

STN P	Funkčné požiadavky na služby elektronickej archivácie	STN P CEN/TS 18170 97 4219
------------------	--	--

Functional requirements for the electronic archiving services

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 07/25

Táto predbežná slovenská technická norma je určená na overenie. Prípadné pripomienky pošlite do mája 2027 Úradu pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.

Obsahuje: CEN/TS 18170:2025

140792

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2025
Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov.

TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

CEN/TS 18170

May 2025

ICS 01.140.20; 35.240.30; 37.080

English Version

**Functional requirements for the electronic archiving
services**

Exigences fonctionnelles pour les services d'archivage
électronique

Richtlinien und funktionale Anforderungen an den
elektronischen Archivierungsdienst

This Technical Specification (CEN/TS) was approved by CEN on 13 May 2025 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword	4
Introduction	5
1 Scope.....	6
2 Normative references.....	6
3 Terms and definitions	6
3.1 Terms related to electronic trust service.....	6
3.2 Terms related to digital objects.....	8
3.3 3.3 Terms related to electronic archiving.....	9
4 Symbols and abbreviated terms.....	10
5 Position statement	10
6 Policies and practices.....	11
6.1 Policy and practice statement.....	11
6.2 Terms and conditions.....	12
6.3 Information security policy.....	12
6.4 Agreements.....	12
6.4.1 General.....	12
6.4.2 Service agreement	12
6.4.3 Submission agreement	14
7 Trust Service Provider management and operation	15
7.1 General.....	15
7.2 Internal organization	15
7.3 Human resources.....	15
7.4 Asset management	15
7.5 Access control.....	15
7.6 Cryptographic controls and monitoring.....	16
7.7 Physical and environmental	16
7.8 Operation	16
7.9 Network.....	16
7.10 Vulnerabilities and incident management.....	16
7.11 Collection of evidence	16
7.12 Business continuity management.....	16
7.13 EATSP termination and termination plans	16
7.14 Compliance.....	16
7.15 Supply Chain	17
8 Information packages — Information Package Format.....	17
9 Submission Information Package	17
9.1 General.....	17
9.2 Submission Information Package Format.....	17
9.3 Components of the SIP	17
9.4 Other metadata in the SIP	17
9.5 Content Data Object Formats.....	18
9.6 Transfer submission.....	18
9.7 Receive submission.....	18
9.8 Audit submission	18
9.8.1 General.....	18
9.8.2 Scope of verification defined in the “submission agreement”	18
10 Archival Information Package.....	19

CEN/TS 18170:2025 (E)

10.1	General	19
10.2	AIP Generation.....	20
10.2.1	General	20
10.2.2	Archival Information Package Format.....	20
10.2.3	Components of the AIP.....	20
10.2.4	Transformation of SIPs into AIPs.....	20
10.2.5	Transformation of Content Data Objects into other formats.....	20
10.2.6	Map and list of archiving formats for Content Data Objects	21
10.3	Storage infrastructure and localization	21
10.4	Storage security - AIP Integrity.....	21
10.5	Media migration and format conversion during preservation period.....	21
10.5.1	Storage media migration	21
10.5.2	Format conversion	21
10.6	Deletion.....	22
11	Dissemination Information Package.....	22
12	Transfer process	23
12.1	General	23
12.2	Transfer Requirements	23
12.2.1	General	23
12.2.2	Identification of transfer Requirements	23
12.2.3	Design of the transfer Interface.....	23
12.2.4	Documentation of transfer process	24
12.3	Responsibilities.....	24
13	Traceability of operations	25
13.1	Traceability of operations	25
13.2	Criticality of events	25
13.3	Common features of critical and non critical events	25
13.3.1	Reliable time of events	25
13.3.2	Traceability of initiator	25
13.3.3	separation of traced events	25
13.4	Non-critical events	25
13.5	Critical events	26
13.6	Integrity protection of critical events and digital objects.....	27
13.6.1	General	27
13.6.2	Protection using digital signature techniques	27
13.6.3	Protection using integrity chains.....	28
14	Reporting.....	28
14.1	General	28
14.2	Format and content of reports.....	30
	Annex A (informative) Green sustainability	31
	Annex B (informative) Concepts	32
B.1	General concepts.....	32
B.2	Electronic archiving trust service concepts	32
B.3	Digital objects concepts.....	33
B.4	Electronic archiving concepts	33
	Bibliography	34

European foreword

This document (CEN/TS 18170:2025) has been prepared by Technical Committee CEN/TC 468 “Preservation of digital information”, the secretariat of which is held by AFNOR.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

CEN/TS 18170:2025 (E)**Introduction**

This document specifies provisions (requirements, recommendations, permissions, possibilities and capabilities) for an Electronic Archiving Trust Service (EATS).

The structure of this document follows “CEN-CENELEC Internal Regulations Part 3:2022 (E), Principles and rules for the structure and drafting of CEN and CENELEC documents”.

The Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 (eIDAS 2) amending Regulation (EU) No 910/2014 (eIDAS) as regards establishing the European Digital Identity Framework establishes a legal framework of requirements for electronic signatures and trust services. This regulation introduces the (qualified) electronic archiving service. It requires standards for services, processes, systems and products related to trust services as well as guidance for conformity assessment of such services, processes, systems and products.

The main objective of this document is to define requirements and recommendations for an electronic archiving trust service which may use procedures and technologies capable of ensuring the durability and legibility of electronic data and electronic documents beyond the technological validity period and at least throughout the legal or contractual preservation period, while maintaining their integrity and the accuracy of their origin.

It is assumed that the Electronic Archiving Trust Service Provider (EATSP) which provides electronic archiving trust services operates the trustworthy system in an environment with a security policy which incorporates general physical, procedural and documentation security requirements for TSP providing electronic archiving trust services.

As explained further, this document follows ETSI EN 319 401 for General Policy Requirements for Trust Service Providers to ensure that the general Trust Service Providers requirements above are met.

NOTE The European Directive (EU) 2022/2555 (NIS2) is also a reference text for technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant for trust service providers.

1 Scope

This document specifies requirements for implementing electronic archiving trust services with specific regard to:

- Functional requirements for electronic archiving to ensure the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period.
- Requirements for qualified electronic archiving trust services, aiming to fulfil the provisions outlined in Article 45j of the eIDAS Regulation
- Procedures and technologies capable of ensuring the durability and legibility of electronic data and electronic documents beyond the technological validity period and at least throughout the legal or contractual preservation period, while maintaining their integrity and the accuracy of their origin.
- Procedures and technologies to ensure that those electronic data and those electronic documents are preserved in such a way that they are safeguarded against loss and alteration, except for changes concerning their medium or electronic format.
- Procedures and technologies that allow authorized relying parties to receive a report in an automated manner that confirms that electronic data and electronic documents retrieved from a QEATS qualified electronic archive trust service enjoy the presumption of integrity of the data from the beginning of the preservation period to the moment of retrieval.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ETSI EN 319 401, *Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers*

ETSI EN 319-421, *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*

ETSI TS 119 312, *Electronic Signatures and Infrastructures (ESI); Cryptographic Suites*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN