	2	310,000 €
Specifications team	0.5	77,500 €	1	155,000 €	3	465,000 €
Incident response	0	0 €	2	310,000 €	1	155,000 €
Training services	0	0 €	2	310,000 €	1	155,000 €
TOTAL		852,500 €		2,170,000€		1,860,000 €
Business Development	FTEs	Cost	FTEs	Cost	FTE	Cost
Project Management and Overall Coordination	1	155,000 €	1	155,000 €	1	155,000 €
Operations income	1	155,000 €	0.5	77,500 €	0.5	77,500 €
Budgeting & Accounting	0.5	77,500 €	1	155,000 €	1	155,000 €
Legal (SLAs, contracts etc.)	0.5	77,500 €	0.5	77,500 €	0.5	77,500 €
TOTAL		465,000 €		465,000 €		465,000 €
Total		**3,487,500 €**		**4,805,000 €**		**2,201,000 €**

The cost above is a rough estimate for the first-time development of such an app. If developed libraries would be provided to other wallet providers, their development and maintenance cost could be reduced.

9.2 ANNEX B. Methodology

The study is based on a mixed method of both quantitative and qualitative analytical techniques supported by multiple data collection exercises. To gather evidence and assess costs and benefits of the different policy options the team relied on a triangulation of findings methodology entailing desk research, interviews and surveys. The way the activities were interconnected is chalked out in the overall approach below. Afterwards the specific approach and statistics results from data collection are set out.

- **Task 1** covered initial scoping activities that were based on literature review, policy interviews with high-level staff of the European Commission and alignment with the team responsible for the *Evaluation study of the eIDAS regulation*. The evidence collected through these channels supported the definition of the rationale for the review of the eIDAS regulation, the definition of the policy objectives, the EU justification to act and description of the policy options.
- **Task 2** entailed different means of data collection. Desk research served the purpose of an initial screening of the sources available and collection of most relevant scientific literature for each of the different elements and measures of the policy options. The team thoroughly reviewed a wide list of legal and policy documents as well as reviewing secondary data to map out the range of costs and benefits of the different policy options (please refer to Annex B: list of sources). It also supported the definition of questionnaires to consult stakeholders through interviews and survey.
- **Task 3** involved an initial identification of the data gaps for an appropriate assessment of the costs and benefits of the different policy options. Accordingly, an additional round of targeted data collection, mainly through interviews and surveys, was carried out with an aim to close as many of the gaps identified as possible.
- In **Task 4** data from different sources collected during the study were analysed and triangulated to build up the evidence for the impact assessment of each policy option. The findings are included in Chapter 5. Afterwards a comparison of options was carried out using a multi-criteria analysis approach to compare the impacts of each policy option according to a number of assessment criteria, in line with the EC Better Regulation Guidelines[414]. The multi-criteria analysis was informed by all data collected, in order to weigh the different types of impacts and trade-offs associated with each policy option and sub-options assessed. The comparison of the different policy options supported the analysis of the effectiveness, efficiency and coherence with regards to the delivery of the objectives.
- In **Task 5** the team drafted a series of conclusions that put into perspective the rationale for the review of the eIDAS regulation and the description of the preferred option with respect to the general, specific and operational objectives for the revision of the eIDAS regulation.

Data collection activities

This section provides an overview of the data collection activities carried out to construct the body of evidence for the impact assessment which are desk research activities and stakeholder consultations.

Desk Research

The literature review covered the analysis of around **100 reports and academic papers published in the field of eIDAS** at national and international level (the full list is available in Annex B). Initially the team screened materials generated from the eIDAS evaluation and wider Commission's work implemented in this field:

- Documentation setting out the Commission's evolving thinking on the proposals being considered for the revision of eIDAS;
- Position papers received by the Commission from key stakeholders;

[414] European Commission. (2017). Better regulation: guidelines and toolbox

- Write-ups from the Commission's interviews with selected personalities (complemented by direct participation of team members in some of the interviews);
- Key documents from the Evaluation study of the eIDAS Regulation (Study no.910/2014, SMART 2019/0046).

After completing the screening of these sources, desk research was extended to a wide range of documents. The policy review was complemented by a review of secondary data sources. The data have been used to quantify the costs and benefits associated to each policy option and sub-option.

Stakeholder consultation

Throughout the study **470 stakeholders** were consulted directly through interviews or by responding to questionnaires.

- **36 stakeholders** were contacted as part of the interview process:
  - **5 high-level policy experts** from the EC;
  - **31 sectoral interviews**, including:
    - 25 interviews with business stakeholders from the eCommerce, health, Financial services, aviation sector;
    - 6 in-depth interviews with subject matter experts of the eID market[415];
- **432 stakeholders** provided input replying to different surveys:
  - 8 members of the Cooperation network provided their input by replying to a targeted survey.
  - 106 stakeholders of the eIDAS ecosystem[416] addressed questions relevant for this Study, integrated into surveys of the *Evaluation study*.
  - 318 stakeholders provided responses as part of the Open Public Consultation.

High level policy interviews

Policy interviews were conducted with high-level EU policy experts with a strategic interest in digital identity. These interviews were used to streamline, where possible, the policy options included in the Terms of Reference and map potential costs and benefits linked to a revision of the eIDAS Regulation[417]. The following high-level experts have been interviwed:

- Slawomir Gorniak, Ioannis Agrafiotis, Evgenia Nikolouzou, ENISA
- Eddy Hartog, DG CNECT, European Commission
- Carlos Gomez Munoz, DG CNECT, European Commission

[415] 3 out of 6 have been interviewed in two different moments. The first interview had a more sectoral perspective, while the second interview had a focus on costs and benefits of Option 3.

[416] I.e. (i) Service providers, (ii) Identity providers, (iii) Technology providers, (iv) Member State representatives, (v) Supervisory Bodies - Conformity Assessment Bodies - Accreditation bodies, (vi) Trust services providers

[417] In addition, the study team participated to a number of interviews with selected personalities organised by the Commission in the context of the evaluation study of eIDAS. This opportunity was used to collect feedback on the three policy options identified by the Commission.

- Joao Rodrigues Frade, DG DIGIT, European Commission
- Andrea Servida, DG CNECT, European Commission

Sectoral and in-depth interviews

The study team conducted also interviews with stakeholders working in four different sectors, namely: financial services; eCommerce; e-Health; aviation. In addition, **four interviews** were conducted with horizontal stakeholders involved in regulation, accreditation and supervision of eID and trust services[418] at the national level and **six in-depth interviews** were conducted with subject-matter experts having an in-depth knowledge of the eID market[419].

The four sectors were selected in close consultation with the European Commission in order to ensure coverage of sectors with strong and diverse customer identification and authentication needs, as well as different levels of adoption of eID and trust services.

The objective of these interviews was to gather evidence on the possible implications of the three policy options and fill relevant gaps. An overview of the people interviewed is provided in the table below, while the full list of interviewees is available in annex C.

Table 14. Number of sectoral interviews conducted

Sector	Number of interviews conducted
Financial service	7
eCommerce	4
eHealth	6
Aviation	4
Horizontal stakeholders	4
Subject matter experts	6
Total	**36**

Surveys

To complement the body of knowledge from desk research and interviews the team designed an ad hoc survey and streamlined additional questions in ongoing parallel surveys. Namely these were:

[418] Chosen from National Competent Authorities, Conformity Assessment Bodies, National Supervisory Bodies, eIDAS node operators.

[419] 3 out of 6 have been interviewed in two different moments, both as sectoral experts and a subject matter experts. The first interview had a more sectoral perspective, while the second interview had a focus on costs and benefits of Option 3.

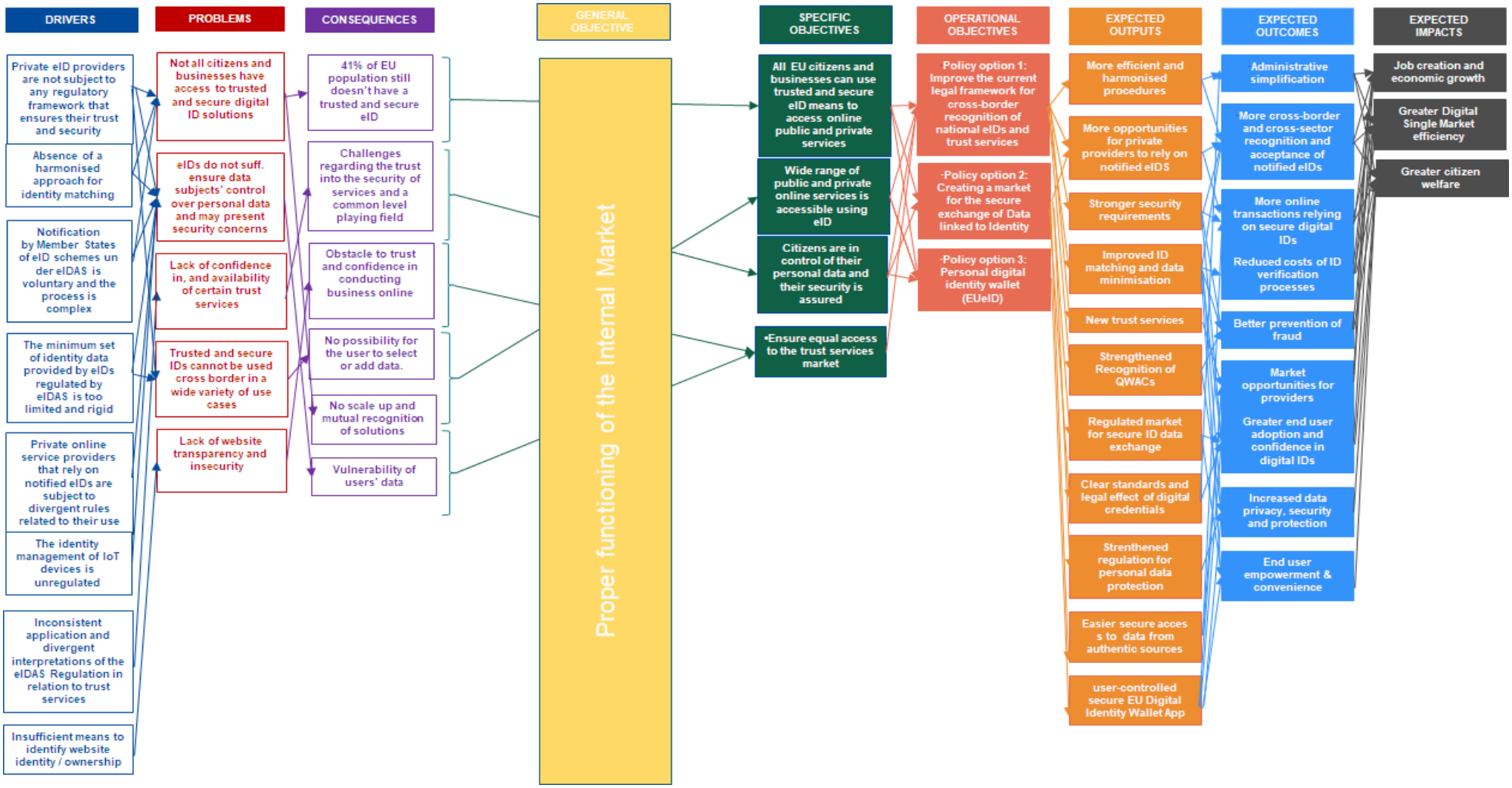
- The Online Public Consultation (OPC), launched on 27 July 2020 and closed on 2 October 2020. A list of four questions and two integrations to existing questions were provided to the Commission on June 24 for incorporation into the OPC questionnaire
- series of questions linked to the possible revision of the eIDAS Regulation were also added to five surveys being conducted in parallel by the team undertaking the study to support the Evaluation of the eIDAS Regulation. The surveys were launched on July 27, together with the OPC, and targeted six stakeholder groups[420].
- At the end of July 2020 the study team launched an online survey for the Cooperation Network. The survey was closed on 15 August 2020, but late responses were reviewed and incorporated into the findings.

[420] i.e. (i) Service providers, (ii) Identity providers, (iii) Technology providers, (iv) Member State representatives, (v) Supervisory Bodies - Conformity Assessment Bodies - Accreditation bodies, (vi) Trust services providers

9.3 ANNEX C. Intervention logic

The intervention logic we set up for the study is presented overleaf

Figure 5. Intervention logic



9.4 ANNEX D. List of sources

Author	Year	Title	Coverage
Academic papers			
European, Mediterranean & Middle Eastern Conference on Information Systems	2015	Creating A European ehealth Space For Cross-Border e-prescription And Patient Summary Services	EU
Urs Gasser and John Palfrey	2007	When and How ICT Interoperability Drives Innovation	Global
Floris Roelofs	2019	Analysis and comparison of identification and authentication systems under the eIDAS regulation	EU
Sandra Wachter	2018	Normative challenges of identification in the Internet of Things: Privacy, profiling,discrimination, and the GDPR	EU
Policy papers			
Accenture	2018	System Initiative on Shaping the Future of Mobility - The Known Traveller Unlocking the potential of digital identity for secure and seamless travel	Global
ATOS Spain and Universitat Jaume I	2018	Feasibility study on cross-border use of eID and Authentication Services (eIDAS compliant) to support student mobility and access to student services in Europe	EU
BBVA	2018	Digital Identity: the current state of affairs	Global
Bryan Richardson and Derek Waldron	2019	Fighting back against synthetic identity fraud, McKinsey & Company	Global
Bruegel (for the EU Parliament)	2019	Contribution to Growth: The European Digital Single Market Delivering economic benefits for citizens and businesses	EU
COCI	2018	Identity in Healthcare	Global
Danish Construction Association	2019	Feedback received on: Secure electronic transactions – application of EU rules. Response by The Danish Construction Association	EU
D-cent	2013	Research on Identity Ecosystem	Global
D-cent	2013	Research on Identity Ecosystem - Decentralised Citizens Engagement Technologies	Global
Deloitte	2016	The use of CEF eID in the CEF eHealth DSI	EU
Deloitte	2018	EIDAS study on pilots for replication of multipliers	8 MS
Deloitte	2019	EIDAS study on pilots for replication of multipliers	8 MS
Deloitte	2018	Study on the opportunities and challenges of eID for Banking	EU
Deloitte	2018	A journey towards smart health: The impact of digitalization on patient experience	Global
Deloitte	2018	BUSINESS PROPOSITION OF EIDAS-BASED EID	EU
Deloitte, Ecorys, VVA, Spark	2020	eIDAS evaluation interim report	EU
DLA Piper et al.	2007	EU Study on the specific policy needs for ICT standardisation	EU
DLA Piper et al.	2013	Feasibility Study on an Electronic Identification, Authentication and Signature Policy (IAS)	EU
ENISA	2019	eIDAS compliant eID Solutions	EU
ENISA	2017	Recommendations for the implementation of trust services	EU
ENISA	2017	eIDAS: Overview on the implementation and uptake of Trust Services One year after the switch over	EU

ENISA	2019	Towards global acceptance of eIDAS audits	EU
European Commission	2017	SSI eIDAS Legal Report How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market	EU
European Commission	2018	The user experience of eIDAS-based eID	EU
European Commission	2019	Assessment of risks and associated mitigating controls, including interoperability of the remote solutions, *European Commission's Expert Sub Working Group 1, Electronic Identification and Remote Know Your Customer processes*	EU
European Commission	2019	Assessing portable kyc/cdd solutions in the banking sector, *European Commission's Expert Sub Working Group 2, Electronic Identification and Remote Know Your Customer processes*	EU
European Commission	2020	Inception impact assessment	EU
European Comimssion	2020	Strategy on Shaping Europe's Digital Future Strategy	
EUROSMART	2019	On the application of eIDAS Regulation	EU
Everis	2018	CEF eID building block for banking and educational domains	EU
Formit	2012	Study on the supply side of EU e-signature market	EU
FESA	2020	Position Paper On the review of the eIDAS Regulation FESA's answer to the European Commission's consultation	EU
Future Trust	2017	Overview of eID Services	Global
Future Trust	2018	Evaluation of eID and Trust Services	Global
Future Trust	2019	Evaluation and Impact Analysis of Pilots	Global
Future Trust	2019	Measurement of Trustworthiness	Global
GSMA	2018	Mobile Connect for Cross-Border Digital Services	EU
GSMA	2018	Mobile Connect for Cross-Border Digital Services Lessons Learned from the eIDAS Pilot	EU
GSMA	2019	Innovative mobile solutions linking health and identity	Global
HEALTHeID	2019	Briefing Document From Business to the Use Case	EU
Infocert	2019	Feedback received on: Secure electronic transactions – application of EU rules. InfoCert Group Contribution to the revision process of the eIDAS Regulation	EU
Intrasoft, TNO Innovation for Life	2012	Study on Impact assessment for legislation on mutual recognition and acceptance of e-Identification and e-Authentication across borders	Global
Javelin Strategy	2016	The Financial Impact of Fraud: Merchants Challenged As E-Commerce Fraud Rises Post-EMV	Global
Joint Action to support the eHealth Network (JASEHN)	2015	Recommendation Paper on Policies Regarding eIDAS eID	EU
McKinsey	2019	Digitizing healthcare – opportunities for Germany	EU country
McKinsey	2019	Digital identification: a key to inclusive growth	Global
McKinsey	2019	GLEIF eBook: LEIs and Client Lifecycle Management in Banking - a U.S.$4 Billion Beginning	Global
MS authorities - Germany	2020	DE Inputs to the eIDAS Review	EU
MS authorities - Luxembourg	2020	Luxembourg position on the review of the eidas regulation	EU
MS authorities - Spain	2020	Spanish proposals for the EIDAS Regulation1 review	EU

MS authorities - Sweden	2020	Swedish Agency for Digital Government's, DIGG's, comments on the eIDAS Regulation	EU
MS authorities - Sweden	2020	Swedish Post and Telecom Authority's standpoint on eIDAS Regulation	EU
Obserwatorium	2019	PAPERLESS BUSINESS Commercialisation of eID and Trust Services in Poland and Europe	EU Country
Open Identity Exchange	2014	The ARPU of Identity	Global
OSE	2019	Cross-border telemedicine: practices and challenges Cross-border telemedicine: practices and challenges	Global
PBQL	2015	International Comparison eID Means	EU
PwC	2018	Study on a marketing plan to stimulate the take-up of eID and trust service for the Digital Single Market	EU
PwC	2018	Study on eID and digital onboarding: mapping and analysis of existing on-boarding bank practices across the EU	EU
PwC	2018	Market study on telemedicine	EU
Sealed	2007	Study of use identification methods in card payments, mobile payments and e-payments (DG MARKT)	EU
Sealed et al.	2007	Study on the standardisation aspects of eSignatures (DG INFSO)	EU
Sealed and Timelex	2009	Study on European Federated Validation Service (EFVS): Feasibility and Global Implementation Plan	EU
Sealed et al.	2010	Study on cross-border interoperability aspects of eSignatures	EU
The EU Blockchain Observatory and Forum	2019	Blockchain and Digital Identity	EU
The Paypers	2019	Web Fraud Prevention, Identity Verification & Authentication Guide 2018-2019	Global
United Nations	2019	Digital Economy Report - Value Creation and Capture: Implications for Developing Economies	Global
University of Oxford	2016	European E-Prescriptions: Benefits and Success Factors	Global
VVA	2018	Cost-Benefits analysis on the introduction of an e-labelling scheme in Europe	EU
WEF/Deloitte	2016	A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity	Global
WHO	2016	From Innovation to Implementation: eHealth in the WHO European Region	Global
World Bank	2016	Digital identity: towards shared principles for public and private sector cooperation	Global
World Economic Forum	2018	Digital Identity On the Threshold of a Digital Identity Revolution	Global
LEPS	2018	Leveraging eID in the Private Sector	EU
Other			
Arthur D Little	2014	Digital signatures: Paving the Way to a Digital Europe	EU
blog.Eidas	2019	Welcome to the Future of Trust	EU
Deloitte	2018	Business proposition of eIDAS-based eID - Aviation Sector	EU
Deloitte	2018	Business proposition of eIDAS-based eID - Banking Sector	EU
Deloitte	2018	Trends in electronic identification: An overview	EU
IATA	2019	One ID - Fact Sheet	Global
IATA	2018	One ID - Concept Paper	Global
IATA	2016	Document verification travel trouble	Global

NCIPHER	2018	The impact of the European eIDAS Regulation Understanding the new requirements and the need for hardware security modules - white paper	EU
PwC	2019	Digital identity - Your key to unlock the digital transformation	EU
Telefonica	2018	Towards a human-centric digitalisation	Global
Signicat	2018	The pros and cons of eIDAS qualified	EU
Ultimaco	2019	An Introduction to the Regulatory Technical Standards for Strong Customer Authentication – Part 3: Achieving Transactional & Account Security	EU
World Economic Forum	2018	Identity in a Digital World A new chapter in the social contract	Global
Katehakis et al.	2017	Security Improvements for Better and Safer Cross-Border ePrescriptionand Patient Summary Services	EU
Stasis et al.	2018	eIDAS - Electronic Identification for Cross Border eHealth	EU

9.5 ANNEX E. Stakeholder consultations

In order to assist the European Commission - DG CNECT in gathering evidence to support the impact assessment for the Digital ID Act, the Study Team collected and analysed the results of three different surveys:

- Cooperation Network Survey;
- Open Public Consultation;
- Deloitte / PwC Survey.

The surveys, used as an alternative tool to the interviews, allow the Team and the European Commission to build additional specific evidence to the results of the literature review and the stakeholders' interviews.

Surveys are either multiple choice or open-ended questions. The questions of the survey were designed in tandem with the interview questions and allowed most of the time for comments (although there were no comments made). In fact, the Team aimed at ensuring to a certain extent a correspondence between questions as to ensure that dataset from the survey and from the interviews can be comparable.

Questions on personal details, although not mandatory, were included in the first part of the surveys in order to be able to differentiate by countries and stakeholders' category.

Considering the three different surveys, we received feedbacks from a total of **432 stakeholders**.

Further, the study team conducted interviews with stakeholders from four key sectors that have been identified as having significant customer identification needs and/or regulatory obligations. In total, **36 stakeholders** were contacted as part of this interview process:

- **5 high-level policy experts** from the EC;
- **31 sectoral interviews**, including:
  - 25 interviews with business stakeholders from the eCommerce, health, Financial services, aviation sector;
  - 6 in-depth interviews with subject matter experts of the eID market[421];

Below, the team provides a detailed analysis of the results obtained from each survey questionnaire and an overall analysis to highlight the main evidences gathered.

Cooperation Network Survey

The Cooperation Network Survey was targeted to Cooperation Network members (henceforth also called members or respondents) with the aim of gathering any initial information retrievable on electronic identity schemes managed by the Member State or mandated to the private sector.

[421] 3 out of 6 have been interviewed in two different moments. The first interview had a more sectoral perspective, while the second interview had a focus on costs and benefits of Option 3.

The Team asked to several EU National Agencies member of the Cooperation Network to also provide a € estimate of:

- one-off adjustment costs[422];
- recurrent costs[423];
- cost savings or other benefits;

These estimates were asked in relation to measures of policy options considered within the impact assessment. Below we report the analysis of the responses obtained from 8 different members of the Cooperation Network on eID.

Further **harmonization through adoption of implementing acts on standards, auditing scheme, conformity assessment reports** and additional guidance to ensure more coherent application of various requirements to be fulfilled by qualified trust services under the eIDAS Regulation (e.g. remote identification, identity proofing) was considered an expensive measure for Cooperation Network members. Adjustment costs result mainly from:

- burying the existing procedures on assessing eID and introducing the new ones;
- the need of several players in the eID scheme to become (qualified) trust service providers;
- Member State often disagree about the requirements making this option very time-consuming and expensive;
- legislative action at national level.
- capital investment;
- skilled personnel;
- integration on other interconnected systems;
- training/education/promotion (workshops, conferences);

Considering only the adjustments costs, one respondent estimates that the work in standardization committees and the adoption of new routines could cost at least 300,000 € and the cost for the initial certification for each private eID providers could be around 1,000,000 €. Another stakeholder involved highlight that in his country, CABs are not established yet (they are currently in the design phase), so new implementing acts would not generate high one-off adjustment costs. The same point goes for auditing schemes and conformity assessment reports. Additional guidance would demand for sure some one-off costs, but they would welcome it.

[422] Adjustment costs are any costs deriving from changes that are necessary for your organization to adapt to the proposed policy intervention on eIDAS. These may include costs related to: capital investment; personnel; systems (IT, network); integration on other, interconnected systems; training/education/promotion; legislative action at national level

[423] Recurrent costs are any costs that will be sustained on an ongoing basis to enforce/comply with the proposed policy intervention on eIDAS

In addition to the adjustment costs, recurrent costs per year to consider are 200,000 € for the work in standardization committees (personnel, attending Cooperation Network working group meetings, training/education/promotion (workshops, conferences) and other 500,000 € for CABs organization.

With regards to these measures, 5 out of 8 respondents do not foresee any cost savings or benefits:

- adhering to alternative procedures or standards is unlikely to create savings;
- some cost savings or benefits would be gained by the CABs, not by the Member States.

Three members claims that clear rules and more transparent regulations across Europe mean less trouble in the certification process by also providing a level playing field for notification: a harmonization of the eIDAS requirements could lead to cost savings of at least 500,000 €.

Regarding the **establishment of a certification at the EU level** as one of the ways to fulfil certain requirements, opinions are mixed. On one hand, this option is considered too costly by MSs that still do not adopt a certification scheme and do not have in place a certification body; adjustments costs should consider at least the need of skilled personnel, the establishment of a certification body and the need of legislative actions at national level. On the other hand, in some countries, certification is already adopted to demonstrate that the requirements of the eIDAS regulation are met; for such cases, this measure would not generate new significant adjustment costs.

Relying on a harmonized, well-functioning certification process (e.g. the common criteria certification scheme being established under the Cyber Act) would contribute to reducing costs and delays related to the lack of commonly agreed assessment methodology of security requirements.

Anyhow, recurrent costs are considered moderate to high. Respondents experience frequent modifications of the eID scheme that would require frequent re-certifications processes.

The respondents are all of the same opinion when considering the possible **extension of the person identification data recognised cross border**: costs would be limited and quantified by one of the respondents with less than 20,000 euros. In this respect, it was highlighted that an extension of the list of attributes is already considered by the eIDAS technical subgroup and will thus not lead to high additional cost; at the same time, based on this experience, some recognised that it might be challenging to reach an agreement on how to standardise the additional attributes. Some costs may arise from the integration of the existing data sources and connection to the eID node, but the estimate would depend on the range and type of attributes covered by the extension.

According to the respondents, regarding benefits and cost savings that could be generated through the implementation of this option, they claimed that:

- for public Service Providers, extending the eIDAS minimum dataset could help to facilitate the ID matching (eIDAS identifier - national identifier) issue when applicable (e.g. by adding a structured 'place of birth' and making it mandatory);
- there might be savings for relying parties in their workflows when needed attributes come with the eID, as well as through higher data quality of these attributes if provided by competent authorities or if not self-declared by applicants;

- a wider applicability of the existing eIDAS framework could be achieved;
- savings and benefits would depend on how this list would be implemented. If in a "once only"-standard-data sharing, workhours could be minimised.

It is equally true that a possible extension of the list of the person identification data recognised cross-border must also consider what is regulated by the GDPR: for private service providers, the existing minimum dataset could already be a problem regarding the principle of minimization / anonymization. Cost savings are however hard to estimate.

Similar to the previous measure, respondents do not foresee significant costs to bear when considering the possibility of **improving the incentives for private sector** to adopt publicly issued eIDs; however, a more precise estimate depend on how the measure is implemented.

The majority of respondents consider as practicable the measure of **enhancing clarity by providing guidance in relation to the LoAs required for specific types of online services.** One-off adjustment costs are mainly represented by the work of analysis to define examples/use cases of digital services who typical needs certain LoA-levels. The economic estimate of such activities could be around 50’000 €.

Harmonization of the understanding regarding the use cases between Member States and more guidance to distinguish LoA 'S' & 'H' would facilitate harmonization of requirements and practices. Clear guidance is always welcome.

Cooperation Network respondents were also asked to provide views on the costs and benefits of a European eID scheme complementary to eIDAS It must be borne in mind that the implementation options that were presented in those surveys were different from the ones considered in the final impact assessment. As a result, the views they provided may not be representative of their position on the EU eID Wallet App proposal as presented in the final impact assessment.

