ENTAKSI SOLUTIONS

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
QUALIFIED TRUST SERVICES
ETSI 319 401 | ETSI 319 411-1 and 2 | ETSI 319 421 | ETSI 119 511
ELECTRONIC SIGNATURES AND SEALS - TIME STAMPS
LONG-TERM PRESERVATION

Manual

MAN eIDAS 20210628 Signature Validation Policy EN

Entaksi Solutions SpA

Table of contents

Document information

Project	Integrated Management System
Type	Manual
Document ID	MAN eCON 20210628 Signature Validation Policy EN
Version	1.3.0
Creation Date	28/06/2021
Last Revision	02/12/2025
Author	Alessia Soccio
Status	Released
Classification	Public
Translation	This document is the original version. Italian translation: "MAN eCON 20210628 Signature Validation Policy".

💡 Paper reproductions of this document are to be considered working copies not registered by the SIG.

Revisions and releases

Date	Version	Name	Role	Action	Release
28/06/2021	0.0.1	Alessia Soccio	IMSM	Draft creation.	Internal
01/12/2021	1.0.0	Alessia Soccio	IMSM	Review and release.	Public
15/12/2023	1.1.0	Alessia Soccio	IMSM	Periodic update, issue of new signature validation policy, review of company presentation, formal review of definitions and regulatory references, minor corrections.	Public
18/06/2024	1.2.0	Alessia Soccio	IMSM	Specifies use of versioning on eIDAS document OIDs, specifies versions of reference standards for signature validation policies.	Public
02/12/2025	1.3.0	Alessia Soccio	IMSM	Update to EU Regulation No. 1183/2024 – eIDAS 2, conformity to ETSI TS 119 441, minor corrections.	Public

Document approval

Date	Employee	Role	Signature
02/12/2025	Alessandro Geri	Sole Manager	*Digitally signed*

1. Introduction

This document is the **Signature Validation Policies regarding the eCON Preservation Service provided by Entaksi Solutions SpA - Irish Branch** (hereinafter "Entaksi"), a branch of the Italian company with VAT-ID IT01621900479 Entaksi Solutions SpA, operating in Ireland with National Trade Register number 909882.

Entaksi is a **Trust Service Provider** for:

- **The issuance of qualified certificates for electronic signatures**.
- **The issuance of qualified certificates for electronic seals**.
- **The qualified preservation service for qualified electronic signatures**.
- **The qualified preservation service for qualified electronic seals**.
- **The creation of qualified electronic timestamps**.

Entaksi is registered as a Trust Service Provider by the competent national supervisory body in Ireland (currently the Department of the Environment, Climate and Communications – DECC) and is included in the national trusted list in accordance with the eIDAS Regulation.

The eCON Preservation Service is a trust service that ensures the long-term preservation of digital signatures and other data using digital-signature techniques. It complies with EU Regulation 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, as amended by EU Regulation No. 1183/2024 – eIDAS 2 (hereinafter “eIDAS”).

The provision of a signature-validation service exists solely to support the eCON Preservation Service, in accordance with ETSI TS 119 441, and does not constitute a service provided to external customers independently of the qualified service.

This Signature Validation Policy describes the rules, constraints and procedures applied by the eCON Signature Validation Service when validating electronic signatures and seals in the context of the qualified preservation service. Entaksi, in this context, acts as a Signature Validation Service Provider (SVSP) and is responsible for performing signature and seal validation in accordance with the applicable requirements defined in eIDAS, ETSI TS 119 441, and any other relevant standards or regulatory frameworks.

The SVSP ensures that all validations are carried out consistently, reliably, and with documented assurance levels, providing the necessary evidence to support the long-term preservation of electronic signatures and seals.

1.1. Document identification

This document is identified by the following OID:

Table 1. Document name and identification.

OID	Description	Permanent Link
`1.3.6.1.4.1.57823.1.4`	MAN eIDAS 20210628 Signature Validation Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.4

The OID is intended to identify the general content and scope of the document, and always refers to the latest available version.
Variations may occur between subsequent versions of the same document and each of them is recorded on the document itself as a new version. To identify a specific version of a document it is possible to point to the OID plus the version (e.g. `1.3.6.1.4.1.57823.1.4.1.0.0` will refer to version 1.0.0 of this document, 1.3.6.1.4.1.57823.1.4.1.1.0` to 1.1.0 and so on).

The OIDs identifying the specific signature validation policies are identified within the document.

1.2. Document maintenance

Entaksi has defined a review process for all the internal documents, including policies, statements and practices.

The documents are periodically reviewed under the responsibility of Entaksi management, in order to assess their compliance with national and international requirements, standards, mandatory legislation, regulations in force, particular needs imposed by the technical and technological evolution, evolution of the business context.

The review and any update take place at least once a year, or whenever one of the following circumstances occurs:

- internal organizational changes that impact on the system;
- major changes to the hardware or software architecture;
- regulatory updates;
- changes in procedures, methodologies or business context.

For this Signature Validation Policy, Entaksi additionally reviews the policy whenever:

- there are changes to standards and regulations that affect the validation process;
- the scope of the Signature Validation Service or its supported formats and algorithms changes.

