BE e-Archiving Certification Scheme

Version: v1.2

Date: 30/03/2021

FPS Economy, S.M.E.s, Self-employed and Energy

1210 Brussels

Be.Sign@economie.fgov.be

Document Version History

Date	Version	Evolution	Author
21.03.2021	1.0	Original version for public consultation	FPS Economy BE
29.03.2021	1.1	Editorial correction Ann A, clause [A1]	FPS Economy BE
30.03.2021	1.2	Editorial correction – paragraph numbering	FPS Economy BE

Contents

1 Foreword

With the entering into force of the eIDAS Regulation [2] the Belgian regulatory authority complemented the list of the eIDAS defined trust services with the service for “electronic archives”. One can indeed consider the need for electronic archiving as a logical consequence of electronic transactions and related online services. Although the trust service for electronic archives is established on a national level only, the aim of the regulator was clearly to align the requirements for this specific trust service as much as possible with the requirements laid down in the eIDAS Regulation [2].

The requirements for electronic archiving services laid down in the Belgian legal framework for trust services [4] are primarily legal and functional in nature. This leads to the need for identifying and clarifying technical, organizational and procedural controls to be put in place by a service provider or a service operator in order to develop and operate an electronic archiving service conformant to the legal requirements and trustworthy for all relying parties.

On initiative of the cabinet of the Minister for the Digital Agenda, a working group with representatives from various sectoral organizations and authorities was created in order to identify one or more normative documents describing technical and organizational controls and measures that can be used for the development, maintenance and conformity assessment of electronic archiving services. This led to the publication of a list of several international standards [3] that can or may be used for specifying controls and measures for establishing conformity to a part of the legal requirements. At that point in time, it was not deemed feasible to find a single normative document covering, into sufficient detail, all the statutory requirements laid down for electronic archiving services.

This observation eventually leads to the need for a specific certification scheme for electronic archiving services – the e-Archiving certification scheme - for facilitating the practical and effective implementation of qualified services for archiving of electronic documents and information in electronic form conformant to the requirements of the Belgian legislation.

This e-Archiving certification scheme has been prepared by a working group of interested parties and stakeholders with the active support of the supervisory body for trust service providers from the FPS Economy.

2 Introduction

Traditionally, 'archiving' means preserving historical records. The records maintained are generally distinctive and serve as original and authentic source for contractual, economical or societal relevant information. Ensuring integrity and authenticity of archived data is important for all parties involved and potentially affected by archived information. The statutory and functional requirements aiming at supporting trust in documents and information archived in an electronic way, are laid down in the Belgian legislation [4].

The present document is intended to apply to archiving systems for electronic documents and information, which are designed and operated for storing and long-term preservation of information in order to be able to present, in some future point in time, to interested or involved parties, the preserved information together with legally acceptable proof of integrity and authenticity of this information.

The present document is also intended to apply to systems for the digitisation of non-digital born documents and information, in order to provide legally acceptable proof of integrity and completeness with the original documents or information, and in order to create an associated metadata package that can be preserved by a system for long-term preservation.

The present document is not intended for the preservation of information for other than statutory reasons like e.g. digital archiving of cultural heritage objects or preservation of research data.

The present document is based on a more general framework created by other international standards. Its purpose is to present context, specific rules and procedures for certifying archiving services for electronic information conformant to the requirements laid down in the Belgian legislation.

3 Objective

The present document describes a scheme for the assessment and certification of archiving services for electronic documents and electronic information (e-Archiving services).

The e-Archiving certification scheme aims at supporting and facilitating the development and the effective realization of electronic archiving services compliant to the requirements of the Belgian Code de droit Economique – Livre XII – Titre 2 [4].

The certification scheme contains certification criteria for electronic archiving services and for the operators or providers of such services in order to demonstrate compliance to the statutory requirements applicable in Belgium [4]. The certification scheme also contains requirements and guidelines for the consistent operation of conformity assessment bodies (CABs) assessing and certifying the conformity of e-Archiving services.

The accreditation of certification bodies and the certification of electronic archiving services under this scheme are subject to the clauses and requirements detailed in the present document.

The present document has three main objectives:

- The description of the general approach of the process for the certification of e-Archiving services ;
- The identification of specific needs and controls to address the risks and statutory requirements of the services in scope of the document ;
- The clarification of requirements for certification bodies seeking to operate the e-Archiving certification scheme.

The e-Archiving certification scheme is drafted in a way to maintain and exploit to a maximum the alignment with the conformity assessment and attestation practices developed for the European eIDAS framework of trust services and their providers. For this reason, an important part of the audit criteria for e-Archiving services and their providers are inspired by, or based on, the requirements and

clauses of some general and specific European or international standards developed for eIDAS trust services. For the same reason, the process requirements for the conformity assessment of e-Archiving services and their providers is totally in line with the requirements applicable to the conformity assessment of eIDAS trust services.

4 Scope

The present document applies to two types of e-Archiving services and to two distinct situations of service provisioning.

The electronic archiving services are:

- The **e-Archiving service for digitisation of information (IDS)** relating to the scanning of paper-based documents with the aim of digitisation of the contained information, and the creation of a faithful and durable electronic copy of the document;
- The **long-term preservation e-Archiving service (LTPS)** for retaining electronic documents or electronic information in a way as to preserve the enclosed information from loss and from any modification other than changes related to its preservation format or storage medium.

The service operators in scope are:

- **Third party trust service provider**s as defined in article 3 of the eIDAS Regulation [2] which offer e-Archiving services to external relying parties. In offering qualified or non-qualified services, providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the legal obligations applicable to them and to the services they provide.
- **Operators of e-Archiving services**: public sector bodies, or natural or legal persons, operating e-Archiving services on its own behalf. In operating qualified or non-qualified e-Archiving services, operators shall be liable for damage caused intentionally or negligently to any external natural or legal person due to a failure to comply with the legal obligations applicable to them and to the e-Archiving services they operate.

5 Regulatory framework and references

5.1 Regulatory framework

The e-Archiving certification scheme is predominantly drafted for facilitating the certification of e-Archiving services in view of its qualification according to the provisions as described in the Belgian regulatory framework for trust services and trust service providers, basically defined by the following legislative acts:

[1] Wetboek van Economisch Recht – Boek XII – Titel 2
Code de Droit Economique – Livre XII – Titre 2.

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[3] Koninklijk besluit van 29 maart 2019 tot vaststelling van referentienummers voor normen inzake de gekwalificeerde elektronische archiveringsdienst.
Arrêté royale du 29 mars 2019 fixant les numéros de référence des normes applicables au service d'archivage électronique qualifié.

By satisfying the audit criteria from this e-Archiving certification scheme, a service provider and the e-Archiving service(s) he provides or operates can demonstrate compliance with the statutory requirements for e-Archiving services laid down in the above mentioned legislation.

It should be observed that the use of this e-Archiving certification scheme is voluntary and that demonstration of compliance with the applicable statutory requirements can be done on the basis of other certification schemes or technical standards.

5.2 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

The following referenced documents are necessary for the application of the present document.

[4] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[5] ISO 14641:2018: “Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications”.

[6] NF Z42-026:2017 :”Définition et spécifications des prestations de numérisation fidèle de documents sur support papier et contrôle de ces prestations“.

[7] ETSI TS 119 612 (V2.1.1): "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[8] ISO/IEC 17065: “Conformity assessment – Requirements for bodies certifying products, processes and services”.

[9] ETSI EN 319 403-1: “Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers”.

[10] ETSI TS 119 403-3: “Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers”.

5.3 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[11] ETSI TS 119 511: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques”.

[12] ETSI TS 119 312: “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”.

[13] ETSI TS 119 512: “Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services”.

6 Definition of terms and abbreviations

6.1 Terms (see annex D)

6.2 Abbreviations (see annex D)

6.3 Verbal forms

In the present document, the term “shall” is used to indicate a requirement strictly to be followed and from which no deviation is permitted. The term “should” is used to indicate that among several possibilities one is recommended as particularly suitable. To further simplify the reading, the term “service operator” is used to indicate either a third party service provider or an entity operating the service on its own behalf, depending on the particular situation, except for these passages where an explicit reference is made either to “third party trust service providers” or to “operators of e-Archiving services”.

7 Certification of electronic archiving services

7.1 General concept

The overall aim of certification is to give confidence to all interested parties that an e-Archiving service and its provider or operator fulfil the requirements of the applicable Belgian regulatory requirements [1].

The certification of e-Archiving services shall be organized and operated as a structural process composed of consecutive activities aiming at demonstrating and upholding the conformity of the e-Archiving service to the applicable requirements and audit criteria. The core elements of the conformity assessment are the evaluation of the e-Archiving service design and the audit of the e-Archiving service operator's organizational structure and operational processes.

The criteria against which an e-Archiving service and its operator are evaluated are those contained in this certification scheme and its normative annexes.

The e-Archiving certification process consists of the steps identified in this paragraph (for more detailed requirements for the certification process, see paragraph 11).

7.2 Application for certification

After designing and implementing an e-Archiving service, the service provider or operator drafts the required documents and supporting descriptions for providing sufficient documented evidence of compliance with eligible requirements and audit criteria.

The service operator shall consequently apply for assessment with the CAB of his choice. With his application, the service operator shall provide a copy of all required documentation and supporting information to allow the CAB to perform a proper application review.

7.3 Scope of certification

The e-Archiving service operator is (part of) a legal person or a public sector body, or a natural person, and shall be unambiguously identified.

The scope of certification shall be described on the basis of the e-Archiving policy governing the service provisioning and identifying overall objectives. The scope shall be delimited by the identification of the e-Archiving profiles covered by this policy. An e-Archiving policy may cover one or more e-Archiving profiles.

7.4 Application review

The CAB shall conduct a review of the information obtained with the application to ensure that it is sufficient for preparing and initiating the certification process. In particular, the CAB shall ensure that the scope of certification sought and the boundaries of the service are unmistakably defined.

The scope of certification is primarily based on the e-Archiving profiles covered by the e-Archiving policy of the applicant. The CAB may guide the applicant in establishing consistent e-Archiving profiles. Such guidance is considered as providing information and clarification about the certification scheme and is not conflicting with impartiality (see clause 4.2.1 of ETSI EN 319 403-1 [9]).

Following the review of the application, when the CAB accepts the certification mission, the CAB shall submit a suitably detailed proposal and audit programme to the applicant.

7.5 e-Archiving services assessment – initial certification

The assessment of an e-Archiving service and its operator shall take the form of an audit carried out against the criteria of this certification scheme. For initial certification, a two- stage audit shall be planned and executed.

The main activities of a stage 1 audit are the appraisal of the service design, the review of the trust service policy and practice statement, and the review of the relevant documented information. The

objectives of a stage 1 audit are to analyse and evaluate the conformity of the service design and to determine the readiness of the service provisioning for a stage 2 audit.

At the end of a stage 1 audit, documented conclusions regarding the planning and preparation of a stage 2 audit, including identification of any areas of concerns (possibly leading to nonconformities) shall be presented to the service operator.

The main purpose of a stage 2 audit is to perform a reality check of the service provisioning system and the organizational and operational controls put in place by the service provider.

In principle, the e-Archiving service in scope of the audit should be ready to operate and subjected to an internal assessment ensuring conformity to the approved design and demonstrating effectiveness of procedures and processes for service provisioning, prior to the start of a stage 2 audit.

The e-Archiving service operator shall make all necessary arrangements for the conduct of the assessment and shall provide access to all relevant documents, records and physical areas, including those of sub-contractors.

7.6 Assessment report

For each audit, a written report shall be provided to the applicant presenting clear and unambiguous audit findings and observations. The report shall comprise an accurate and clear record of the audit activities to enable an informed certification decision.

If, during the assessment process, nonconformities are detected and the evaluation is continued after the provision and execution of a plan of corrective actions, details of each nonconformity, of the corrective actions and their evaluation and acceptance by the audit team, shall be annexed to the report.

The report shall be completed by adding a statement on the conformity of the service and its provisioning and the effectiveness of the organizational and operational processes and a recommendation on certification.

7.7 Assessment review

Prior to making a decision, the CAB shall conduct an independent review of the audit file and the assessment.

7.8 Certification decision and attestation

Based on audit conclusions and the results of the review, the CAB makes a decision to grant certification if there is sufficient audit evidence of conformity, or not to grant certification in all other cases. The CAB shall take a formal decision for granting or refusing certification upon initial assessment (or for expanding or reducing the scope of certification, suspending or restoring, renewing or withdrawing certification in subsequent assessments).

Based on the decision, the CAB shall draft a certificate of conformity and its annexes, unambiguously identifying the certificate holder and clearly delineating the scope of the certification. The e-Archiving profiles in scope of the certification shall be noticeably referenced (title, version and date).

The CAB shall provide to the applicant a complete set of certification documents, including the certificate of conformity and its annexes, the complete assessment report in order to enable, in case of a formal request for qualification of the trust service, the eIDAS supervisory body to evaluate the extensiveness and reliability of the conformity assessment.