Specifically, respondents were asked to comment on the following implementation scenarios:

- Option 3.1 Aggregate existing national eID schemes – extension of the current eIDAS framework (The sub-option will be an evolution of the current eIDAS framework, it implies maximum diversity of eID means and identity providers)
- Option 3.2 Introduction of a new European eID scheme managed by an EU body (The sub-option will be separated from the current eIDAS framework, it implies limited diversity of eID means, one single identity provider)
- Option 3.3 Introduction of a new European eID scheme managed by a consortium / association (The sub-option will be separated from the current eIDAS framework, it implies limited diversity of eID means, several identity providers (at least one per MS)

According to the opinion of the respondents, **EU Digital Identity as an aggregator of national eID schemes** will require some investments which will depend on the technical standards employed (if the existing eIDAS profile will be used, costs should be compared to the integration of notified MS eIDs). If the current interoperability framework is not completely reused in this context, the design and implementation of a new one as well as the connection of all services to this system will induce significantly higher costs that cannot be approximated at the moment. One

of the main cost-driver will depend on whether data quality and lifecycle management are carried out by the operator of the aggregator. Other adjustment costs to consider are capital investment, skilled personnel, integration on other interconnected systems, training/education/promotion (workshops, conferences).

There are also further obstacles to consider:

- private eID providers may not be interested in hiding behind another brand;
- it has not been demonstrated how or why the private sector might prefer a model where eIDs would be seen as a trust service or how it would make it easier to go through the notification procedure, nor has the desired effect itself of the changed approach been documented;
- it is unclear how it would be easier for a conformity assessment body to complete a review of an eID when national experts from each Member State already participate in the peer-review process;
- it would also likely turn into an audit, as opposed to the current situation, where the peer review builds trust and promotes knowledge sharing across the different Member States, which has long been a valued and protected principle;
- service providers would have to understand the difference between privately issued eIDs and ones issued by Member States in order to adopt appropriate risk profiles for their specific services;
- if the aggregated eID will have the same shortcomings as the underlaying eIDs, it will not solve any problem.

Moreover, one respondent is not favourable to a centrally issued eID and remains a supporter of the idea that each Member State should provide a national eID mean to its citizens, which meets the requirements of Level of Assurance “High”.

Recurrent cost would be represented by some maintenance costs; these however cannot be assessed at this stage.

In case of implementation of this policy option, similar to the integration of Policy Option 2, relying parties may have some cost-saving due to higher eID penetration and, thus, a higher share of electronic processes over conventional processes.

The option related to the **EU Digital Identity as a new scheme at European level, managed by an EU body (3.2)**, entailing a newly created, centrally managed scheme with a single digital identity provider (the EU body responsible for the scheme), is considered the most expensive one. Costs for the implementation of this option would be over 100’000’000 € totally. Recurrent cots could be comparable to maintaining support of a notified eID.

Experience and insights from the work of MSs on the implementation of the eIDAS Regulation over the past years raise concerns regarding the development of a distinct EUid, especially if separated from the eIDAS Regulation. The establishment of a single digital identity provider would most likely be redundant with the digital identity providers already in place at National level, and would most likely negatively impact the return on investments made at national level since the entry into force of the eIDAS Regulation 5 years ago and/or would incur several Member States

in stranded costs. It is necessary to consider that Member States are very different with respect to their implemented eID schemes and the general approach to electronic identification and electronic service provision. Negotiations about an EUid could expose many technical, political, legal and practical uncertainties and challenges as well as challenges to eID-issuance, basic subsidiarity concerns on issuance of identities, general governance and division of responsibilities.

This option is not widely accepted by the stakeholders involved: this solution should be considered just in case the principles for cross boarder eIDs, defined by the eIDAS Regulation, would fail but it will take many years and great investments before it will be of interest within EU.

Despite the very high costs to sustain, there would also be benefits to be considered:

- the new scheme could significantly help some Service Providers who needs to authenticate non-resident foreigners (as far as the scheme is available to that target and could be issued/delivered outside EU)
- the new scheme could be an alternative for Member States who haven't notified its eID scheme.

The third option consider the EU Digital Identity as a new scheme at European level, managed by a consortium/association of public and/or private organizations. Similarly to the previous, the establishment of a new EU Digital ID scheme and the infrastructure needed for interoperability purposes would most likely be redundant with investments made by EU Member States since the entry into force of the eIDAS regulation to establish national eID schemes and their eIDAS nodes. It would likely negatively impact the return on investments already made at national level. Also in this case the costs to be incurred would be a figure of around 100 million €. Recurrent cots could be comparable to maintaining support of a notified eID.

Benefits to consider are the same as the previous option.

Open Public Consultation

The Open Public Consultation[424], distributed online from 24 July to 2 October, aimed to collect feedback on drivers and barriers to the development and uptake of eID and trust services in Europe and on the impacts of the options for delivering an EU digital identity. It targets broad public (e.g. citizens and end-users, including older persons and persons with disabilities) as well as companies directly impacted by the eIDAS Regulation (e.g. trust service providers, identity providers), competent authorities in the Member States, international organisations and concerned stakeholders on the eIDAS framework.

The Open Public Consultation received responses from a total of **318 stakeholders**. The figures below report the overview of the geographical distribution of the countries and the categories to which the respondents belong.

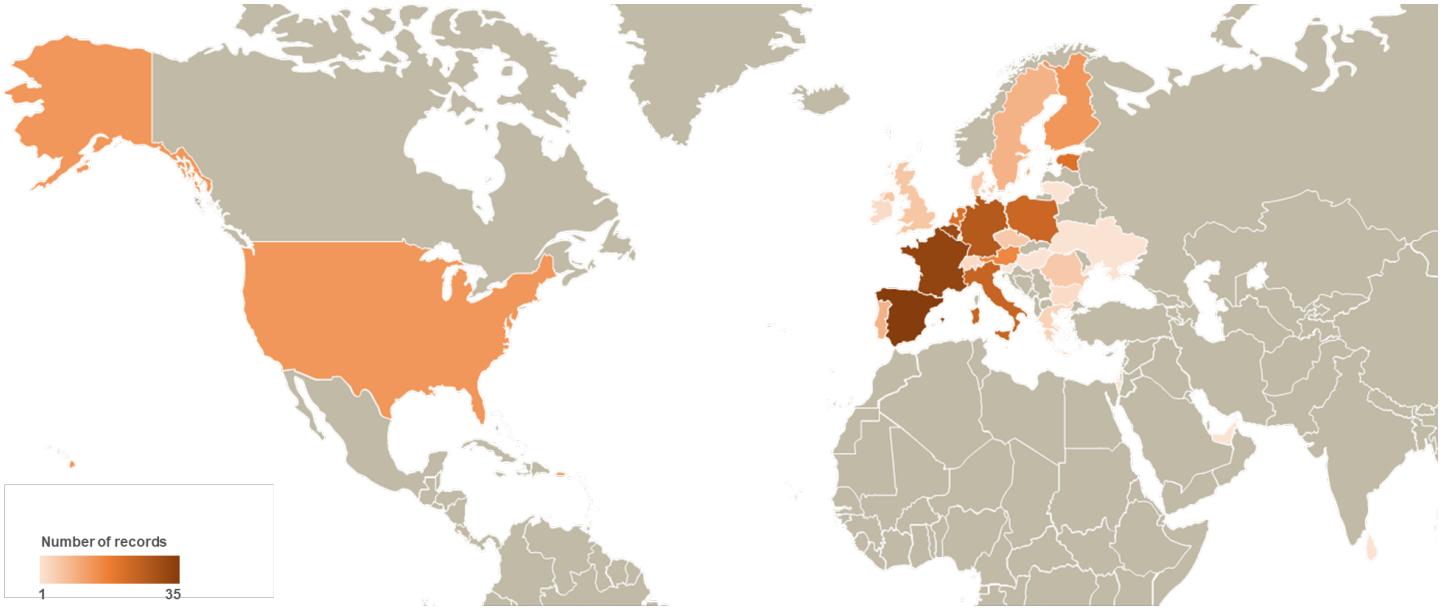


Figure 6 - Geographical distribution of respondents

[424] https://ec.europa.eu/digital-single-market/en/news/eidas-open-public-consultation

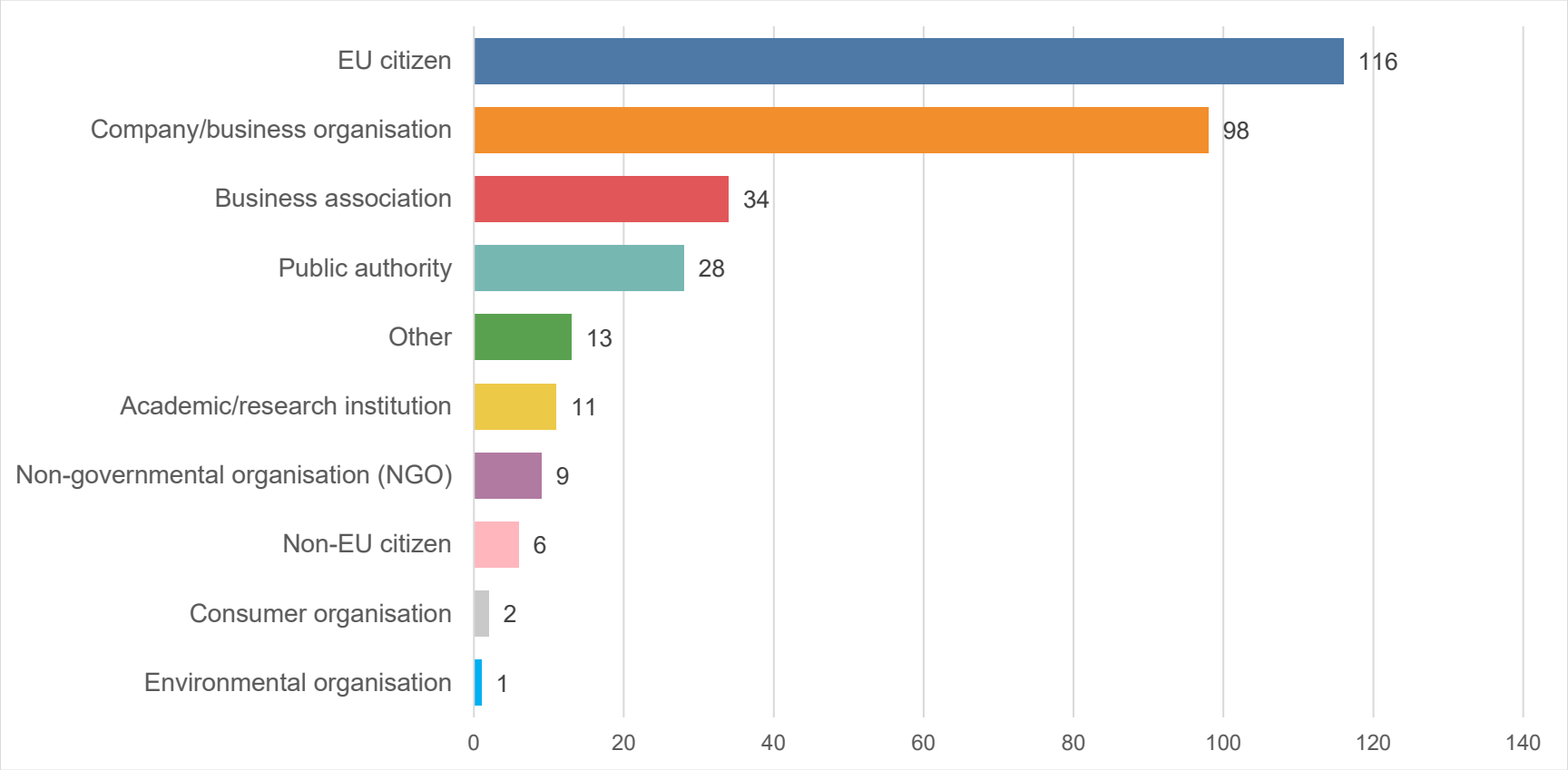


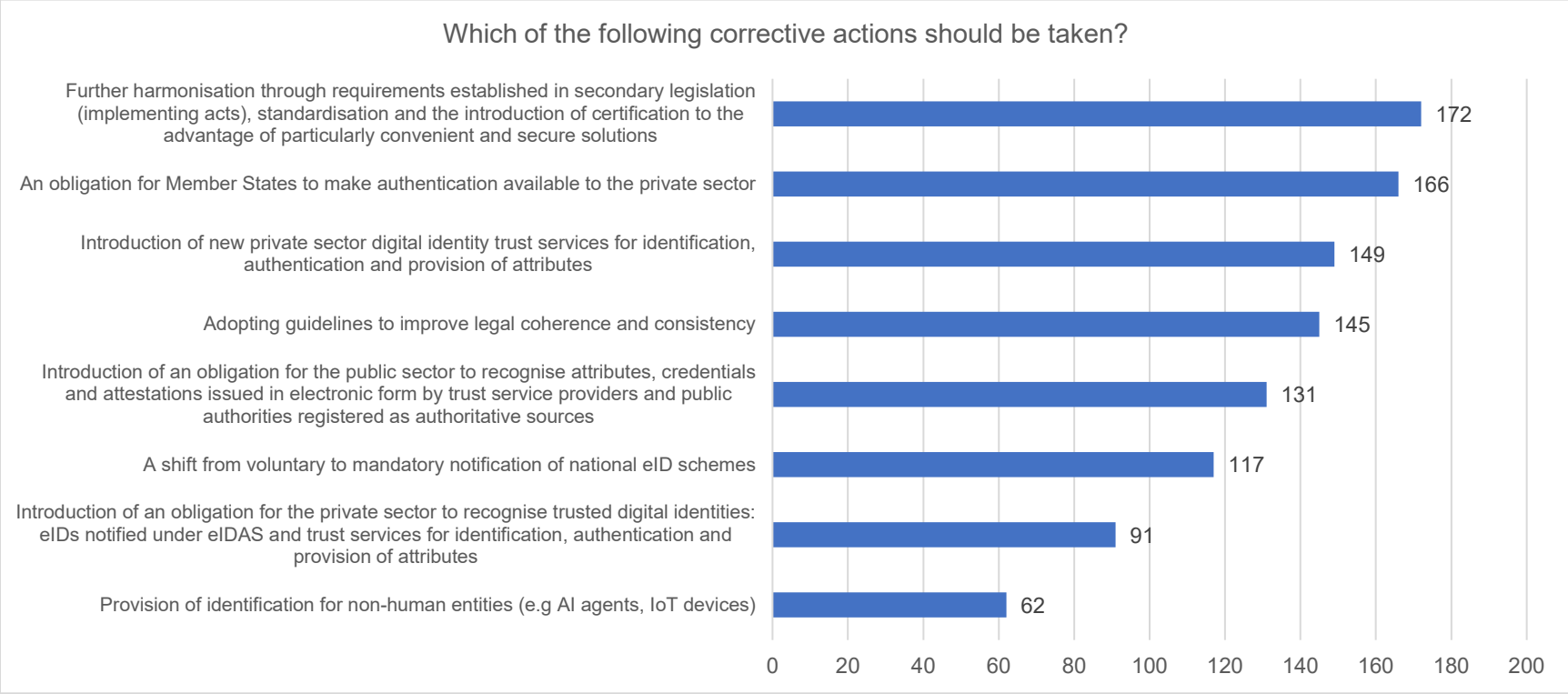
Figure 7 - Stakeholders' categories

The Study Team contributed to the drafting of the questionnaire by inserting some specific questions useful for the elaboration of the impact assessment for the Digital ID Act. The results obtained are reported in the following paragraphs. The first question was intended to understand which **corrective actions should be taken in the context of the revision of eIDAS** to try to overcome the shortcomings of the current eIDAS regulation. Respondents had the possibility to choose **one or more preferences** from the following options:

- adopting guidelines to improve legal coherence and consistency;

- further harmonisation through requirements established in secondary legislation (implementing acts), standardisation and the introduction of certification to the advantage of particularly convenient and secure solutions;
- a shift from voluntary to mandatory notification of national eID schemes;
- an obligation for Member States to make authentication available to the private sector;
- introduction of new private sector digital identity trust services for identification, authentication and provision of attributes;
- introduction of an obligation for the public sector to recognise attributes, credentials and attestations issued in electronic form by trust service providers and public authorities registered as authoritative sources;
- introduction of an obligation for the private sector to recognise trusted digital identities: eIDs notified under eIDAS and trust services for identification, authentication and provision of attributes;
- provision of identification for non-human entities (e.g. AI agents, IoT devices)[425].

[425] For the purpose of this Study, only the most relevant actions were analysed.



81 respondents did not provide any answers to this question. The remaining 237 respondents, who provided one or more answers to the question, considered the actions:

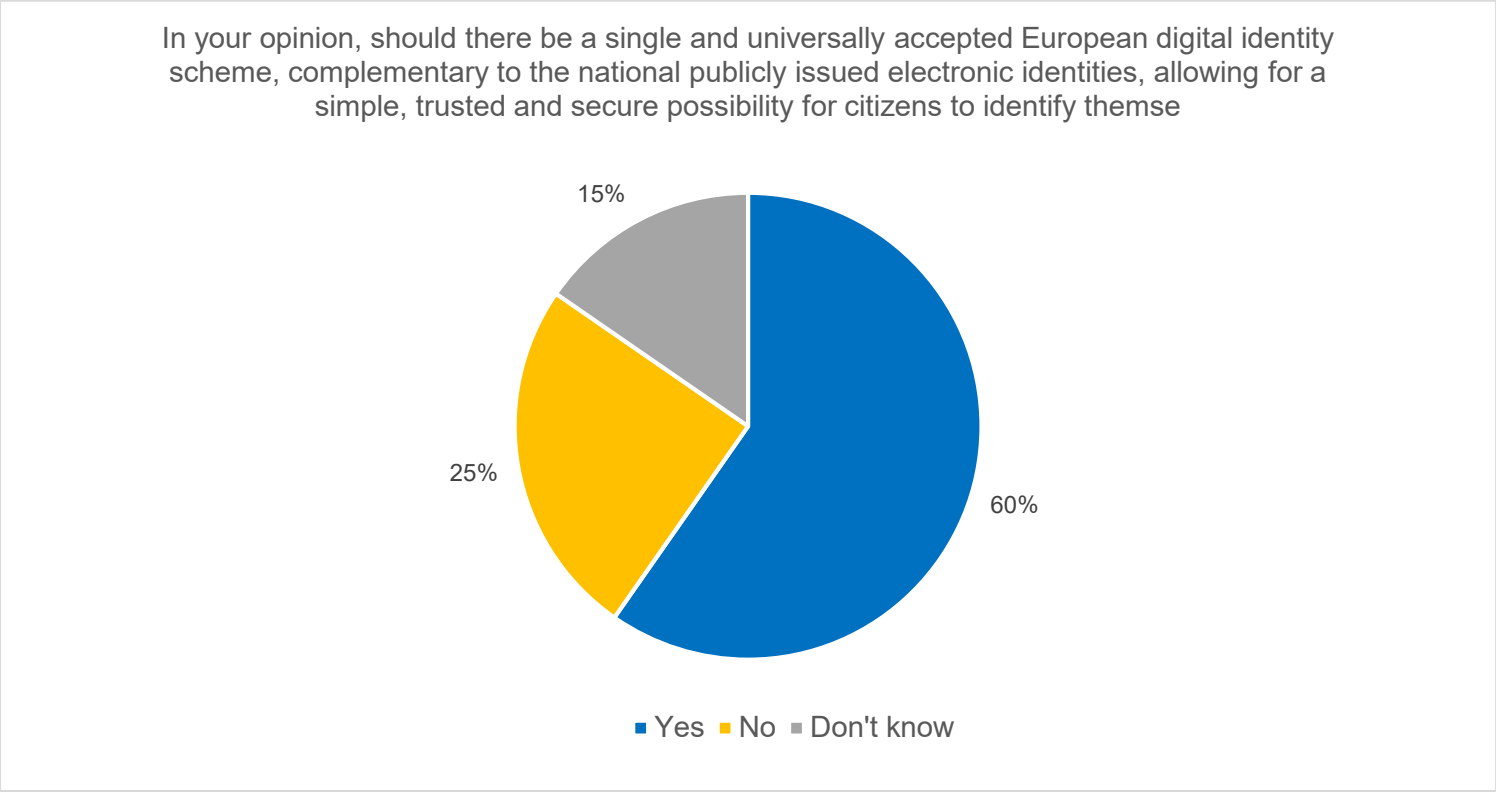
- further harmonisation through requirements established in secondary legislation (implementing acts), standardisation and the introduction of certification to the advantage of particularly convenient and secure solutions;
- an obligation for Member States to make authentication available to the private sector;
- introduction of new private sector digital identity trust services for identification, authentication and provision of attributes,

as the main corrective actions to be taken at EU level to overcome the shortcomings of the current eIDAS regulation. The preferred action, namely “further harmonisation through requirements established in secondary legislation (implementing acts), standardisation

and the introduction of certification to the advantage of particularly convenient and secure solutions", received 172 votes, corresponding to **54% of the total respondents**.

As a second preference, the action who received more votes is "**an obligation for Member States to make authentication available to the private sector".** This corrective action was indicated by **52% of the total respondents.**

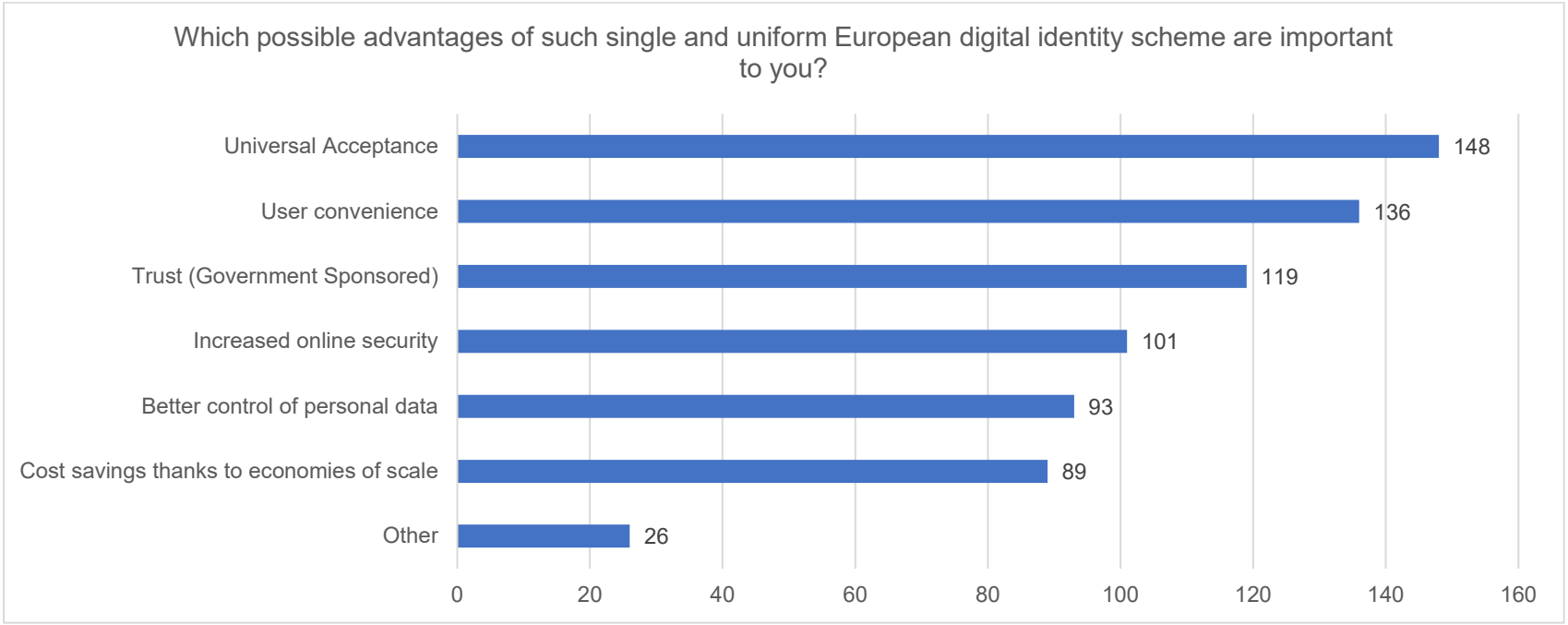
The second question aimed to understand the possible need to create **a single and universally accepted European digital identity scheme**, **complementary to the national publicly issued electronic identities**, allowing for a simple, trusted and secure possibility for citizens to identify themselves online.



A large majority of respondents (**60%**) would welcome the creation of a single and universally accepted European digital identity scheme, complementary to the national publicly issued electronic identities.

The various participants were also asked which **possible advantages of such single and uniform European digital identity scheme are important** to them. Respondents had the possibility to choose **one or more preferences** from the following options:

- trust (Government Sponsored);
- universal Acceptance;
- user convenience;
- better control of personal data,
- increased online security;
- cost savings thanks to economies of scale;
- other.



155 respondents did not provide any answers to this question. The main advantage indicated by the remaining participants is the **universal acceptance (148 votes)** that a single and uniform European digital identity scheme could bring to the EU citizens. The universal acceptance has been indicated as the main advantage by **47% of the total respondents**.

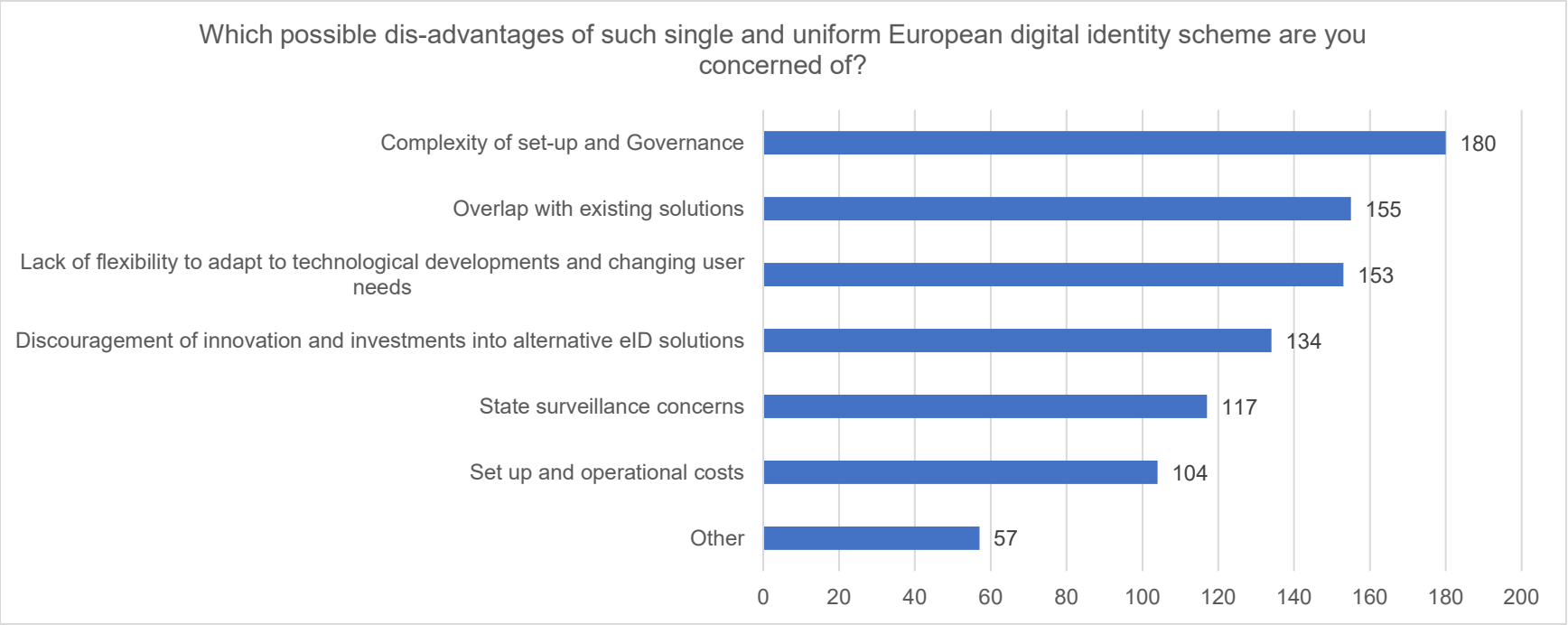
As a second and third possible advantage that were indicated by the participants there are:

- **user convenience**, voted by **43% of the total respondents;**
- **trust (Government Sponsored),** voted by **37% of the total respondents.**

Participants were also asked to indicate which **possible dis-advantages of such single and uniform European digital identity scheme** are to consider. Respondents had the possibility to choose **one or more preferences** from the following options:

- complexity of set-up and Governance;

- lack of flexibility to adapt to technological developments and changing user needs;
- overlap with existing solutions;
- discouragement of innovation and investments into alternative eID solutions;
- state surveillance concerns;
- set up and operational costs;
- other.



35 respondents did not provide any answers to this question. **57% of the respondents** to the Open Public Consultation indicated the **complexity of set-up and Governance** of a single and uniform European digital identity scheme as the main possible dis-advantage.

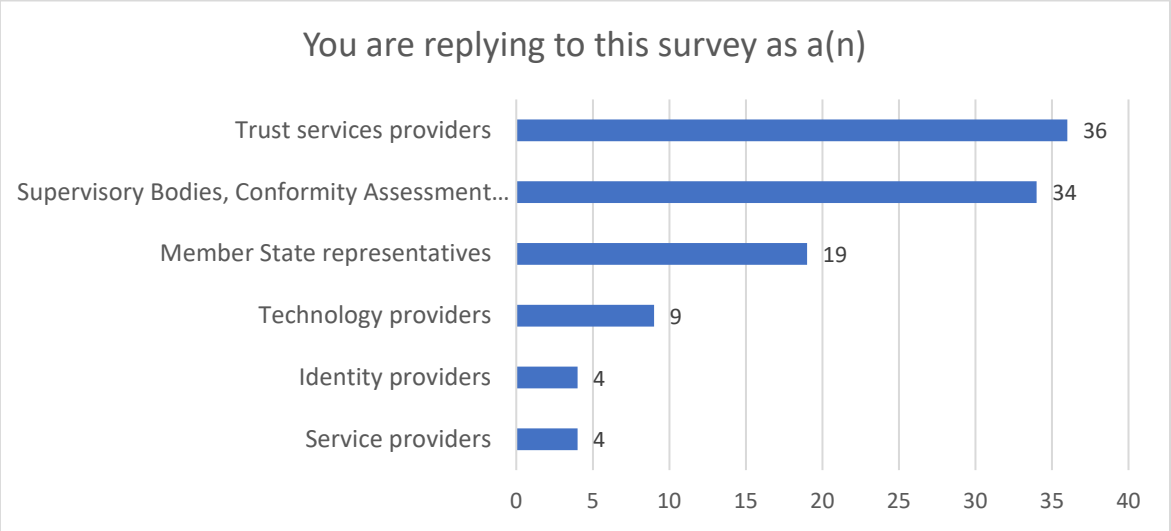
The overlap with existing solutions (**49% of the total respondents**) and the lack of flexibility to adapt to technological developments and changing user needs (**48% of the total respondents**) are also to consider as possible dis-advantages.

Stakeholder Survey (Deloitte / PwC Survey)

In the context of the "eIDAS Review", PwC made a commitment to gather and share data and information to the European Commission - DG CNECT to support the impact assessment for the Digital ID Act.

In pursuit of this goal, PwC drafted questions addressed to different categories of stakeholders to complement findings of other data collection activities. The results have been analysed and reported below.

We received a total of **106 responses** to the survey from the following categories of stakeholders:



Different questions were sent to each stakeholder category based on the most suitable policy options for each specific category. This report includes **13 graphs** and it is divided into 3 sections that analyse the responses obtained to each policy option considered.

Policy Option 1

Under this option, a European Digital Identity would be created in the form of a strengthened legislative framework for national eIDs notified under eIDAS, requiring Member States to make eIDs available to all citizens and companies for cross-border use and improve the effectiveness and efficiency of mutual recognition. The use of national eIDs by private online service providers would be triggered and facilitated through harmonised cost and liability rules, extended data sets and access obligations. All these measures would be taken without extending the regulation scope nor affecting its underlying principles (e.g. applicable to eID solutions notified by Member States, mutual recognition and technological neutrality).

Questions about the Policy Option 1 were targeted to the following stakeholders' categories:

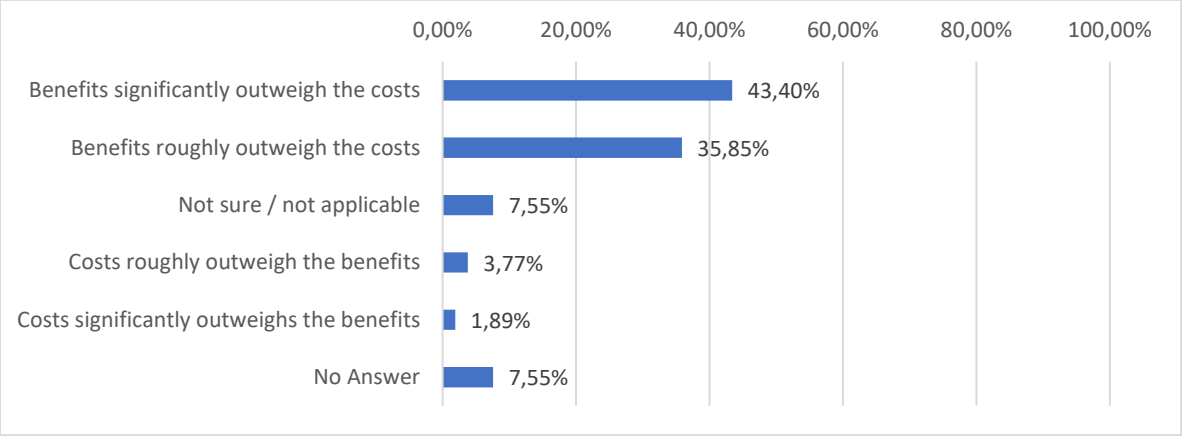
- Member State representatives;
- Supervisory Bodies, Conformity Assessment Bodies, Accreditation bodies.

Questions asked concerned the following measures:

1.1. Adoption of implementing acts referencing standards (audit schemes, conformity assessment, supervisory authorities) and adoption of targeted guidelines on the application of specific provisions (e.g. remote identification, identity proofing)

	Answers	%
Benefits significantly outweigh the costs	23	43,40%
Benefits roughly outweigh the costs	19	35,85%
Not sure / not applicable	4	7,55%

	Answers	%
Costs roughly outweigh the benefits	2	3,77%
Costs significantly outweighs the benefits	1	1,89%
No Answer	4	7,55%

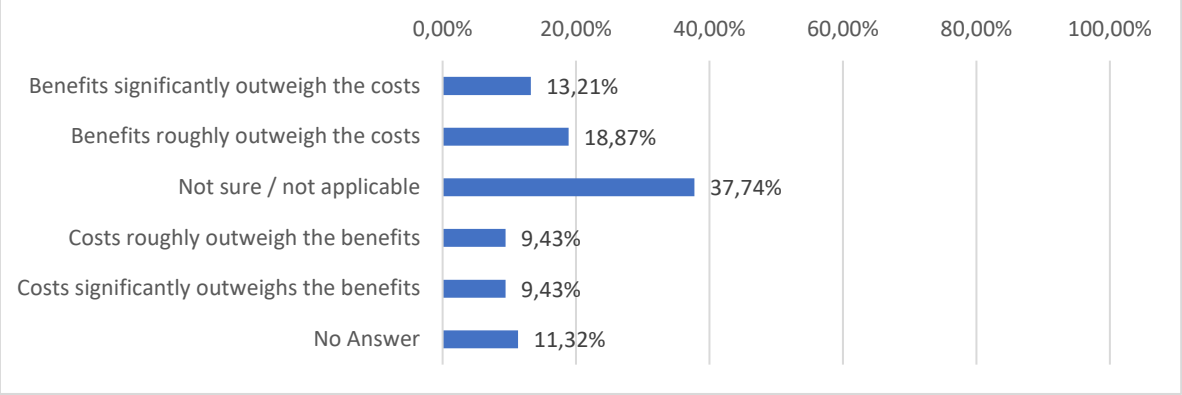


The results show how **79,25% of stakeholders** consider that the benefits from the adoption of implementing acts referencing standards and the adoption of targeted guidelines on the application of specific provisions would outweigh the costs.

Replies to this measure with “Benefits significantly outweigh the costs” amounted to **more than 43%** and “Benefits roughly outweigh the costs” a bit lower than **36% of respondents**.

1.2. Introduction of new requirements for the certification of eID means e.g. by referencing European cybersecurity certification schemes in the IA on LoAs.

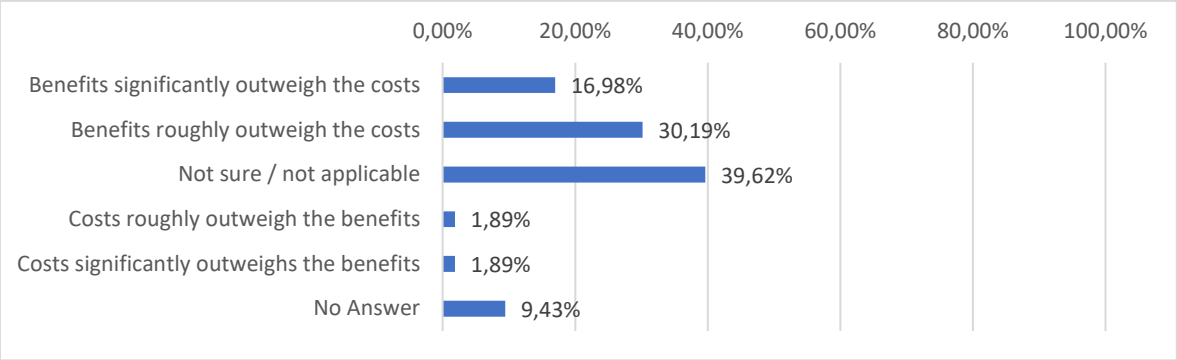
	Answers	Ratio
Benefits significantly outweigh the costs	7	13,21%
Benefits roughly outweigh the costs	10	18,87%
Not sure / not applicable	20	37,74%
Costs roughly outweigh the benefits	5	9,43%
Costs significantly outweighs the benefits	5	9,43%
No Answer	6	11,32%



The respondents involved are a bit more dubious about the measure above. **Thirty-two per cent of respondents** indicate that benefits would outweigh the costs while **19% of respondents** estimate that costs would outweigh the benefits.

1.3. Introduce guidelines for the private sector on costing, liability and on the opportunities to fulfil various regulatory requirements by the use of eiDs

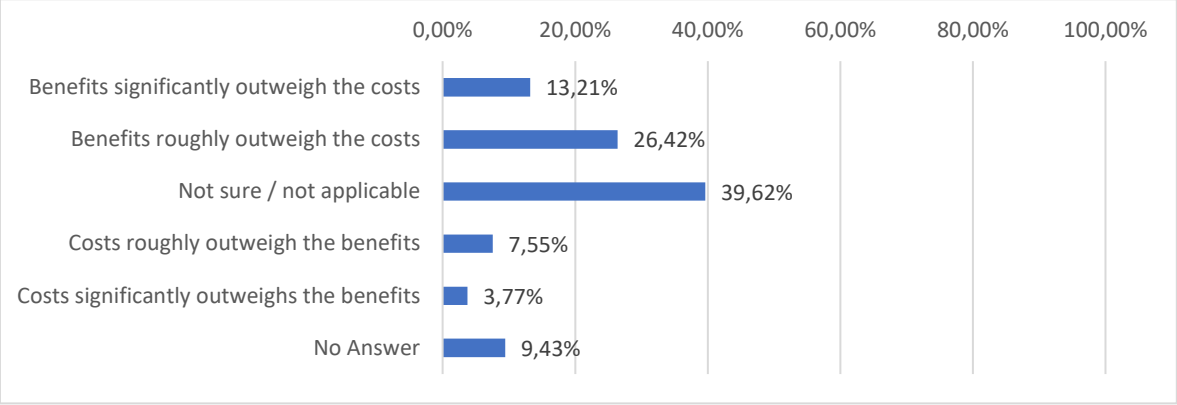
	Answers	Ratio
Benefits significantly outweigh the costs	9	16,98%
Benefits roughly outweigh the costs	16	30,19%
Not sure / not applicable	21	39,62%
Costs roughly outweigh the benefits	1	1,89%
Costs significantly outweighs the benefits	1	1,89%
No Answer	5	9,43%



Considering the measure above**, 47% of respondents** estimate that benefits would outweigh the costs. This percentage represents a clear majority compared to **4% of respondents** who estimate that costs would outweigh the benefits.

1.4. Establish Regulatory obligations for Member States to make available to their citizens highly secure and convenient national eID schemes

	Answers	Ratio
Benefits significantly outweigh the costs	7	13,21%
Benefits roughly outweigh the costs	14	26,42%
Not sure / not applicable	21	39,62%
Costs roughly outweigh the benefits	4	7,55%
Costs significantly outweighs the benefits	2	3,77%
No Answer	5	9,43%



A similar pattern as that recorded for Q 1.3 can be found in the result of the Q 1.4 considering the possibility to establish regulatory obligations for Member States to make available to their citizens highly secure and convenient national eID schemes.

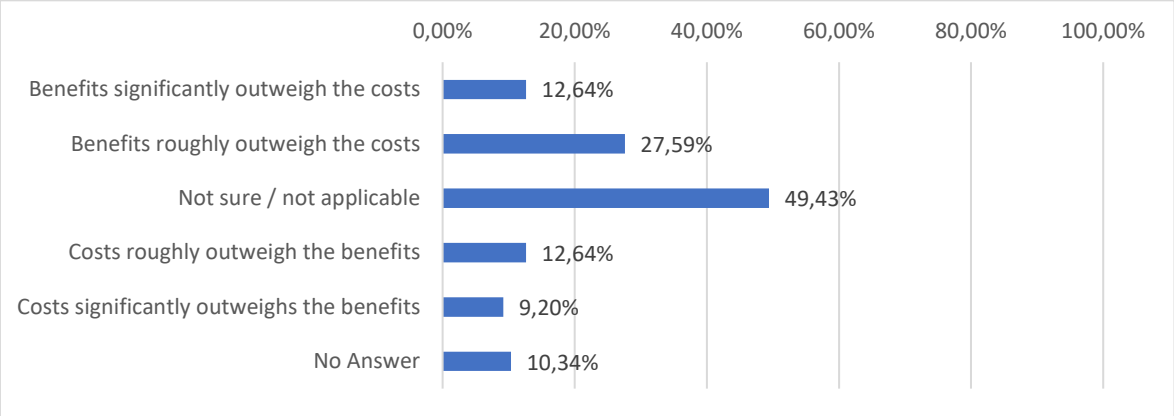
40% of respondents in total consider that benefits outweigh the costs compared to a small percentage of **11% of respondent** who expect costs to exceed benefits.

Policy Option 2

Under this option, the private sector would support the delivery of a European digital identity ecosystem in the form of a new qualified trust service for the exchange of digital identity attributes, such as proof of age (e.g. for accessing age restricted social media), professional qualifications (e.g. lawyer, student, doctor), digital driving licences, vaccination certificates etc. across borders. The scope of eIDAS would be expanded to cover this new trust service. In this new ecosystem, identity data and attributes would, whenever required, be securely linked to the legal eID of the user, making the data trustworthy and legally enforceable across borders. National eIDs notified under eIDAS would continue to be the sole means to provide legal identity across borders when this is required (e.g for public services, such as submitting a tax declaration online).

2.1. Focus on protection of data and privacy (establish Obligations on digital services providers to split data between data collected for the purpose of user identification and the provision of the digital ID service, and (2) data generated by the user's subsequent activity on the third party service providers' website, and transparency)

	Answers	Ratio
Benefits significantly outweigh the costs	11	12,64%
Benefits roughly outweigh the costs	24	27,59%
Not sure / not applicable	43	49,43%
Costs roughly outweigh the benefits	11	12,64%
Costs significantly outweighs the benefits	8	9,20%
No Answer	9	10,34%



Forty per cent of stakeholders, answering to this question believe that benefits would outweigh the costs Only **22% of respondents** do not see significant benefits from implementing this measure.

Policy Option 3

Policy Option 3 would introduce a European Digital Identity scheme (EUid). Questions about this option were asked in summer 2020 as part of the stakeholder surveys, and targeted to the following stakeholders' categories:

- Member State representatives;
- Supervisory Bodies, Conformity Assessment Bodies, Accreditation bodies;
- Identity providers.

It must be borne in mind that the implementation options that were presented in those surveys were different from the ones considered in this impact assessment. Specifically, respondents were asked to comment on the following implementation scenarios:

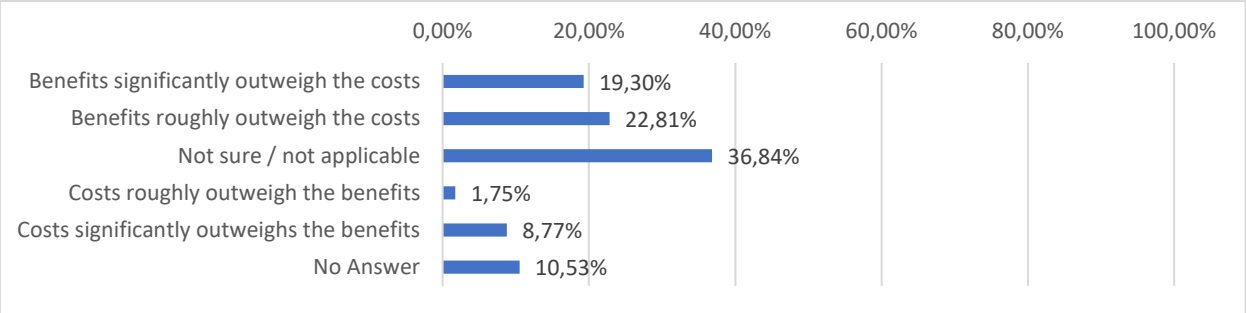
- Option 3.1 Aggregate existing national eID schemes – extension of the current eIDAS framework (The sub-option will be an evolution of the current eIDAS framework, it implies maximum diversity of eID means and identity providers)

- Option 3.2 Introduction of a new European eID scheme managed by an EU body (The sub-option will be separated from the current eIDAS framework, it implies limited diversity of eID means, one single identity provider)
- Option 3.3 Introduction of a new European eID scheme managed by a consortium / association (The sub-option will be separated from the current eIDAS framework, it implies limited diversity of eID means, several identity providers (at least one per MS)

The results recorded for Policy Option 3 show more clearly how the various stakeholders involved are not convinced about the benefits or applicability of these three sub-options. As noted above, however, these results may not be representative of stakeholder opinions on an EU eID Wallet App as presented in this impact assessment, since their comments were based on different implementation options and significantly less implementation detail on the proposals for an EU eID.

3.1. Aggregate existing national eID schemes – extension of the current eIDAS framework (The sub-option will be an evolution of the current eIDAS framework, it implies maximum diversity of eID means and identity providers)

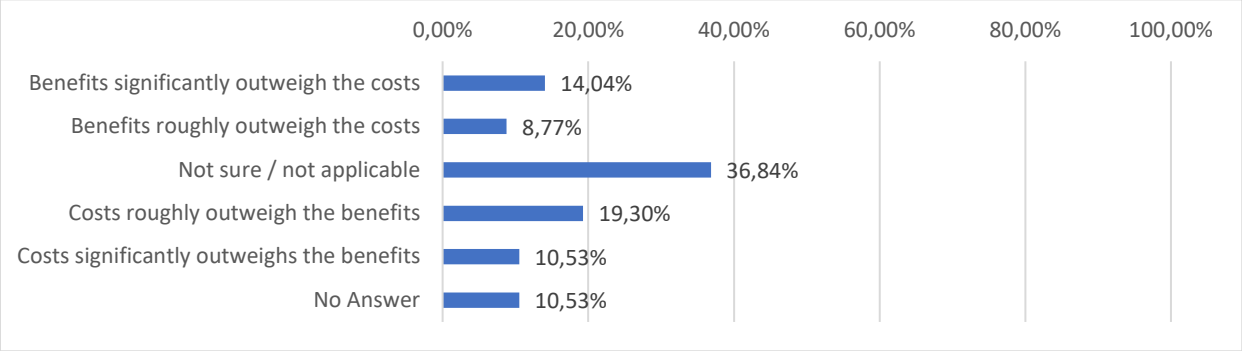
	Answers	Ratio
Benefits significantly outweigh the costs	11	19,30%
Benefits roughly outweigh the costs	13	22,81%
Not sure / not applicable	21	36,84%
Costs roughly outweigh the benefits	1	1,75%
Costs significantly outweighs the benefits	5	8,77%
No Answer	6	10,53%



The option Q 3.1 is the only one of the three considered in this section in which the various stakeholders are more in favour of adopting the policy than against: 42,11% of respondents estimate that benefits would outweigh the costs and 10,52% of respondents think opposite.

3.2. Introduction of a new European eID scheme managed by an EU body (The sub-option will be separated from the current eIDAS framework, it implies limited diversity of eID means, one single identity provider)

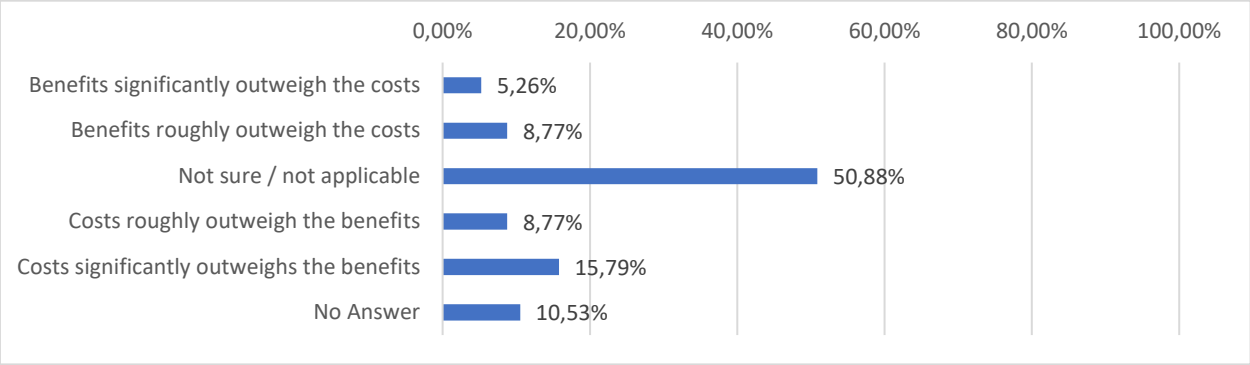
	Answers	Ratio
Benefits significantly outweigh the costs	8	14,04%
Benefits roughly outweigh the costs	5	8,77%
Not sure / not applicable	21	36,84%
Costs roughly outweigh the benefits	11	19,30%
Costs significantly outweighs the benefits	6	10,53%
No Answer	6	10,53%



In this case the respondents are not in favour of applying the measure: **29,82% of respondents** estimate that costs would outweigh the benefits compared to **22,81% of respondents** who argue otherwise.

3.3 Introduction of a new European eID scheme managed by a consortium / association (The sub-option will be separated from the current eIDAS framework, it implies limited diversity of eID means, several identity providers (at least one per MS)

	Answers	Ratio
Benefits significantly outweigh the costs	3	5,26%
Benefits roughly outweigh the costs	5	8,77%
Not sure / not applicable	29	50,88%
Costs roughly outweigh the benefits	5	8,77%
Costs significantly outweighs the benefits	9	15,79%
No Answer	6	10,53%



The last option shows an even sharper orientation than the previous one: **24,56% of respondents** estimate that the measure would involve more costs than achievable benefits compared to **14,04% of respondents** who see benefits achievable from the application of the policy option.

Interviews

The interviews conducted were mainly designed to gauge views on the costs and benefits of different policy options. As part of these interviews, however, participants also provided comments on some of the proposals, which enabled the team to identify areas of agreement/disagreement with the options and measures therein included, which are reported below.

Stakeholders participating in the interviews commented on various aspects of **Option 1**. Multiple interviewees flagged support for the measures relating to require Member States to allow the private sector to rely on notified eIDs and to establish a cost-model and liability rules (PO 1.2 and PO 1.3). Interviewees acknowledged that the absence of an obligation and the lack of clarity and homogeneity on access conditions for the notified eIDs were a barrier to private sector uptake.

Support was generally expressed with regard to the extension of the minimum dataset (PO 1.4), as interviewees from different sectors noted that the lack of some personal and sector-specific attributes had limited uptake of notified eIDs in the past.

Positive comments were further received on the introduction of EU-wide security certification requirements on a voluntary basis (PO 1.5). While they recognised that this would be an additional cost initially, they indicated that simplification and harmonisation would create benefits that outweigh this initial cost. They also indicated, however, that one risk with certification may arise when requirements fall behind technological developments, and therefore it should be ensured that these requirements are reviewed periodically.

In the interviews, there was also general consensus on the necessity of greater harmonisation of supervisory procedures for Trust Services, which more than one interview considered as long due.

In terms of **Option 2**, interviewees provided general perspectives on the notion of extending the regulation's scope to the private sector, including by creating new trust services covering identification, authentication and provision of attributes (which is most relevant to PO2 M1: Creating a new Qualified Trust Service for the secure exchange of data linked to identity). The stakeholders generally welcomed this idea, noting that a comprehensive legal framework for digital identity should take into account private actors, given their increasingly important role in the landscape, and that enhancing the cross-border exchange of attributes related to identity in a secure way would benefit both end users and the service providers. They also noted the market opportunities that may emerge from the possibility of providing credentials, noting however that the choice of business models for providers may not be obvious and would require careful consideration.

In this context, multiple stakeholders also indicated that the regulation of non-human entities (e.g. IoT devices) would be increasingly important because they recognised it as an area where IT security and data privacy need to be strengthened as a matter of priority. For example, one stakeholder noted that these devices generally do not come with guarantees of timely and ongoing software updates and cited research showing that 82% of IT professionals predicted that unsecured IoT devices would cause a data breach — likely "catastrophic" — within their organisation.

Measures to strengthen the protection of personal data PO 2.6) were also generally welcomed, in light of the fact that an extension of the regulation to private actors would require clear and strong safeguards to the privacy of end users.

Finally, on the notion of creating an EU Digital identity included **in Option 3,** stakeholders generally recognised the potential benefits of an eID means that would be recognised across borders and usable across a wide range of public and private services, with some exceptions. The interviewees who expressed opposition or concerns about the measure did so for a number of reasons that were mostly linked to the demanding implementation of the measure or its political feasibility[426]. Interviewees recognised that the scheme could have broad application across a number of sectors (e.g. mobility, education, health, finance, eCommerce) if it allowed users to exchange a wide range of qualified attributes and credentials related to their identity, and welcomed proposals for the scheme to be designed in line with principles of user-centricity,

[426] The interviews were conducted before the Council and the Commission publicly expressed the political ambition to create such scheme, so these views must be considered in the specific context where a clear political commitment had not been made

privacy and security. They saw the required negotiations with mobile manufacturers and network operators for the required access to the SE/eSIM as potentially complex, but viable.

Overall Analysis

Considering the results obtained from the three different surveys, it is possible to understand to what extent respondents are favourable to the implementation of the corrective actions under the three policy options.

Specifically, considering **Policy Option 1** (PO1), this would revise and complement the existing eIDAS framework as necessary to improve cross-border recognition of national eIDs and trust services.

Measure aiming "*enhancing clarity by providing guidance in relation to the LoAs required for specific types of online services*" was considered as viable by the majority of respondents to the Cooperation Network Survey. Harmonization of the understanding regarding the use cases between Member States and more guidance to distinguish LoA would facilitate harmonization of requirements and practices. Clear guidance is always welcome. Moreover, one-off adjustment would be limited; **56% of respondents** to the Deloitte / PwC Survey also estimate that benefits would outweigh the costs.

The Open Public Consultation indicates that PO 1.5 and PO 0.4 are well received by respondents: **43% of the total respondents** selected "*further harmonization through requirements established in secondary legislation (implementing acts), standardization and the introduction of certification to the advantage of particularly convenient and secure solutions"* among the corrective action to be taken. On the issue of establishing EU-wide certification of security requirements, however, several members of the Cooperation Network thought that the implementation of this policy may involve significant one-off adjustment costs, as well as some recurrent costs per year to consider. This proposal was also generally supported by the interviews.

Results from the Deloitte / PwC Survey also show that according to **79% of respondents**, the *adoption of implementing acts referencing standards and adoption of targeted guidelines on the application of specific provisions*) would bring important benefits compared to implementation costs. This view was echoed by many of the interviews who provided comments on this. Clear, more harmonized rules and more transparent regulations across Europe mean less trouble in the certification process and cost savings.

Concerning the *possible extension of the list of attributes covered by Implementing Regulation 2015/1501* , the respondents to the Cooperation Network Survey indicated that costs would be limited to standardisation work. In this respect, it was highlighted that an extension of the list of attributes is already considered by the eIDAS technical subgroup and will thus not lead to high additional cost; at the same time, based on this experience, some recognised that it might be challenging to reach an agreement on how to standardise the additional attributes. Some costs may arise from the integration of the existing data sources and connection to the eID node, but the estimate would depend on the range and type of attributes covered by the extension. **Forty-seven per cent of respondents** to the Deloitte / PwC Survey also argued that the implementation of PO1.4 would bring greater benefits than costs (ranking as the third preference within the overall survey results). Views from the interviews also highlight the potential benefits of this measure.

With regard to the corrective actions proposed under **Policy Option 2** (PO2 would create a market for the secure exchange of data linked to identity), the OPC suggests significant stakeholder interest in PO2.1, which encompasses the *introduction of new private sector digital identity trust services for identification, authentication and provision of attributes* (41%) and the *provision of identification for non-human entities* (20%). Further, 41% of respondents to the Deloitte / PwC survey were positive towards measures to strengthen data protection and privacy,

(PO2.6) perceiving their benefits as greater than their cost. The interviewees were also generally positive to the idea of regulating the provision of trusted identity attributes and the provision of identification for non-human entities

Finally, in relation to the corrective actions proposed under **Policy Option 3** (PO3 would introduce a European Digital Identity scheme). The results of the Open Public Consultation indicate that a large majority of respondents **(63%)** would gladly welcome the creation of a single and universally accepted European Digital Identity scheme, complementary to the national publicly issued electronic identities. However, **52% of the respondents** to the Open Public Consultation also indicated the complexity of set-up and Governance of a single and uniform European digital identity scheme as the main possible disadvantage. Interviewees were also broadly positive about the idea of an EU eID scheme, with only some expressing doubts over political feasibility and implementation and generally positive comments on the notion of providing a secure, privacy-preserving, user centric EU-wide scheme.

9.6 ANNEX F. List of interviewees

The tables below provide an overview of the stakeholders interviewed in this study.

Organisation	Organisation	Interviewees	Date
eHealth	Oviva	Manuel Baumann	29/07/2020
	Kaiku Health	Joel Lehikoinen	29/07/2020
	TNO	Oscar van Dewenter	29/07/2020
	Istituto Carlo Besta	Francesca De Giorgi	04/08/2020
eCommerce	European Digital SME Alliance	Andrea Caccia	27/07/2020
	Chainge Digital	Yanis Kyriakides	28/07/2020
	PayPal	Gareth Jones	30/07/2020
	EdRi	Jan Penfrat	30/07/2020
Financial Services	ITSME	Wim Coulier	28/07/2020
	ING	Katharina Hermann	31/07/2020
	Confidential (Financial institution operating in Europe)	*Confidential*	28/07/2020
	Unicredit	Gianluca D'Imperio	26/07/2020
	Nexi	Gianluca Botta, Flaminio Francisci, Francesco Fanelli	03/08/2020
	DNB Bank	Ronny Khan*	22/07/2020 & 16/12/2021
	ING	Katharina Hermann, Harsh Mohan	31/07/2020
	Mastercard	Charles Walton	31/07/2020
Transport	EUROCONTROL	Abdel Youssouf	31/07/2020
	CLECAT	Dominique Willems and Constantino Canu	3/08/2020
	Technical Officer ICAO	Andre de Kok	20/8/2020
Horizontal	Adobe	John Joliffe, Andrea Valle	24/07/2020
	AgID	Francesco Tortorelli	29/07/2020
	InfoCert	Carmine Auletta*, Igor Marcolongo	28/07/2020 & 17/12/2021**
	CSQA	Andrea Castello, Anna Conte	05/08/2020
	A-SIT MS Cooperation network	Herbert Leitold*	11/08/2020 & 17/12/2021
	Obserwatorium	Mihal Tabor	24/07/2020
Subject matter expert	Deutschebahn	Claudia Plattner	16/12/2021
	Erste Group	Erik Wagner	23/12/2021
	Digipolis	Daniel du Seuil	16/12/2021

* Considered also as a subject matter expert and consulted in two interviews
**Second interview conducted only with Carmine Auletta.

9.7 ANNEX G: Explanatory note on the macroeconomic model used

This annex provides the basic elements of the methodology adopted for the construction of an industry-level macro-economic model for the simulation of the economic effects of investments in the provision of eID services. From the point of view of the official statistical information, production of eID services are included in the Telecommunication sector accounts.

The research objective is to evaluate the impact of investments in the provision and use of eID services on the produced output and on employment in the other sectors in the economy.

The analysis relies on an estimated/calibrated general equilibrium model, whose supply-side is based on input-output relationships among industries, and the demand side is fully specified under the hypothesis of monopolistic competition among industries, such that firms are price-setters, i.e. they consider a mark-up over their own marginal costs in their pricing decisions, and demand is defined considering the full set of industry-specific relative prices.

Production takes place considering an input-output production technology in which the input mix is chosen optimally based on the relative prices of intermediate factor inputs. The telecommunication sector is isolated and included into the several production functions, such that a simulated investment decision affects each sector both directly and indirectly through the other sectors' responses. The impact in each sector is captured by an increase in the telecommunication input, leading to production effects and substitution effects, the latter driven by the relative price changes.

9.7.1 The model

The model used is a large-scale **Input-Output Dynamic Stochastic General Equilibrium Model (IO-DSGEM)** consisting of an Input-Output structure for the supply side and of a symmetric demand side, and which assumes monopolistic competition. This provides an instrument that allows an internally consistent evaluation of the potential macroeconomic effects of investment in the provision and adoption of eID services at a high level of macroeconomic detail.

To enhance the generality of results, a flexible translog production technology employing 16 factor inputs is adopted for each of the two-digits NACE classification (Rev. 1.1) [427] addressed in the analysis. The attractive feature of the translog functional form is that it imposes no *a priori* restrictions on substitution and price elasticities (Berndt, 1990), that can be derived from the estimated parameters of the implied cost share functions.

On the demand side, following a standard approach (see Blanchard and Kiyotaki (1987)), sector-specific demand and price setting functions are analytically derived under the hypothesis of monopolistic competition.

Given the limited sample size and the nonlinearity of the key output production functions and of the related cost shares, the Bayesian estimator is employed to parameterize the supply side of the model. The parameterization of the demand side is instead calibrated.

9.7.2 The supply-side

On the supply side, we define the production technology employing N simultaneous-equations, where N is the number of sectors in the economy (disaggregated according to the NACE classification system, with N=58). Each production function defines the amount of output that can be produced for given amounts of inputs, and satisfies the non-negativity, linear homogeneity

[427] NACE is a 4-digit activity classification used by the European Union since 2002. More details are available at: http://ec.europa.eu/eurostat/ramon/relations/index.cfm. The classification of economic activities according to NACE is totally coherent with ISIC and can be considered its European counterpart. Concordance tables from NACE to ISIC are available at: http://www.foost.org/database/nace/nace-en_2002c.php.

and concavity properties. Each produced commodity serves equivalently as a final consumption good and as an intermediate input.

Sector *j*'s (with *j* = 1, 2 ..., N) production function includes: energy inputs (*E*), materials (*M*), services (*S*), capital services from ICT assets (*ICT*), capital services from non-ICT assets (*K*) and labour (*L*). The production inputs evaluated at their basic costs are obtained by aggregating NACE sectoral inputs *h* = 1, ..., I_X as $p_i X_{ij} = \sum_{h=1}^{I_x} p_{h,i} X_{h,ij}$, with *i* = 1...6 (i.e. the six inputs *E*, *M*, *S*, *ICT*, *K*, *L*), where *X* denotes the amount of input *i* used in sector *j*, *p* denotes prices, and upper-case letters denote quantities.

The nominal value of sectoral output of industry *j* is given by the revenue function:

$$p_Y Y_j = f\left(p_E E_j, p_M M_j, p_S S_j, p_{ICT} ICT_j, p_K K_j, p_L L_j\right) \quad (1)$$

To simplify the analysis, we assume constant return to scale and single-output technologies. Under these conditions, the production function and the cost function match each other. In other words, even though one function is defined with respect to quantities, and the other with respect to prices, both convey the same information about the production technology. Because of this duality property between production and cost functions, the total cost function of (1) can be written as:

$$C_j = g(p_E, p_M, p_S, p_{ICT}, p_K, p_L) \quad (2)$$

On these formal premises, results strongly depend on substitution among factor inputs. This implies that the definition of the partial elasticities of substitution plays a key role. In order to enhance the generality of the analysis (by allowing that inputs demands depend on the level of output), we assume a non-homothetic translog cost function[428], which is given by:

$$ln(C_j) = ln(\alpha_{0j}) + \sum_{i=1}^{6} \alpha_{ij} ln(p_i) + \frac{1}{2} \sum_{i=1}^{6} \sum_{k=1}^{6} \gamma_{ikj} ln(p_i) ln(p_k) + \alpha_{Yj} ln(Y_j) + \frac{1}{2} \gamma_{YYj} ln(Y_j^2) + \sum_{i=1}^{6} \gamma_{iYj} ln(p_i)\, ln(Y_j) \quad (3)$$

where $\gamma_{ikj} = \gamma_{kij}$, Y_j denotes sector *j*'s output and C_j is the total cost. To obtain homogeneity of degree 1 in prices conditional on Y_j, the following restrictions are imposed:

$$\sum_{i=1}^{6} ln(\alpha_{ij}) = 1 \quad (4)$$

$$\sum_{i=1}^{6} ln(\gamma_{ikj}) = \sum_{i=1}^{6} ln(\gamma_{kij}) = \sum_{i=1}^{6} ln(\gamma_{iYj}) = 0 \quad (5)$$

Note that alternative specifications can be obtained by imposing additional restrictions to the translog production function (3). First, the homothetic property, i.e. that inputs demand does not depend on the level of output can be imposed by assuming $\gamma_{iYj} = 0 \ \forall$ *i* = 1...6; second, homogeneity of a constant degree in output $1/\alpha_{0Yj}$can be obtained if the condition $\gamma_{iYj} = 0$ is added to the homotheticity condition; third, constant returns to scale are obtained when, in

[428] The translog cost function is basically a second order Taylor approximation to an arbitrary cost function.

addition to the restrictions above, $\alpha_{Yj} = 1$; fourth, the Cobb-Douglas production function is obtained when, in addition to all the above restrictions, $\gamma_{ikj} = 0$ ∀*i,k* = 1...6.

Because of data availability and potential gains in efficiency, the cost production function (3) is better estimated indirectly, by solving it with respect to the cost shares. These are derived from cost-minimizing input demand equations, obtainable by differentiating (3) with respect to input prices and employing the Shephard's Lemma:

$$\frac{\partial ln(C_j)}{\partial ln(p_i)} = \frac{p_i}{C_j}\frac{\partial C_j}{\partial p_i} = \frac{p_i X_{ij}}{C_j} = \alpha_{ij} + \sum_{k=1}^{6}\gamma_{kij} ln(p_k) + \gamma_{iYj} ln(Y_j) \quad (6)$$

where $C_j = \sum_{i=1}^{6} p_i X_{ij}$. By denoting the cost share $p_i X_{ij}/C_j$ with S_{ij}, i=1...6, the following cost share equations for the six inputs (*E,M,S,ICT,K,L*) are:

$$S_{Ej} = \alpha_{Ej+}\gamma_{EEj} ln(p_E) + \gamma_{EMj} ln(p_M)+\gamma_{ESj} ln(p_S)+\gamma_{EICTj} ln(p_{ICT}) + \gamma_{EKj} ln(p_k)+\gamma_{ELj} ln(p_l)+\gamma_{EYj} ln(Y_j)$$

$$S_{Mj} = \alpha_{Ej+}\gamma_{Mj} ln(p_E) + \gamma_{MMj} ln(p_M)+\gamma_{MSj} ln(p_S)+\gamma_{MICTj} ln(p_{ICT}) + \gamma_{MKj} ln(p_k)+\gamma_{MLj} ln(p_l)+\gamma_{MYj} ln(Y_j)$$

$$S_{Sj} = \alpha_{Ej+}\gamma_{SEj} ln(p_E) + \gamma_{SMj} ln(p_M)+\gamma_{SSj} ln(p_S)+\gamma_{SICTj} ln(p_{ICT}) + \gamma_{SKj} ln(p_k)+\gamma_{SLj} ln(p_l)+\gamma_{SYj} ln(Y_j)$$

$$S_{ICTj} = \alpha_{Ej+}\gamma_{ICTEj} ln(p_E) + \gamma_{ICTMj} ln(p_M)+\gamma_{ICTSj} ln(p_S)+\gamma_{ICTICTj} ln(p_{ICT}) + \gamma_{ICTKj} ln(p_k)+\gamma_{ICTLj} ln(p_l)+\gamma_{ICTYj} ln(Y_j)$$

$$S_{Kj} = \alpha_{Ej+}\gamma_{KEj} ln(p_E) + \gamma_{KMj} ln(p_M)+\gamma_{KSj} ln(p_S)+\gamma_{KICTj} ln(p_{ICT}) + \gamma_{KKj} ln(p_k)+\gamma_{KLj} ln(p_l)+\gamma_{KYj} ln(Y_j)$$

$$S_{Lj} = \alpha_{Lj+}\gamma_{LEj} ln(p_E) + \gamma_{LMj} ln(p_M)+\gamma_{LSj} ln(p_S)+\gamma_{LICTj} ln(p_{ICT}) + \gamma_{LKj} ln(p_k)+\gamma_{LLj} ln(p_l)+\gamma_{LYj} ln(Y_j)$$

(7)

This system of equations has 48 parameters (eight in each of the six equations) for each *j* sector (with *j* = 1...56). By imposing the 15 symmetry restrictions, $\gamma_{ikj} = \gamma_{kij}$, ∀*i,k* = 1...6, and the eight homogeneity restrictions in input prices, $\sum_{i=1}^{6} ln(\alpha_{ij}) = 1$, $\sum_{i=1}^{6} ln(\gamma_{ikj}) = 0$ ∀*k* = 1...6, $\sum_{i=1}^{6} ln(\gamma_{kij}) = 0$, we reduce the number of parameters to be estimated to 25 (for each sector *j*). Moreover, since for simulation purposes constant returns to scale are preferred, we also estimate a version of the system above in which we impose the six additional restrictions $\sum_{i=1}^{6} ln(\gamma_{iYj}) = 0$ ∀*i* = 1...6. These restrictions reduce further the number of parameters to be estimated to 18 for each *j* sector (the restriction $\sum_{i=1}^{6} ln(\gamma_{iYj}) = 0$ becomes redundant).