1.3. Approval and publication

This document and all the internal policies and practices mentioned in it have been approved by Entaksi’s management, published and communicated to employees and, as regards those classified as "public", published on the company website at the following link: https://www.entaksi.eu/en/documentation.html.
The website is available on 24x7 basis.

Entaksi makes available to all customers of trust services and relying parties any update of this document and other relevant documentation as soon as the update is approved and revised on the basis of what is described in the revision procedure.

Entaksi, will communicate any change that might affect the acceptance of the service by the subject, subscriber or relying parties through the communication channel established in the terms and conditions of the service.

2. Definitions and abbreviations

2.1. Definitions

Certificate Status Authority

authority providing certificate status information.

Container

Data object, which contains a set of data objects and optional additional information, which describes the contained data objects and optionally its content and its interrelationships.

Data Object

Actual binary/octet data being operated on (e.g. transformed, digested, or signed) by an application and which may be associated with additional information like an identifier, the encoding, size or type.

EU qualified preservation service

Preservation service that meets the requirements for qualified preservation service for qualified electronic signatures and/or for qualified electronic seals as laid down in EU Regulation No. 910/2014 - eIDAS.

Evidence record

Unit of data, which can be used to prove the existence of an archived data object or an archived data object group at a certain time.

Expected Evidence Duration

For a preservation service with temporary storage or without storage, duration during which the preservation service expects that the preservation evidence can be used to achieve the preservation goal long-term: time period during which technological changes may be a concern.

Metadata

Data about other data.

Notification interface

Interface provided by the preservation client supporting the notification protocol.

Notification Protocol

Protocol used by a preservation service to notify the preservation client.

Preservation Client

Component or a piece of software which interacts with a preservation service via the preservation protocol.

Preservation Evidence

Evidence produced by the preservation service which can be used to demonstrate that one or more preservation goals are met for a given preservation object.

Preservation Evidence Policy

Set of rules that specify the requirements and the internal process to generate or how to validate a preservation evidence.

Preservation Evidence Retention Period

For a preservation service With Temporary Storage (WTS) the time period during which the evidences that are produced asynchronously can be retrieved from the preservation service.

Preservation Goal

One of the following objectives achieved during the preservation time frame: extending over long periods of time the validity status of digital signatures, providing proofs of existence of data over long periods of time, or augmentation of externally provided preservation evidences.

Preservation Interface

Component implementing the preservation protocol on the side of the preservation service preservation manifest: data object in a preservation object container referring to the preservation data objects or additional information and metadata in the preservation object container.

Preservation Mechanism

Mechanism used to preserve preservation objects and to maintain the validity of preservation evidences.

Preservation Object

Typed data object, which is submitted to, processed by or retrieved from a preservation service.

Preservation Object Container

Container which contains a set of data objects and optionally related metadata providing information about the data objects and optionally preservation manifest(s) specifying its content and relationships.

Preservation Object Identifier

Unique identifier of a (set of) preservation object(s) submitted to a preservation service.

Preservation Planning

Monitoring changes and risks e.g. concerning innovations in storage, access and preservation technologies, new design strategies, etc.

Preservation Period

For a preservation service with storage, duration during which the preservation service preserves the submitted preservation objects and the associated evidences.

Preservation Profile

Uniquely identified set of implementation details pertinent to a preservation storage model and one or more preservation goals which specifies how preservation evidences are generated and validated.

Preservation Protocol

Protocol to communicate between the preservation service and a preservation client.

Preservation Scheme

Generic set of procedures and rules pertinent to a preservation storage model and one or more preservation goals which outlines how preservation evidences are created and validated.

Preservation Service

Service capable of extending the validity status of a digital signature over long periods of time and/or of providing proofs of existence of data over long periods of time.

Preservation Storage Model

One of the following ways of implementing a preservation service: with storage, with temporary storage, without storage.

Preservation Submitter

Legal or natural person using the preservation client to submit the submission data object.

Preservation Subscriber

Legal or natural person bound by agreement with a preservation trust service provider to any subscriber obligations.

Proof of Existence

Evidence that proves that an object existed at a specific date/time.

Proof of Integrity

Evidence that data has not been altered since it was protected.

Signer

Entity being the creator of a digital signature.

Submission Data Object

Original data object provided by the client.

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.

Time Stamping Service

Trust service for issuing time stamps.

Time Stamping Unit

Set of hardware and software which is managed as a unit and has a single time stamp signing key active at a time.

Trusted List

List that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation.

Validation Data

Data that is used to validate a digital signature.

2.2. Abbreviations

AUG

Augmentation Goal.

PDS

Preservation of Digital Signatures.

PGD

Preservation of General Data.

PO

Preservation Object.

POC

Preservation Object Container.

PRP

Preservation Service Protocol.

PSP

Preservation Service Provider.

SigS

Digital Signature creation Service.

SubDO

Submission Data Object.

ValS

Validation Service.

WOS

Without Storage.

WST

With Storage.

WTS

With Temporary Storage.

