KPMG Advisory
Luchthaven Brussel Nationaal 1K
B- 1930 Zaventem

Tel. +32 (0)2 708 43 00
Fax +32 (0)2 708 43 99
www.kpmg.be

KPMG e-Archiving Certification Scheme for services relating to long term preservation of digital signatures or general data using digital signature techniques

Version: v1.2-1
Date: 1/12/2023

Zetel - Siège:
Luchthaven Brussel Nationaal 1K
B-1930 Zaventem

KPMG Advisory BV/SRL
Ondernemingsnummer / Numéro d'entreprise 0439.819.279
BTW - TVA BE 0439.819.279
RPR Brussel - RPM Bruxelles
IBAN : BE 65 4377 5158 1296
BIC: KREDBEBB

KPMG Advisory
Luchthaven Brussel Nationaal 1K
B- 1930 Zaventem

Tel. +32 (0)2 708 43 00
Fax +32 (0)2 708 43 99
www.kpmg.be

Document Version History

Date	Version	Evolution	Author
3/8/2022	1.0	Initial	Dirk Timmerman
17/10/2022	1.1	Correction of typos + add Annex with details of the requirements	Dirk Timmerman
7/2/2023	1.2	3. Scope : additional paragraph to clarify link with EU and BE legislation ; 4.1 Regulatory framework and 10 Requirements for certification bodies : deleted reference to Royal Decree of 29/3/2019 - added reference to ETSI TS 119 403-3 10. Requirements for certification bodies : added reference to ETSI TS 119 403-3	Dirk Timmerman
1/12/23	1.2-1	Annex A - added : REQ-7.3.2-02 ; REQ-7.3.2-03; REQ-7.8-14A; REQ-7.8-16; REQ-7.8-17 - deleted : REQ-6.1-12	Dirk Timmerman

Zetel - Siège:
Luchthaven Brussel Nationaal 1K
B-1930 Zaventem

KPMG Advisory BV/SRL
Ondernemingsnummer / Numéro d'entreprise 0439.819.279
BTW - TVA BE 0439.819.279
RPR Brussel - RPM Bruxelles
IBAN : BE 65 4377 5158 1296
BIC: KREDBEBB

Table of contents

1. Introduction

On 21 March 2021, the FPS Economy has published its first version of the *BE e-Archiving Certification Scheme*, in order to facilitate 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 as a response to the eIDAS Regulation (see section 4.1), although the latter does not include e-Archiving services.
Trust Service Providers that have received a certificate from an accredited Conformity Assessment Body can be put by the FPS Economy on the Belgian list of Qualified Trust Service Providers but cannot be put an the EU list of Qualified Trust Service Providers as the service for "electronic archives" is not included in the list of the eIDAS defined trust services.
KPMG Certification has identified in the market a need of Trust Service Providers of long-term preservation of digital signatures to be put on the EU list of Qualified Trust Service Providers and has therefore developed this current KPMG e-Archiving Certification Scheme. This Scheme can also be used to have Trust Service Providers be put on the BE list of Qualified Trust Services Providers for the delivery of services relating to the long-term preservation of general data using digital signature techniques.

2. Objective

The present document describes a scheme for the assessment and certification of the e-Archiving services described in the **Scope** paragraph (see section 3).

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 **Regulatory framework** (see section 4). The certification scheme also contains a description of the operation of KPMG Certification as a conformity assessment body (CAB) for assessing and certifying the conformity of e-Archiving services.

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 regulatory requirements of the services in scope of the document;
- The clarification of how KPMG Certification seeks to operate the e-Archiving certification scheme.

The criteria stated in the KPMG e-Archiving certification scheme are primarily based on the requirements of the ETSI TS 119 511 for long term preservation with storage (thus excluding long term preservation with temporarily storage and without storage).

3. 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 **long-term preservation with storage of digital signatures, seals and time stamps**
- The **long-term preservation with storage of general data using digital signature techniques**

The service operators in scope are:

- **Third party trust service provider**s as defined in article 3 of the eIDAS Regulation (see section 4) 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.

The issuance of a certificate based on this certification scheme together with the related Certification Audit Report can be the basis of the request to become recognized by the Supervisory Body (SPE Economy) as a qualified Trust Service Provider of:

- Qualified preservation services for qualified electronic signatures (EU regulation 910/2014 article 34)
- Qualified preservation services for qualified electronic seals (EU regulation 910/2014 article 40)
- Qualified long-term preservation e-Archiving services (Belgian Digital Act, Wetboek van Economische Recht - boek XII/Code de Droit Economique – Livre II – Title 2)

4. Regulatory framework and references

4.1 Regulatory framework

The e-Archiving certification scheme is predominantly drafted for facilitating the certification of e-Archiving services (as defined in the **Scope** paragraph– section 3) in view of its qualification according to the provisions as described in:

a) the EU regulatory framework for services relating to **long term preservation with storage of digital signatures, seals and time stamps**
   - 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.

b) the Belgian regulatory framework for services relating to **long term preservation with storage of general data using digital signature techniques**
   - Wetboek van Economisch Recht – Boek XII – Titel 2
     Code de Droit Economique – Livre XII – Titre 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.

4.2 Normative references

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

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

(2) 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".

(3) ISO/IEC 17065: "Conformity assessment – Requirements for bodies certifying products, processes and services".

(4) 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".

(5) ETSI TS 119 403-3: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessmentbodies assessing EU qualified trust service providers".

4.3 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.

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

(2) ETSI TS 119 512: "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services".

5. Definition of terms and abbreviations

5.1 Terms (see annex A)

5.2 Abbreviations (see annex A)

5.3 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".

6. Certification of electronic archiving services

6.1 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 **Regular framework** (see section 4.1).
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.
The e-Archiving certification process consists of the steps identified in this paragraph.

6.2 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 KPMG Certification. With his application, the service operator shall provide a copy of all required documentation and supporting information to allow the KPMG Certification to perform a proper application review.

6.3 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 limited to the services described above in the **Scope** paragraph (section 3) and shall be described based on 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.

6.4 Application review

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

6.5 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.

6.6 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.

6.7 Assessment review

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

6.8 Certification decision and attestation

Based on audit conclusions and the results of the review, KPMG Certification makes a decision to grant certification if there is sufficient audit evidence of conformity, or not to grant certification in all other cases.
KPMG Certification 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, KPMG Certification 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).
KPMG Certification 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.

6.9 Surveillance, expanding scope and recertification.

To maintain certification, the service (operator) shall be subject to surveillance by KPMG Certification.

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. KPMG Certification 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.

6.10 Modular certification approach

In performing the conformity assessment of e-Archiving services, KPMG Certification 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 FPS Economy.
Where KPMG Certification 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. KPMG Certification shall evaluate the extensiveness and consistency of the conformity assessment leading to the certification. The documentation shall support the fulfilling of the regulatory requirements and certification criteria.
When applying a modular approach, KPMG Certification 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.

7. Certification criteria for e-Archiving services and service operators

For the certification criteria for the e-Archiving services as described in the **Scope** paragraph (section 3), we are referring to the requirements stated in the following sections of ETSI TS 119 511 V1.1.1 (2019-06), excluding the requirements relating to long term preservation "With Temporary Storage" (WTS) and "Without Storage" (WOS):

5. Risk assessment
6. Policies and practices
7. PSP management and operation
8. Operational and notification protocols
9. Preservation process

Annex A
(see **Annex A** with an Overview of applicable requirements)

8. Application for certification

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

9. Complementary requirements

9.1 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 the **Scope** paragraph (section 3), 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".

9.2 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.

9.3 Termination of agreement

No complementary requirements.

10. Requirements for certification bodies

KPMG Certification shall be organized and operate conformant to the requirements of ISO/IEC 17065, complemented with ETSI EN 319 403-1.

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

11. Ownership and scheme responsibilities

11.1 Ownership

This e-Archiving certification scheme is developed by KPMG Certification,
Luchthaven Brussel national 1K – B-1930 Zaventem
Ondernemingsnummer.: 0444.646.713
This e-Archiving certification scheme is distributed freely.

11.2 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.
Certificate holders are responsible for ensuring that certified services continue to comply with the relevant requirements and criteria of the scheme.

12. 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.

13. Annexes

Annex A (Normative): Overview of applicable requirements
Annex B (Informative): Definition of terms and abbreviations.
Annex C (Informative): e-Archival profile.