The Hicks-Allen partial elasticities for the general dual cost function can be computed as $\sigma_{ik} = (C/C_i)(C_{ik}/C_k)$, while the price elasticities can be computed as $\epsilon_{ij} = \partial ln(X_i)/\partial ln(p_k) = (\partial X_i/\partial p_k)(p_k/X_i) = S_k\sigma_{ik}$. Under translog function assumption, the partial and own elasticities turn out to be:

$$\sigma_{ik} = \frac{\gamma_{ik}+S_i S_k}{S_i S_k} \quad (8a)$$

$$\sigma_{ii} = \frac{\gamma_{ii}+S_i^2-S_i}{S_i^2} \quad (8b)$$

whereas price elasticities can be calculated as:

$$\epsilon_{ik} = \frac{\gamma_{ik}+S_i S_k}{S_i} \quad (9a)$$

$$\epsilon_{ii} = \frac{\gamma_{ii}+S_i^2-S_i}{S_i} \quad (9b)$$

9.7.3 The demand-side

On the demand side, the demand for good *j* (D_j) is given by:

$$D_j = \left(\frac{p_j}{p}\right)^{-\varepsilon} D \quad (10)$$

where $p = \left[\sum_{j=1}^{N} p_j^{1-\varepsilon}\right]^{\frac{1}{1-\varepsilon}}$ is the price index resulting from the Dixit-Stiglitz aggregator, ε denotes the (demand) elasticity of substitution among differentiated products, and $D = \left[\sum_{j=1}^{N} D_j^{\frac{\varepsilon-1}{\varepsilon}}\right]^{\frac{\varepsilon}{\varepsilon-1}}$ is aggregate demand. At each point in time, only a fraction of prices are re-optimized, whereas the remaining fraction is held fixed at the previous time level. Reset prices (optimal) are defined by maximizing profits subject to the supply equations and (12) and turn out to depend on the sectoral marginal cost MC_j. In the aggregate:

$$p_{j,t} = \theta \frac{\varepsilon}{\varepsilon-1} MC_{j,t}(1-\theta)p_{j,t-1} \quad (11)$$

where θ is a convolution of parameters summarizing the (complement to one) of the degree of nominal price rigidity, $\varepsilon/\varepsilon - 1$ is the price mark-up from monopolistic competition and $MC_{j,t}$ are marginal costs in sector *j*. Goods market equilibrium is satisfied when demand equals supply for each product-factor *j*. Under flexible prices hypothesis, the symmetric equilibrium holds period by period.

The instantaneous and cumulated effects on output and employment can be evaluated in terms of both percentage deviations from control (i.e. a situation in which no investment/adoption occurs) and in terms of variations of volumes, i.e. output value effects (in Euros), and employment effects (in jobs).

The estimation requires detailed statistical information on sectoral outputs and inputs, i.e. industry by industry input-output tables, publicly provided by the Eurostat (European System of Accounts - ESA 95), while other operational variables and data are obtained from the Eurostat Structural Indicators and from the STAN - OECD database. A detailed description of the statistical information is provided in the next section.

9.7.4 Estimation

The econometric methodology used - given the shortage of data availability over the time dimension and the small number of degrees of freedom over the sectional dimension - is the Bayesian seemingly unrelated regression equation (SURE) estimator. The Bayesian Monte-Carlo integration method ensures convergence in estimation while maintaining consistency even with small samples.

The scope of Bayesian estimators is to get the posterior distribution for model parameters conditioning on prior beliefs on models, structural parameters, and sample information. The methodology thus nests a formalized prior distribution for the *q*-th Model's parameters and the conditional distribution (pseudo-likelihood) to get the posterior density. This is obtained by employing the Bayes' rule.

The posterior distribution of interest is the result of a weighted average of prior non sample information and the conditional distribution (i.e. the empirical information). Weights are inversely related to, respectively, the variance of the prior distributions and the variance of the sample information ("precisions"). Thus, formalizing a tight prior will result in highly constrained estimation, while a diffuse prior will result in weakly constrained estimation. Asymptotically, the conditional distribution (objective information) dominates the prior distribution (subjective information) and the posterior distribution of the parameters collapses to their pseudo-true values. This property ensures that the relevance of priors in posterior estimates vanishes as the sample size increases. A further feature of the Bayesian estimator that is particularly important in standard applications is that its small sample performances outperform those of the FIML estimator (Geweke et al., 1997; Fernandez-Villaverde and Rubio-Ramirez, 2004).

The posterior density of interest is a complex nonlinear function of the deep parameters, thus its analytical calculation is not generally feasible analytically. For this reason, we calculate the posterior distribution via numerical integration. Operationally, the Bayesian MCMC posterior estimates are obtained adopting a two steps procedure, employing the Kalman smoother to approximate the conditional distribution and the Gibbs sampler implemented in BACC to perform Monte Carlo integration.

Measures of sectoral outputs and inputs require industry by industry input-output tables which are provided by the Eurostat (European System of Accounts - ESA 95). Other variables are obtained from the Eurostat Structural Indicators and from the STAN - OECD database.

9.7.5 Data

The model parameterization is obtained from the information provided by a panel of years and sectors. The data are available from 1995. According to the 2-digit NACE classification systems, 58 production sectors are included in the estimates and in the model simulation (NACE-P is omitted because of data constraints). These 58 economic sectors cover all the economic activities, that is, only mentioning the macro-areas (1-digit NACE): *Agriculture, hunting and forestry (A), Fishing* (B), *Mining and quarrying* (C), *Manufacturing* (D), *Electricity, gas and water supply* (E), *Construction* (F), *Wholesale and retail trade, repair of motor vehicles, motorcycles and personal and household goods* (G), *Hotels and restaurants* (H), *Transport, storage and communication* (I), *Financial intermediation* (J), *Real estate, renting and business activities* (K), *Public administration and defense; compulsory social security* (L), *Education* (M), *Health and social work* (N), *Other community, social and personal service activities* (O).

The econometric analysis relies on the following set of data:

- values of the 1-digit 17 inputs used (including labour) at purchaser prices
- values of the 2-digit sectoral output at basic prices
- inputs' prices (except labour)
- labour compensation

All this information is obtained by three main data sources:

1. OECD – *STAN* STructural ANalysis Database;

2. Eurostat - Industry, trade and services – Industry and construction Industry;

3. ESA 95 Table – Input-output tables – Eurostat.

Inputs and Outputs at basic prices are obtained from all the sectors (A/01-Q/99) ESA 95 Table - Input-output tables - Eurostat: Supply and Use Tables, Current Prices. Two-digit NACE aggregation system. This dataset is key in the definition of the model structure, i.e. of the number of production sectors, relative prices and demand functions being considered in the model, as well as for the model estimation stage. The supply, the use and the merged input-output tables provide a detailed picture of the interdependencies of the production system. In particular, information on the use of goods and services (products) and the output generated in each production is provided by the supply and use tables.

The symmetric input-output table is a transformation of the supply and use tables under a fully consistent classification system[429].

The supply table illustrates where in the production system goods and services are produced; in other words, it offers information on the supply of goods and services by type of product of an economy in each year. By column, information on the production programme for each sector is provided, i.e. the domestic output of primary and secondary productions is reported. The principal activities of each industry are identifiable in the main diagonal of the matrix table, whereas the off-diagonal elements provide information on secondary activities.

The use table conveys information on the use of goods and services by product, by type of use for intermediate consumption (i.e. where intermediate consumption by industry is paired to final consumption by individuals) and by industry. Its structure can be described as follows: by columns, the input structure of each industry is reported; by row, instead, the use of different products and primary inputs is shown for each production sector. The costs of production can be obtained in the table's columns for each sector and the total cost of each product can be obtained from the sum across columns for each row. The total output measured at basic prices for each sector is reported as sum across rows for each column.

The use input-output table is the results of intersections between (rows) product and value added and (columns) sectors and individuals as final users (exemplified in Table 2.1). The rows report the use of goods and services by sector (intermediate consumption) and by individuals (final consumption). The columns of sectors reflect the production structure (used inputs) of each specific sector.

Table 1 - Structure of a use I/O table of an economic system composed by only 3 sectors (Agriculture, Manufacture and Transport)

	Sectors			Final users	TOTAL
Products	**Agriculture**	**Manufacture**	**Transport**		
Cereals Textiles Transport services	Intermediate consumption			Final consumption by product	**Total consumption by product**
Value added	Value added by sector				**Total Value added**
TOTAL	**Total output by sector**			**Total consumption by final users**	

In the example reported in **Error! Reference source not found.** below, 10% of the cereal production is used as input in the productive process of agriculture and 33% in manufacture. 57%

[429] The classification used for the included sectors is the "General Industrial Classification of Economic Activities within the European Communities" (NACE), whereas the classification employed for products is the 'Classification of Products by Activity' (CPA), which are one the counterpart of the other.

is consumed by individuals. With respect to columns, the transport sector employs 50% of textiles and 50% of transport services for the total production of 15 units.

Table 2 - Example of a use I/O table of an economic system composed by only 3 sectors (Agriculture, Manufacture and Transport).

	Sectors			Final users	TOTAL
Products	**Agriculture**	**Manufacture**	**Transport**		
Cereals	10	33	0	57	**100**
Textiles	5	67	5	41	**118**
Transport services	21	23	5	19	**68**
Value added	2	5	5		**12**
TOTAL	**38**	**128**	**15**	**117**	

The combination of the supply and the use tables gives the symmetric input-output table, which requires a transformation procedure in order to move from the product by industry system of the supply and use tables to the product by product system or the industry by industry system.

It is worth stressing that, given the single output technology hypothesis, which implies that a sector produces a single product/service, the only needed information for the purposes of our analysis is the use input-output tables (made by 58 rows and 17 columns).

Price deflators for the industries/productions of the Supply and Use Tables are obtained from different sources' data elaborations and harmonization. Data from STAN are sometimes aggregated at a less detailed ISIC level. In this case, average prices as given by STAN in the ISIC category are used. For instance, agriculture and fishing that are in the ISIC_group 01_02 are distinct categories in NACE. To this purpose, the same price (given by STAN) within the ISIC_group 01_02 was associated to the two categories 01 and 02 in the NACE classification. The associated price is the average of the prices in sectors agriculture and fishing weighted by the relative output shares. In the specific of the various sectors, the following data sources are considered:

- Agriculture, hunting and forestry (A/01-02): OECD - STAN - Two-digit ISIC aggregation system
- Fishing (B/05): OECD - STAN - Two-digit ISIC aggregation system
- Mining and quarrying (C/10-14): OECD - STAN - Two-digit ISIC aggregation system
- Manufacturing (D/15-37): Eurostat - Industry, trade and services - Industry and construction - Industry - Production price indices - Two-digit NACE Rev. 1 aggregation system
- Electricity, gas and water (E/40-41): OECD - STAN - Two-digit ISIC aggregation system
- Construction (F/45): OECD - STAN - Two-digit ISIC aggregation system
- Wholesale and retail trade; repair of motor vehicles, motorcycles and personal and house-hold goods (G/50-52): OECD - STAN - Two-digit ISIC aggregation system
- Hotels and restaurants (H/55): OECD - STAN - Two-digit ISIC aggregation system
- Transport, storage and communication (I/60-64): OECD - STAN - Two-digit ISIC aggregation system
- Financial intermediation (J/65-67): OECD - STAN - Two-digit ISIC aggregation system
- Real estate, renting and business activities (K/70-74): OECD - STAN - Two-digit ISIC aggregation system
- Public administration and defence; compulsory social security (L/75): OECD - STAN - Two-digit ISIC aggregation system

- Education (M/80): OECD - STAN - Two-digit ISIC aggregation system
- Health and social work (N/85): OECD - STAN - Two-digit ISIC aggregation system
- Other community, social and personal service activities (O/90-93): OECD - STAN - Two-digit ISIC aggregation system
- Activities of households (P/95): OECD - STAN - Two-digit ISIC aggregation system
- Extra-territory organizations and bodies (Q/99): OECD – STAN - Two-digit ISIC aggregation system

Employment is obtained as a result of some elaborations. Data from all sectors (A/01-Q/99) STAN - Two-digit ISIC aggregation system - Total employment (number of persons employed) are sometimes aggregated at a less detailed ISIC level than in the I/O tables. In these cases, STAN provides the aggregate value for employment, i.e. total workers in the ISIC category are used, and these aggregates are spread into the relevant subcategories by using a schedule of weights based on relative output shares obtained from the NACE sub-categories.

Labour compensation data are obtained from the all sectors (A/01-Q/99) OECD - STAN - Labour compensation - Two-digit ISIC aggregation system. Labour compensation represents the wage rates, which include: i) basic wages, cost-of-living allowances, and other guaranteed and regularly paid allowances) + ii) overtime payments + iii) bonuses and gratuities regularly paid + iv) remuneration for time not worked + v) bonuses and gratuities irregularly paid + vi) payments in kind + vii) employer contribution to statutory social security schemes or to private funded social insurance schemes + viii) unfunded employee social benefits paid by employers.

Publications Office
of the European Union

doi: 10.2759/671740
ISBN 978-92-76-37859-4