The certification shall be granted for a determined period not exceeding 24 months for third party e-Archiving service providers and not exceeding 36 months for operators of e-Archiving services for own behalf. The certification cycle commences on the date of the certification decision.

7.9 Surveillance, expanding scope and recertification.

In order to maintain certification, the service (operator) shall be subject to surveillance by the CAB.

In principle, a certification cycle for third party e-Archiving service providers consists of one surveillance audit in the year following the (re)certification decision, and a recertification audit in the second year and prior to expiration of certification.

For operators of e-Archiving services for their own behalf, a certification cycle consists of two surveillance audits in the first and the second year following the (re)certification decision, and a recertification audit in the third year and prior to expiration of certification.

The objective of a surveillance audit is to perform a follow-up on the (re)certification audit and an effectivity check. The CAB shall evaluate the stability of the service and the service provisioning. The assessment includes inspection of services delivered (sample based case analysis), and the review of records, registrations and loggings (backward looking).

Any modification or alteration to the service shall be evaluated in detail in order to confirm that proper change management procedures are applied, including the required or mandatory notification of changes and modifications.

The objective of a recertification audit is to confirm the stability and the continuing conformity of the e-Archiving service and its operator.

7.10 Modular certification approach

In performing the conformity assessment of e-Archiving services, the CAB may rely on existing certification of e-Archiving solutions or partial services used as building blocks for the e-Archiving service (provisioning), solely under the condition that these certifications have been delivered according to a specific certification scheme accepted by the e-Archive certification scheme owner.

Where the CAB is taking account of certification already granted, it shall have access to sufficient evidence, such as the certification certificate, its annexes and the associated assessment reports and documents. The CAB shall evaluate the extensiveness and consistency of the conformity assessment leading to the certification. The documentation shall support the fulfilling of the statutory requirements and certification criteria.

When applying a modular approach, the CAB shall reference in the assessment report the documents and information forming the basis of its modular analysis, and shall articulate the results of the analysis.

8 Certification criteria for e-Archiving services and service operators

8.1 Certification criteria for e-Archiving services for long-term preservation (LTPS)

Annex A

8.2 Certification criteria for e-Archiving services for digitisation of information (IDS)

Annex B

9 Application for certification

The service operator shall apply for assessment with the CAB of his choice. With his application, the service operator shall provide a copy of all required documentation and supporting information to allow the CAB to perform a proper application review.

10 Complementary requirements

10.1 Subscriber agreement in the case of an operator of e-Archiving services

In general, terms and conditions supplemented by an individual subscriber agreement are used to express the boundaries and the specific rules of the service and its provisioning, as well as to describe the mutual obligations and engagements of the parties involved in a contractual relation. Whereas this situation is common in the case of a third party e-Archiving service provider, it is not viable in the case of an internal e-Archiving service operated on one's own behalf.

For this reason and for the purpose of applying the present certification scheme to the particular situation of an operator of e-Archiving services as defined in paragraph 4, whenever the certification criteria require an element or topic to be included in the "terms and conditions" and/or the "subscriber agreement", this requirement must be read as follows: "the referenced element or topic shall be included in an internal policy or procedural document with the purpose of defining corporate binding rules outlining the agreements between a service operator and any other part of the same entity wanting to use that service".

10.2 Data location

A third party e-Archiving service provider shall document and communicate to the user the location of the storage and processing of the data in a transparent way.

10.3 Termination of agreement

No complementary requirements.

11 Requirements for certification bodies

The CAB has the responsibility to assess sufficient objective evidence upon which to base a certification decision. Conformity assessments shall be carried out in a proportionate manner, avoiding unnecessary burdens for operators. CABs shall perform their activities taking due account of the size of the scope of certification, the sector in which it operates, its structure, the degree of complexity of the technology involved and the nature of the service provisioning.

The CAB shall be organized and operate conformant to the requirements of ISO/IEC 17065 [8], complemented with ETSI EN 319 403-1 [9].

The execution of e-Archiving certification activities should be in compliance with the requirements of ETSI TS 119 403-3 [10].

The CAB shall inform the scheme owner of all initial certifications granted. For each certified operator, the CAB shall inform without undue delay the scheme owner of any subsequent decision modifying the status of the certification (expanding or reducing the scope of certification, suspending or restoring, renewing or withdrawing certification).

By operating this e-Archiving certification scheme, the CAB commits to respect the clauses and requirements of the scheme, and to conduct the certification activities in an impartial, competent and responsible way. CABs shall keep at the disposal of the eiDAS supervisory body the relevant documents concerning the certification of e-Archiving services and its operators.

12 Procedures for Resolving Complaints

12.1 Complaints and appeals about a decision relating to certification.

An operator who wants to appeal to a decision to grant, maintain, suspend, revoke, withdraw or refuse a certificate of conformity to that operator, shall submit the appeal to the CAB who made that decision. The complaint shall be actioned by the CAB in accordance with the applicable clauses of ISO/IEC 17065 [8].

12.2 Complaints about claims on a certificate of conformity.

An entity or individual who has a complaint that relates to the way a service operator refers to his (alleged) certification, may take the complaint to the certification body who granted certification or to the scheme administrator.

12.3 Complaints about a decision made by the Scheme Administrator.

An entity or individual who has a complaint that relates to a decision or an undertaking of the scheme administrator, may take the complaint to the scheme owner.

The scheme owner shall take necessary measures to ensure that the decision to be communicated to the complainant shall be made or approved by a person not previously involved in the subject of the complaint.

13 Ownership and scheme responsibilities

13.1 Ownership

The e-Archiving certification scheme is developed under supervision of:
FOD Economie, K.M.O., Middenstand en Energie
Algemene Directie Kwaliteit en Veiligheid – Dienst Reglementering Metrologie
Vooruitgangstraat 50 — 1210 Brussel
Ondernemingsnr.: 0314.595.348

The e-Archiving certification scheme is distributed freely.

13.2 Certification mark

No certification mark shall be used in conjunction with this e-Archiving certification scheme. Reference to certification is only permitted in written and unambiguous statement.

13.3 Scheme responsibilities

The role of Scheme administrator lies with the Digital Trust team of the FPS Economy.

Accreditation of CABs is a role the national accreditation body in accordance with Regulation (EC) No 765/2008.

Each CAB is responsible for the certificates of conformity that it may issue to a certificate holder.

Certificate holders are responsible for ensuring that certified services continue to comply with the relevant requirements and criteria of the scheme.

14 Disclaimer

Compliance with the e-Archiving certification scheme is not a substitute for the statutory or regulatory requirements applicable to certain specific type of documents or (personal) data.

Moreover, this scheme is based on a user's data protection objective, but does not provide strong technical guarantees or barriers against access by the service provider to the data processed on the service's information system infrastructure: It only allows for the best consideration of the necessary contractual commitments. Users wishing to ensure the technical protection of their data against access by the service provider will therefore have to implement additional means of encryption, under their control, of their data.

15 Annexes

Annex A (Normative): Certification criteria for e-Archiving services for long-term preservation.

Annex B (Normative): Certification criteria for e-Archiving services for digitisation of information.

Annex C (Informative): Definition of terms and abbreviations.

Annex E (Informative): e-Archival profile.

Annex A (Normative)
Certification criteria for e-Archiving services for long-term preservation

1. Introduction

The present annex describes the audit criteria for the assessment and certification of e-Archiving services for long-term preservation of electronic documents or electronic information in a way as to preserve the enclosed information from loss and from any modification other than changes related to its preservation format or storage medium.

By satisfying the audit criteria presented in this annex, the e-Archiving service provider or operator can demonstrate compliance to the applicable statutory requirements for a qualified electronic archiving service and its provider or operator as laid down in Belgian legislative framework.

2. References

2.1. Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

The following referenced documents are necessary for the application of the present annex.

[4] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[5] ISO 14641:2018: “Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications”.

[7] ETSI TS 119 612 (V2.1.1) (2015-07): "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

2.2. Informative references

The following referenced documents are not necessary for the application of the present annex but they assist the user with regard to a particular subject area.

[11] TSI TS 119 511: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques”.

[12] ETSI TS 119 312: “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”.

[13] ETSI TS 119 512: “Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services”.

3. Definition of terms and abbreviations

3.1. Terms

The terms and abbreviations are defined in annex D.

3.2. Abbreviations

The terms and abbreviations are defined in annex D.

3.3. Verbal forms

In the present document, the term “shall” is used to indicate a requirement strictly to be followed and from which no deviation is permitted. The term “should” is used to indicate that among several possibilities one is recommended as particularly suitable.

4. Responsibility

In the context of the present e-Archiving certification scheme, when describing the audit criteria for assessment and certification, the term “e-Archiving service operator (e-AO)” is used either in the sense of third party service provider or in the sense of service operator as described in paragraph 4 of the body text.

The e-Archiving service operator seeking certification according to the present e-Archiving certification scheme has the responsibility of demonstrating fulfilment of the audit criteria.

5. Risk assessment

[A-1] The requirements specified in ETSI EN 319 401 [4] clause 5 shall apply.

6. Policies and practices

6.1. Archiving service practice statement

[A-2] The requirements specified in ETSI EN 319 401 [4] clause 6.1 shall apply

[A-3] The e-AO shall list in its archiving service practice statement the supported archival profiles.

[A-4] The e-AO shall state in its archiving service practice statement how the archiving goals are achieved.

[A-5] The e-AO shall define in its archiving service practice statement how the availability of the submitted data objects and the associated archival evidences is achieved.

[A-6] The e-AO shall identify in its archiving service practice statement the obligations of all external organizations supporting the archival services.

[A-7] The e-AO shall state in its archiving service practice statement the details on the process of requesting export-import package(s).

[A-8] The e-AO shall specify in its archiving service practice statement the production methods of the export-import package(s).

[A-9] The e-AO shall specify in its archiving service practice statement what happens to the data at the end of the preservation period.

[A-10] The requirements specified in ISO 14641:2018 [5] clause 5.4.1 shall accordingly apply.

[A-11] The requirements specified in ISO 14641:2018 [5] clause 5.4.3 shall accordingly apply.

6.2. Terms and conditions

[A-12] The requirements specified in ETSI EN 319 401 [4] clause 6.2 shall apply

[A-13] The e-AO shall state where to find information on the supported archival profiles.

[A-14] When the archive submitter is allowed to take a role in the preservation process (e.g. providing needed validation data), the e-AO shall describe in its terms and conditions under which conditions this can be done, and specify in particular which are the responsibilities taken by the archiving service and the ones that shall be taken by the submitter.

[A-15] The e-AO shall state in its terms and conditions how the request for an export-import package can be done.

[A-16] The e-AO shall state in its terms and conditions the strategy that it will follow when it is unable to collect and verify all the validation data.

[A-17] The e-AO shall provide a subscriber agreement which shall include an acceptance of the terms and conditions.

[A-18] The e-AO shall state in the subscriber agreement who has the right to access to archival objects including archival evidences

[A-19] The e-AO shall state in the subscriber agreement who has the right to request traces on the actions related to the archival objects .

6.3. Information security policy

[A-20] The requirements specified in ETSI EN 319 401 [4] clause 6.3 shall apply.

6.4. Archival profile

[A-21] An archival profile shall be uniquely identified.
See Annex E for guidance regarding the archival profile description.

[A-22] The same archival profile shall apply during the whole preservation period.

[A-23] The archival profile should not change over time, thus all dynamic aspects should be specified outside the archival profile (e.g. the archival evidence policy or signature validation policy).

[A-24] The archival evidence policies or signature validation policies referenced by the archival profile may change over time. However, all versions related to a specific archival profile shall be publicly available, and it shall be clear which version applies at which time.

[A-25] The requirements specified in ISO 14641:2018 [5] clause 5.3 shall accordingly apply.

6.5. Archival evidence policy

[A-26] The archival evidence policy shall contain the description of how the archival evidence is generated including which cryptographic algorithms are used.

[A-27] The archival evidence policy shall contain how the archival evidence can be validated, including:
1) Which trust anchors can be used to validate digital signatures within the archival evidence.
2) Which trust anchors can be used to validate time-stamps within the archival evidence.

[A-28] The archiving service evidence policy, where applicable, shall state how evidence is augmented (see [A-72]).

[A-29] The archival evidence policy shall describe the format of the archival evidence.

[A-30] The archival evidence policy shall state if and, in this case, how, the evidence contains explicit information of the applicable:
a) archiving service;
b) archival evidence policy; or
c) archival profile.

[A-31] During the preservation period, the archiving service shall make sure that the archival evidence can be used to achieve the corresponding archiving goal.

[A-32] The e-AO shall augment the archival evidences before they cannot be used anymore to achieve the corresponding archiving goal, to make sure that the archival evidence can be used.

[A-33] Time-stamps used within the archival evidence shall be provided by a qualified TSA.

[A-34] If the archival evidence policy cannot be identified from the context, the archival evidence policy should be included directly in the archival evidence.

[A-35] If the archival evidence policy is included in the archival evidence, it should be cryptographically protected.

[A-36] The e-Archiving service policy shall have one service digital identifier as defined in clause 5.5.3 of ETSI TS 119 612 [7] which allows to uniquely and unambiguously identify the service within an EU Member States' trusted list.

6.6. Signature validation policy (for qualified electronic signature and qualified electronic seal)

[A-37] If present in the archival profile, the signature validation policy shall state the strategy to how the validation material is selected, e.g. trust anchors, validation model (chain/shell), etc.

[A-38] If the validation data is not submitted by the client, the archiving service shall make its best efforts to collect and verify the validation data according to the signature validation policy supported by the archival profile.

[A-39] If the validation data is submitted by the client, the archiving service should verify the submitted validation data according to the signature validation policy supported by the archival profile, and verify that the submitted validation data is appropriate, otherwise it should collect and verify the appropriate validation data.

[A-40] To extend the ability to validate a digital signature and to maintain its validity status, the archiving service shall, on one side, provide a proof of existence of the signature and of the validation data needed to validate the signature and on the other side a proof of existence of the signed data.

[A-41] In the case of a detached signature, the archiving service shall not allow the client to provide only a hash value of the signed data instead of the signed data itself.

[A-42] The archiving service shall preserve all information needed to check the qualification status of the electronic signature or seal that would not be publicly available until the end of the preservation period.

7. Archival management and operation

7.1. Internal organization

[A-43] The requirements specified in ETSI EN 319 401 [4] clause 7.1 shall apply.

7.2. Human resources

[A-44] The requirements specified in ETSI EN 319 401 [4] clause 7.2 shall apply.

7.3. Asset management

[A-45] The requirements specified in ETSI EN 319 401 [4] clause 7.3 shall apply.

[A-46] The requirements specified in ISO 14641:2018 [5] clause 5.2 shall accordingly apply.

[A-47] The requirements specified in ISO 14641:2018 [5] clause 6 shall be considered.

7.4. Access control

[A-48] The requirements specified in ETSI EN 319 401 [4] clause 7.4 shall apply.

7.5. Cryptographic control

[A-49] The requirements specified in ETSI EN 319 401 [4] clause 7.5 shall apply.

7.6. Physical and environmental security

[A-50] The requirements specified in ETSI EN 319 401 [4] clause 7.6 shall apply.

7.7. Operation security

[A-51] The requirements specified in ETSI EN 319 401 [4] clause 7.7 shall apply.

[A-52] The requirements specified in ISO 14641:2018 [5] clause 5.5.4 shall accordingly apply.

[A-53] The requirements specified in ISO 14641:2018 [5] clause 5.5.5 shall accordingly apply.

[A-54] The requirements specified in ISO 14641:2018 [5] clause 5.5.7 shall accordingly apply.

[A-55] The requirements specified in ISO 14641:2018 [5] clause 5.5.8 shall accordingly apply.

7.8. Network security

[A-56] The requirements specified in ETSI EN 319 401 [4] clause 7.8 shall apply.

[A-57] The archiving service shall be integrated in the IT environment implemented in such a way that all storage access by the client changing the content of the storage shall only be done by the archiving service.

[A-58] The communication channel between the client and the e-AO shall be secured; i.e. the e-AO shall offer a way to be authenticated and the confidentiality of the data shall be ensured.

7.9. Incident management

[A-59] The requirements specified in ETSI EN 319 401 [4] clause 7.9 shall apply.

7.10. Collection of evidence

[A-60] The requirements specified in ETSI EN 319 401 [4] clause 7.10 shall apply.

[A-61] The requirements specified in ISO 14641:2018 [5] clause 5.7.1 shall accordingly apply.

[A-62] The requirements specified in ISO 14641:2018 [5] clause 5.7.2 shall accordingly apply.

[A-63] The requirements specified in ISO 14641:2018 [5] clause 5.7.3 shall accordingly apply.

[A-64] The requirements specified in ISO 14641:2018 [5] clause 5.7.4 shall accordingly apply.

7.11. Business continuity management

[A-65] The requirements specified in ETSI EN 319 401 [4] clause 7.11 shall apply.

7.12. Termination and termination plans

[A-66] The requirements specified in ETSI EN 319 401 [4] clause 7.12 shall apply.

[A-67] The termination plan shall include what happens with the stored archival objects at the termination of the archiving service

7.13. Compliance

[A-68] The requirements specified in ETSI EN 319 401 [4] clause 7.13 shall apply.

[A-69] The requirements specified in ISO 14641:2018 [5] clause 12.1.1 shall accordingly apply.

[A-70] The requirements specified in ISO 14641:2018 [5] clause 12.2 shall accordingly apply.

7.14. Cryptographic monitoring

[A-71] For every supported active archival profile, the e-AO shall monitor the strength of every cryptographic algorithm that was used in connection with this profile. In case, one of the used algorithms or parameters is thought to become less secure or the validity of a relevant certificate is going to expire, it shall either update the related archival evidence policy or create a new archival profile to handle newly submitted archival objects.

[A-72] If one of the algorithms or parameters which were used in an archival evidence, is thought to become less secure or the validity of a relevant certificate is going to expire, the archival evidence shall be augmented by the archiving service according to a new version of the archival evidence policy during the preservation period.

[A-73] For the evaluation of the cryptographic algorithms, ETSI TS 119 312 [12] should be considered.

7.15. Subcontractors

[A-74] The requirements specified in ISO 14641:2018 [5] clause 13 shall be considered.

[A-75] The requirements specified in ISO 14641:2018 [5] clause 14 shall be considered.

8. Archival operations

8.1. General

No specific criteria.

8.2. Scanning

No specific criteria.

8.3. Import / capture

[A-76] The e-AO shall allow the client or another authorized archiving service to request the export-import package(s), containing the preserved data, the evidences and all information needed to validate the evidences.

[A-77] The export-import package(s) shall only be delivered to an authorized legal or natural person

[A-78] The e-AO shall keep records of all released export-import packages including:
1) The date of the event.
2) The criteria that has been used to select the set of archival objects to be included in the export-import package.

[A-79] The requirements specified in ISO 14641:2018 [5] clause 10.1.1 shall accordingly apply.

[A-80] The requirements specified in ISO 14641:2018 [5] clause 10.1.2 shall accordingly apply.

[A-81] The requirements specified in ISO 14641:2018 [5] clause 10.1.3 shall accordingly apply.

[A-82] The requirements specified in ISO 14641:2018 [5] clause 10.1.4 shall accordingly apply.

[A-83] The requirements specified in ISO 14641:2018 [5] clause 10.1.5 shall accordingly apply.

[A-84] The requirements specified in ISO 14641:2018 [5] clause 10.1.6 shall accordingly apply.

[A-85] The requirements specified in ISO 14641:2018 [5] clause 10.1.7 shall accordingly apply.

[A-86] The requirements specified in ISO 14641:2018 [5] clause 10.1.8 shall accordingly apply.

[A-87] The requirements specified in ISO 14641:2018 [5] clause 10.1.9 shall accordingly apply.

[A-88] An archiving service may allow to provide a new version of an already submitted archival object. The newly provided version may be specified only by the difference to the previous version.

8.4. AIP Generation

[A-89] The requirements specified in ISO 14641:2018 [5] clause 10.1.10 shall accordingly apply.

8.5. Access

[A-90] The requirements specified in ISO 14641:2018 [5] clause 11.2.1 shall accordingly apply.

[A-91] The requirements specified in ISO 14641:2018 [5] clause 11.2.3 shall accordingly apply.

[A-92] The requirements specified in ISO 14641:2018 [5] clause 11.2.4 shall accordingly apply.

8.6. Export / Restitution

[A-93] The archival protocol as defined in ETSI TS 119 512 [13] should be used.

[A-94] The protocols shall be protected against unauthorized usage.

[A-95] An archiving service shall allow to retrieve information about the currently and previously supported archival profiles.

[A-96] An archiving service shall allow one or more submission data objects to be preserved under a specific archival profile, and to receive back either an archival object identifier or to receive back immediately an archival evidence.

[A-97] An archiving service may allow to get the traces of all operations related to a specific archival object identifier.

[A-98] An archiving service may allow to search for specific archival objects and retrieve a set of archival object identifiers, which can be used in other operations.

[A-99] An archiving service shall allow to retrieve evidences and/or archival objects.

[A-100] An archiving service should allow to request a set of archival object identifiers, which can be used to retrieve archival objects.

[A-101] The requirements specified in ISO 14641:2018 [5] clause 11.3 shall accordingly apply.

8.7. Disposal

[A-102] An archiving service shall allow to delete stored archival objects. In case of the deletion of the archival evidence, the corresponding submission data objects shall be deleted as well.

[A-103] The archiving service shall assure that stored archival objects can only be deleted before the end of the preservation period when the delete request are submitted together with a justification. Any submitted justification shall be logged together with the information of the deletion request.

[A-104] An archiving service should allow to request a set of archival object identifiers, which can be used to delete archival objects.

[A-105] The requirements specified in ISO 14641:2018 [5] clause 11.4 shall accordingly apply.

Annex B (Normative)
Certification criteria for e-Archiving services for digitisation of information

1. Introduction

The present annex describes the audit criteria for the assessment and certification of e-Archiving services for the scanning of paper-based documents with the aim of digitisation of the contained information, and the creation of a faithful and durable electronic copy of the document.

By satisfying the audit criteria presented in this annex, the e-Archiving service provider or operator can demonstrate compliance to the applicable requirements for an qualified electronic archiving service and its provider or operated as laid down in the Belgian legislative framework.

2. References

2.1. Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

The following referenced documents are necessary for the application of the present annex.

[4] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[6] NF Z42-026:2017 :"Définition et spécifications des prestations de numérisation fidèle de documents sur support papier et contrôle de ces prestations".

[7] ETSI TS 119 612 (V2.1.1) (2015-07): "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

2.2. Informative references

The following referenced documents are not necessary for the application of the present annex but they assist the user with regard to a particular subject area.

[5] ISO 14641:2018: "Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications"

[12] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

3. Definition of terms and abbreviations

3.1. Terms

The terms and abbreviations are defined in annex D.

3.2. Abbreviations

The terms and abbreviations are defined in annex D.

3.3. Verbal forms

In the present document, the term "shall" is used to indicate a requirement strictly to be followed and from which no deviation is permitted. The term "should" is used to indicate that among several possibilities one is recommended as particularly suitable.

4. Responsibility

In the context of the present e-Archiving certification scheme, when describing the audit criteria for assessment and certification, the term “e-Archiving service operator (e-AO)” is used either in the sense of third party service provider or in the sense of service operator as described in paragraph 4 of the body text.

The e-Archiving service operator seeking certification according to the present e-Archiving certification scheme has the responsibility of demonstrating fulfilment of the audit criteria.

5. Risk assessment

[B-1] The requirements specified in ETSI EN 319 401 [4] clause 5 shall apply.

6. Policies and practices

6.1. Archiving service practice statement

[B-2] The requirements specified in ETSI EN 319 401 [4] clause 6.1 shall apply

[B-3] The e-AO shall list in its archiving service practice statement the supported archival profiles.

[B-4] The e-AO shall state in its archiving service practice statement how the archiving goals are achieved.

[B-5] The e-AO shall identify in its archiving service practice statement the obligations of all external organizations supporting the archiving service services including the applicable policies and practices.

[B-6] The objectives and requirements specified in NF Z 42-026 0 clause 4.2 shall accordingly apply.

[B-7] The objectives and requirements specified in NF Z 42-026 [6] clause 4.3 shall accordingly apply.

Note: When the clauses of NF Z 42-026 [6] require an item to be clarified in the archiving service agreement (convention de numérisation), these items must at least be incorporated in one of the following documents: the archiving service practice statement; the terms and conditions; or the subscriber agreement. See also paragraph 10.1 of the body text.

6.2. Terms and conditions

[B-8] The requirements specified in ETSI EN 319 401 [4] clause 6.2 shall apply

[B-9] The e-AO shall state where to find information on the supported archival profiles.

[B-10] The e-AO shall provide a subscriber agreement which shall include an acceptance of the terms and conditions.

6.3. Information security policy

[B-11] The requirements specified in ETSI EN 319 401 [4] clause 6.3 shall apply.

6.4. Archival profile

[B-12] An archival profile shall be uniquely identified.
See Annex E for guidance regarding the archival profile description.

[B-13] For an IDS with temporary storage, the archival profile shall contain the archival evidence retention period, i.e. the time period during which the electronic document can be retrieved from the archiving service by the submitter.

[B-14] The expected evidence duration shall be based on the estimation of the suitability of cryptographic algorithms.

[B-15] The expected evidence duration should be based on ETSI TS 119 312 [12].

6.5. Archival evidence policy

[B-16] The archival evidence policy shall contain the description of how the archival evidence is generated including which cryptographic algorithms are used.

[B-17] The archival evidence policy shall contain the description of which trust service providers (e.g. digital signature creation service or time stamping authorities, certificate status authorities) may be used by the archiving service.

[B-18] The archival evidence policy shall contain how the archival evidence can be validated, including:
1) Which trust anchors can be used to validate digital signatures within the archival evidence.
2) Which trust anchors can be used to validate time-stamps within the archival evidence.

[B-19] The archival evidence policy shall describe the format of the archival evidence.

[B-20] The archival evidence policy shall state if and, in this case, how, the evidence contains explicit information of the applicable:
a) archiving service;
b) archival evidence policy; or
c) archival profile

[B-21] Time-stamps used within the archival evidence shall be provided by a qualified TSA.

[B-22] If the archival evidence policy cannot be identified from the context, the archival evidence policy should be included directly in the archival evidence.

[B-23] If the archival evidence policy is included in the archival evidence, it should be cryptographically protected

[B-24] The archiving service (policy) shall have one service digital identifier as defined in clause 5.5.3 of ETSI TS 119 612 [7] which allows to uniquely and unambiguously identify the service within an EU Member State trusted list.

[B-25] The objectives and requirements specified in NF Z 42-026 [6] clause 8.1 shall accordingly apply.

6.6. Signature validation policy

Not applicable.

7. Archival management and operation

7.1. Internal organization

[B-26] The requirements specified in ETSI EN 319 401 [4] clause 7.1 shall apply.

7.2. Human resources

[B-27] The requirements specified in ETSI EN 319 401 [4] clause 7.2 shall apply.

7.3. Asset management

[B-28] The requirements specified in ETSI EN 319 401 [4] clause 7.3 shall apply.

[B-29] The objectives and requirements specified in NF Z 42-026 [6] clause 5.2 shall accordingly apply.

7.4. Access control

[B-30] The requirements specified in ETSI EN 319 401 [4] clause 7.4 shall apply.

7.5. Cryptographic control

[B-31] The requirements specified in ETSI EN 319 401 [4] clause 7.5 shall apply.

7.6. Physical and environmental security

[B-32] The requirements specified in ETSI EN 319 401 [4] clause 7.6 shall apply.

[B-33] The objectives and requirements specified in NF Z 42-026 [6] clause 5.1.3 shall accordingly apply.

7.7. Operation security

[B-34] The requirements specified in ETSI EN 319 401 [4] clause 7.7 shall apply.

7.8. Network security

[B-35] The requirements specified in ETSI EN 319 401 [4] clause 7.8 shall apply.

[B-36] The communication channel between the preservation client and the e-AO shall be secured; i.e. the e-AO shall offer a way to be authenticated and the confidentiality of the data shall be ensured.

7.9. Incident management

[B-37] The requirements specified in ETSI EN 319 401 [4] clause 7.9 shall apply.

7.10. Collection of evidence

[B-38] The requirements specified in ETSI EN 319 401 [4] clause 7.10 shall apply.

7.11. Business continuity management

[B-39] The requirements specified in ETSI EN 319 401 [4] clause 7.11 shall apply.

7.12. Termination and termination plans

[B-40] The requirements specified in ETSI EN 319 401 [4] clause 7.12 shall apply.

7.13. Compliance

[B-41] The requirements specified in ETSI EN 319 401 [4] clause 7.13 shall apply.

7.14. Cryptographic monitoring

[B-42] For the evaluation of the cryptographic algorithms, ETSI TS 119 312 [12] or equivalent shall be considered.

7.15. Subcontractors

No specific criteria.

8. Archival operations

8.1. General

No specific criteria.

8.2. Scanning

[B-43] The objectives and requirements specified in NF Z 42-026 [6] clause 6 shall accordingly apply.

[B-44] The objectives and requirements specified in NF Z 42-026 [6] clause 8.2 shall accordingly apply.

[B-45] Viewing and reading applications shall be independent from the tools that were used to create archived documents. Therefore, an electronic document should be captured in a software and hardware environment different to the environment used for viewing or reading.

[B-46] An IDS which stores the data to be preserved after the evidence has been created should state the reasons for doing so in its terms and conditions.

8.3. Import / capture

[B-47] The objectives and requirements specified in NF Z 42-026 [6] clause 7.1 shall accordingly apply.

[B-48] The objectives and requirements specified in NF Z 42-026 [6] clause 7.2 shall accordingly apply.

8.4. AIP Generation

[B-49] The objectives and requirements specified in NF Z 42-026 [6] clause 7.3 shall accordingly apply.

[B-50] The objectives and requirements specified in NF Z 42-026 [6] clause 7.4 shall accordingly apply.

[B-51] The objectives and requirements specified in NF Z 42-026 [6] clause 7.5 shall accordingly apply.

[B-52] The objectives and requirements specified in NF Z 42-026 [6] clause 7.6 shall accordingly apply.

[B-53] The objectives and requirements specified in NF Z 42-026 [6] clause 7.7 shall accordingly apply.

[B-54] The objectives and requirements specified in NF Z 42-026 [6] clause 7.8 shall accordingly apply.

8.5. Access

No specific criteria.

8.6. Export / Restitution

[B-55] The e-AO shall allow the client or another authorized archiving service to request the export package(s), containing the preserved data, the evidences and all information needed to validate the evidences.

[B-56] The export package(s) shall only be delivered to an authorised legal or natural person.

[B-57] The objectives and requirements specified in NF Z 42-026 [6] clause 7.9 shall accordingly apply.

[B-58] The objectives and requirements specified in NF Z 42-026 [6] clause 7.10 shall accordingly apply.

[B-59] The objectives and requirements specified in NF Z 42-026 [6] clause 8.3.1 shall accordingly apply.

[B-60] The objectives and requirements specified in NF Z 42-026 [6] clause 8.3.2 shall accordingly apply.

8.7. Disposal

[B-61] The objectives and requirements specified in NF Z 42-026 [6] clause 7.12 shall accordingly apply.

Annex C (Informative)
Definition of terms and abbreviations

1. Terms

For the purposes of the present document, the following terms apply:

applicant: service provider or service operator seeking certification of its trust services

archival evidence: evidence produced by the electronic archiving service which can be used to demonstrate that one or more archiving goals are met for a given archival object

archival evidence policy: set of rules that specify the requirements and the internal process to generate or how to validate archival evidence

archival evidence retention period: the time period during which the evidences that are produced can be retrieved from the preservation service

archival profile: uniquely identified set of implementation details (characteristics, procedures and rules) relevant to a specific type of submission (data) object linked to one or more archiving goals which outlines how archival evidences are generated and validated

archiving goal: providing proofs of existence and integrity of data during a predefined preservation period

audit conclusions: outcome of an audit after consideration of the audit objectives and all audit findings

audit criteria: set of policies, procedures or requirements used as a reference against which objective evidence is compared

audit evidence: records, statement of facts or other information which are relevant to the audit criteria and verifiable

audit findings: results of the evaluation of the collected audit evidence against audit criteria.
Note: audit findings indicate conformity or nonconformity

audit programme: arrangement for a set of one or more audits planned for a specific time frame and directed towards a specific purpose

certification criteria: audit criteria listed in the certification scheme

certification scheme: certification system related to specified services to which the same specified requirements, specific rules and procedures apply

(archival) client: component or a piece of software which interacts with a electronic archiving service via the archival protocol

conformity assessment body: body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides

data object: actual binary data being operated on by an application and which may be associated with additional information like an identifier, the encoding, size or type

electronic archiving service: trust service consisting in the retention of electronic data or the digitisation of paper documents, offered by a trust service provider within the meaning of the eIDAS Regulation or operated on its own behalf by a public sector body, or a natural or legal person

electronic archiving service for digitisation of information (IDS): electronic archiving service for the scanning of paper-based documents with the aim of digitisation of the contained information, and the creation of a faithful and durable electronic copy of the document

electronic archiving service for long-term preservation (LTPS): electronic archiving service for retaining electronic documents or electronic information in a way as to preserve the enclosed information from loss and from any modification other than changes related to its preservation format or storage medium

electronic archiving service policy: trust service policy for an electronic archiving service

electronic archiving service practice statement: trust service practice statement for an electronic archiving service

e-Archiving service: electronic archiving service

e-Archiving policy: electronic archiving service policy:

effectiveness: extent to which planned activities are realized and planned results achieved

eIDAS supervisory body: the public sector body designated by the Belgian Government for supervisory tasks in accordance with Section 2 and Section 3 of the eIDAS Regulation

electronic document :any content stored in electronic form

evaluation: combination of the selection and determination functions of conformity assessment activities

expected evidence duration: duration during which the archiving service expects that the archival evidence can be used to achieve the goal

export-import package: information extracted from the preservation service including the submission data object, the preservation evidence and preservation-related metadata, allowing another preservation service to import it in order to continue to achieve the archiving goal based on this information.

preservation period: duration during which a long-term preservation service preserves the submitted archival objects and the associated evidences

process: set of interrelated or interacting activities that use inputs to deliver an intended result

protocol: protocol to communicate between the electronic archiving service and a client

qualified electronic archiving service: electronic archiving service compliant to the applicable requirements of title 2 and annexe I of book XII of the Belgian "Code de droit économique - Wetboek van economisch recht"

requirement: need or expectation that is stated, generally implied or obligatory

scheme owner: organization responsible for developing and maintaining a specific certification scheme

scope of certification: extent and boundaries of a certified electronic archiving service, identifying the archival profiles for which certification is granted

submission (data) object or **submitted (data) object**: original (data) object provided by the submitter or the client
Note: in case of an e-Archiving service for digitisation of information: paper-based document(s)"

submitter: legal or natural person using the archival client to submit the submission data object

subscriber: in case of a third party service provider: legal or natural person bound by agreement with an electronic archiving trust service provider to any user obligations;
in case of a service operator: (part of) a legal person or a public sector body, or a natural person, bound to any user obligations by the archival policy and related corporate procedures

time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

time-stamping authority: trust service provider which issues time-stamps using one or more time-stamping units

2. Abbreviations

For the purposes of the present document, the following abbreviations apply:

CAB	Conformity Assessment Body
e-AO	e-Archiving service operator
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
IDS	e-Archiving service for digitisation of information
LPS	e-Archiving service for long-term preservation
TSA	Time stamping authority

Annex C: Definition of terms and abbreviations

Annex E (Informative)
e-Archival profile

1. Introduction

For the purpose of the present certification scheme an archival profile is defined as a set of implementation details like characteristics, procedures and rules, relevant to a specific type of submission object linked to one or more archiving goals and which outlines how archival evidences are generated and validated.

2. Objectives

2.1. Archival profile objectives

The first objective of the archival profile is to identify the essential characteristics of the submission object in order to be suitable for being processed by the e-Archiving services. In general, these characteristics may contain qualifying (shall have), optional (may have) and disqualifying (shall not have) features.

A second objective of the archival profile to identify one or more archiving goals that can be achieved by the related e-Archiving service. An archiving goal may be expressed by referencing a specific legal framework, or by specifying the boundaries of the preservation period.

An archiving goal is closely linked to, and sometimes dependent of the archival evidence policy, and if applicable the signature validation policy that are applicable to the profile described. For that reason, the archival profile shall explicitly identify the archival evidence policy and the signature validation policy that shall be applied by the e-Archiving service operator for this particular archival profile.

A further objective of the archival profile is to identify or describe the import-export procedures and other relevant procedures detailing specifics of the service provisioning and practicalities.

2.2. Archival scheme

One or more archival profile may be grouped in an archival scheme combining generic set of procedures and rules commonly applicable to all profiles in scope of the archival scheme.

3. Identification and preservation

An archival profile shall be uniquely identified and kept accessible for an appropriate period of time for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of archives. Such preservation may be done electronically.

4. Elements of an archival profile

4.1. An identifier uniquely identifying the archival profile.

4.2. Qualifying and disqualifying and, if applicable, optional characteristics, including aspects of confidentiality and access rights.

4.3. The supported input formats.

4.4. The metadata associated with the submission objects.

4.5. The supported output formats.

4.6. Format conversion operations that shall or can be used on the submitted objects or archival objects. If no such operations are foreseen, this shall be stated explicitly in the archival profile.

4.7. If applicable, other supported operations that may be applied to submitted or archival objects.

4.8. Transfer procedures and/or protocols (e.g. on termination of the subscriber agreement).

4.9. Disposal schedules and procedures (e.g. on authorized request of the submitter).

4.10. (Reference to) the archival evidence policy and supported evidence formats.

4.11. (Reference to) the signature validation policy if applicable. If (preservation of) signature validation (data) is not part of the e-Archiving service for this archival profile, this shall be stated explicitly in the archival profile.

4.12. Archival goals intended to be met by the archival profile, including at minimum the intended preservation period.

4.13. Indication of the type of storage media used for preservation of archival objects and its maintenance.

4.14. Validity period, in terms date and time of activation (operational start date) and, if applicable, planned date and time of deactivation (end date).

One or more of these elements may be covered by a reference to (a clause of) a specific document or procedure, identified by name, date of publication and/or edition number or version number. The referenced passages shall remain unchanged and readily available to the subscriber during the entire preservation period and the length of the subscriber agreement.