Annex A (Normative)
Overview of applicable requirements

Category	Subcategory	ETSI TS 119511	ETSI 319401
Risk assessment	Risk assessment	OVR-5-01	REQ-5-01 REQ-5-02 REQ-5-03 REQ-5-04 REQ-5-05
Policies & practices	Preservation service practice statement	OVR-6.1-01	REQ-6.1-01 REQ-6.1-02 REQ-6.1-03A REQ-6.1-04 REQ-6.1-05A REQ-6.1-06 REQ-6.1-07 REQ-6.1-08 REQ-6.1-09A REQ-6.1-10 REQ-6.1-11
		OVR-6.1-02 OVR-6.1-03 OVR-6.1-04 OVR-6.1-05 OVR-6.1-06 OVR-6.1-07 OVR-6.1-08 OVR-6.1-09	
	Terms and conditions	OVR-6.2-01	REQ-6.2-01 REQ-6.2-02 REQ-6.2-03 REQ-6.2-04 REQ-6.2-05 REQ-6.2-06
		OVR-6.2-02 OVR-6.2-03 OVR-6.2-04 OVR-6.2-05 OVR-6.2-06 OVR-6.2-07 OVR-6.2-08	
	Information security policy	OVR-6.3-01	REQ-6.3-01 REQ-6.3-02 REQ-6.3-03

Category	Subcategory	ETSI TS 119511	ETSI 319401
			REQ-6.3-04 REQ-6.3-05 REQ-6.3-06 REQ-6.3-07 REQ-6.3-08 REQ-6.3-09 REQ-6.3-10
	Preservation profiles	OVR-6.4-01 OVR-6.4-02 OVR-6.4-03 OVR-6.4-04 OVR-6.4-09 OVR-6.4-10 OVR-6.4-11 OVR-6.4-13 OVR-6.4-14	
	Preservation evidence policy	OVR-6.5-01 OVR-6.5-02 OVR-6.5-03 OVR-6.5-04 OVR-6.5-05 OVR-6.5-06 OVR-6.5-07 OVR-6.5-08 OVR-6.5-09	
	Signature validation policy	OVR-6.6-01 OVR-6.6-02 OVR-6.6-03	
	Subscriber agreement	OVR-6.7-01 OVR-6.7-02 OVR-6.7-03 OVR-6.7-04 OVR-6.7-05	
PSP management and operation	Internal organization	OVR-7.1-01	REQ-7.1.1-01 REQ-7.1.1-02 REQ-7.1.1-03 REQ-7.1.1-04 REQ-7.1.1-05 REQ-7.1.1-06 REQ-7.1.1-07 REQ-7.1.1-08 REQ-7.1.1-09 REQ-7.1.1-10 REQ-7.1.2-01

Category	Subcategory	ETSI TS 119511	ETSI 319401
	Human resources	OVR-7.2-01	REQ-7.2-01 REQ-7.2-02 REQ-7.2-03 REQ-7.2-04 REQ-7.2-05 REQ-7.2-06 REQ-7.2-07 REQ-7.2-10 REQ-7.2-11 REQ-7.2-12 REQ-7.2-13 REQ-7.2-14 REQ-7.2-15 REQ-7.2-16A REQ-7.2-16B REQ-7.2-17
	Asset Management	OVR-7.3-01	REQ-7.3.1-01 REQ-7.3.1-02 REQ-7.3.2-01 REQ-7.3.2-02 REQ-7.3.2-03
	Access control	OVR-7.4-01	REQ-7.4-01 REQ-7.4-04A REQ-7.4-05 REQ-7.4-06 REQ-7.4-07 REQ-7.4-08 REQ-7.4-09 REQ-7.4-10
	Cryptographic control	OVR-7.5-01	REQ-7.5-01
		OVR-7.5-02 OVR-7.5-03 OVR-7.5-04 OVR-7.5-05 OVR-7.5-06 OVR-7.5-07	
	Physical & environmental security	OVR-7.6-01	REQ-7.6-01 REQ-7.6-02 REQ-7.6-03 REQ-7.6-04 REQ-7.6-05
	Operation Security	OVR-7.7-01	REQ-7.7-01 REQ-7.7-02

Category	Subcategory	ETSI TS 119511	ETSI 319401
			REQ-7.7-03 REQ-7.7-04 REQ-7.7-05 REQ-7.7-08 REQ-7.7-09
	Network security	OVR-7.8-01	REQ-7.8-01 REQ-7.8-02 REQ-7.8-03 REQ-7.8-04 REQ-7.8-05 REQ-7.8-06 REQ-7.8-07 REQ-7.8-08 REQ-7.8-09 REQ-7.8-10 REQ-7.8-11A REQ-7.8-12 REQ-7.8-13 REQ-7.8-14 REQ-7.8-14A REQ-7.8-15 REQ-7.8-16 REQ-7.8-17
		OVR-7.8-02	
	Incident management	OVR-7.9-01	REQ-7.9-01 REQ-7.9-02 REQ-7.9-03 REQ-7.9-04 REQ-7.9-05 REQ-7.9-06 REQ-7.9-07 REQ-7.9-08 REQ-7.9-09 REQ-7.9-10 REQ-7.9-11 REQ-7.9-12
	Collection of evidence	OVR-7.10-01	REQ-7.10-01 REQ-7.10-02 REQ-7.10-03 REQ-7.10-04 REQ-7.10-05 REQ-7.10-06 REQ-7.10-07

Category	Subcategory	ETSI TS 119511	ETSI 319401
			REQ-7.10-08
		OVR-7.10-02	
	Business continuity mgt	OVR-7.11-01	REQ-7.11-01 REQ-7.11-02
	TSP Termination & termination plans	OVR-7.12-01	REQ-7.12-01 REQ-7.12-02 REQ-7.12-03 REQ-7.12-04 REQ-7.12-05 REQ-7.12-06 REQ-7.12-07 REQ-7.12-08 REQ-7.12-09 REQ-7.12-10 REQ-7.12-11
		OVR-7.12-02	
	Compliance	OVR-7.13-01	REQ-7.13-01 REQ-7.13-02 REQ-7.13-03 REQ-7.13-04 REQ-7.13-05
	Cryptographic monitoring	OVR-7.14-01 OVR-7.14-02 OVR-7.14-03	
	Augmentation of preservation evidences	OVR-7.15-01 OVR-7.15-02 OVR-7.15-03	
	Export-import package	OVR-7.16-01 OVR-7.16-02 OVR-7.16-03 OVR-7.16-04	
Operational and notification protocols	Preservation protocol	PRP-8.1-01 PRP-8.1-02 PRP-8.1-03 PRP-8.1-04 PRP-8.1-05 PRP-8.1-06 PRP-8.1-07 PRP-8.1-08 PRP-8.1-09	

Category	Subcategory	ETSI TS 119511	ETSI 319401
		PRP-8.1-10 PRP-8.1-11 PRP-8.1-12 PRP-8.1-13 PRP-8.1-14	
	Notification protocol	OVR-8.2-01 OVR-8.2-02 OVR-8.2-03	
Preservation process	Preservation evidences	OVR-9.2-01 OVR-9.2-02 OVR-9.2-03 OVR-9.2-04 OVR-9.2-05	
	Preservation of digital signatures	OVR-9.3-01 OVR-9.3-02 OVR-9.3-03 OVR-9.3-04 OVR-9.3-05 OVR-9.3-06 OVR-9.3-07 OVR-9.3-08	
Annex A	Qualified preservation service for QES as defined by article 34 the Regulation (EU) No 910/2014	OVR-A-00 OVR-A-01 OVR-A-02 OVR-A-03 OVR-A-04	

Annex B (Informative)
Definition of terms and abbreviations

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 evidence 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 evidence 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

Zetel - Siège:
Luchthaven Brussel Nationaal 1K
B-1930 Zaventem

KPMG Advisory BV/SRL
Ondernemingsnummer / Numéro d'entreprise 0439.819.279
BTW - TVA BE 0439.819.279
RPR Brussel - RPM Bruxelles
IBAN : BE 65 4377 5158 1296
BIC: KREDBEBB

electronic archiving service: trust service consisting in the retention of electronic data, 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 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 evidence

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

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
LPS	e-Archiving service for long-term preservation
TSA	Time stamping authority

Annex C (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 evidence is generated and validated.

2. Objectives

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.

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

- An identifier uniquely identifying the archival profile.
- Qualifying and disqualifying and, if applicable, optional characteristics, including aspects of
- confidentiality and access rights.
- The supported input formats.
- The metadata associated with the submission objects.
- The supported output formats.
- 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.
- If applicable, other supported operations that may be applied to submitted or archival objects.
- Transfer procedures and/or protocols (e.g. on termination of the subscriber agreement).
- Disposal schedules and procedures (e.g. on authorized request of the submitter).
- (Reference to) the archival evidence policy and supported evidence formats.
- (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.
- Archival goals intended to be met by the archival profile, including at minimum the intended preservation period.
- Indication of the type of storage media used for preservation of archival objects and its maintenance.
- 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.