3. References

In order to ensure the compliance of the eCON Preservation Service to rules and regulation, Entaksi defines the criteria and the processes of the Service according to the relevant Italian and European legislation, and, as well, implements international standards that define the theoretical, operational and functional management of the system. Below are enlisted the normative and informative references the company is subject to.

This policy complies with the normative references enlisted below, as required by eIDAS and the Italian digital preservation regulation.

3.1. Normative references

3.1.1. eIDAS Regulation

Entaksi's Integrated Management System, which also oversees the processes described within this document, is certified against the following international standards:

- **ISO 9001:2015**: Quality management systems - Requirements.
- **ISO/IEC 20000-1:2018**: Information technology - Service management - Part 1: Service management system requirements.
- **ISO/IEC 27001:2022**: Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
- **ISO/IEC 27017:2015**: Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- **ISO/IEC 27018:2019**: Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
- **ISO/IEC 27035:2016**: Information technology — Security techniques — Information security incident management.
- **ISO/IEC 22301:2019**: Security and resilience — Business continuity management systems — Requirements.
- **UNI ISO 37001:2016**: Anti-bribery management systems - Requirements with guidance for use.
- **eIDAS Regulation for Qualified Trust Service Providers**:
  - **ETSI EN 319 401 V3.1.1 (2024-06)**: Electronic Signatures and Infrastructures (ESI) - General Policy Requirements for Trust Service Providers.
  - **ETSI EN 319 411-1 V1.5.1 (2025-04)**: Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 1: General requirements.
  - **ETSI EN 319 411-2 V2.6.1 (2025-06)**: Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 2: Requirements for trust service providers issuing EU qualified certificates.
  - **ETSI EN 319 412-1 V1.6.1 (2025-06)**: Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 1: Overview and common data structures.
  - **ETSI EN 319 412-2 V2.4.1 (2025-06)**: Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 2: Certificate profile for certificates issued to natural persons.
  - **ETSI EN 319 412-3 V1.3.1 (2023-09)**: Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 3: Certificate profile for certificates issued to legal persons.
  - **ETSI EN 319 412-5 V2.5.1 (2025-06)**: Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 5: QCStatements.
  - **ETSI EN 319 421 V1.3.1 (2025-07)**: Electronic Signatures and Infrastructures (ESI) - Policy and Security Requirements for Trust Service Providers issuing Time-stamps.
  - **ETSI EN 319 422 V1.1.1 (2016-03)**: Electronic Signatures and Infrastructures (ESI) - Time-stamping protocol and time-stamp token profiles.
  - **ETSI TS 119 511 V1.2.1 (2025-10)**: 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.
- **CSA STAR**: Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) Level 2.

All the certifications are publicly available at the following link: https://www.entaksi.eu/en/certifications.html.

The Trust Services Management System, a subcomponent of Entaksi's Integrated Management System, complies with the relevant requirements laid down in eIDAS 2 and meets the additional conformity requirements of the following standards:

- ETSI Standards:
  - **ETSI EN 319 102-1 V1.3.1 (2021-11)**: Electronic Signatures and Infrastructures (ESI) - Procedures for Creation and Validation of AdES Digital Signatures - Part 1: Creation and Validation;
  - **ETSI TS 119 102-2 V1.4.1 (2023-06)**: Electronic Signatures and Infrastructures (ESI) - Procedures for Creation and Validation of AdES Digital Signatures - Part 2: Signature Validation Report;
  - **ETSI TS 119 172-4 V1.1.1 (2021-05)**: Electronic Signatures and Infrastructures (ESI) Signature Policies - Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists;
  - **ETSI TS 119 431-1 V1.3.1 (2024-12)**: Electronic Signatures and Trust Infrastructures (ESI) - Policy and security requirements for trust service providers - Part 1: TSP services operating a remote QSCD / SCDev;
  - **ETSI TS 119 441 V1.3.1 (2025-10)**: Electronic Signatures and Trust Infrastructures (ESI) - Policy requirements for TSP providing signature validation services;
  - **ETSI TS 119 442 V1.1.1 (2019-02)**: Electronic Signatures and Infrastructures (ESI) - Protocol profiles for trust service providers providing AdES digital signature validation services;
  - **ETSI TS 119 461 V2.1.1 (2025-02)**: Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service components providing identity proofing of trust service subjects;
  - **ETSI TS 119 495 V1.7.1 (2024-07)**: Electronic Signatures and Trust Infrastructures (ESI) - Sector Specific Requirements - Certificate Profiles and TSP Policy Requirements for Open Banking;
  - **ETSI TS 119 512 V1.2.1 (2023-05)**: Electronic Signatures and Infrastructures (ESI) - Protocols for trust service providers providing long-term data preservation services;
  - **ETSI EN 301 549 V2.1.2 (2018-08)**: Accessibility requirements for ICT products and services;
- ISO Standards:
  - **ISO 14641:2018**: Electronic document management - Design and operation of an information system for the preservation of electronic documents - Specifications;
  - **ISO/IEC 14721:2025**: Space data and information transfer systems - Open archival information system (OAIS) - Reference model;
  - **CEN/TS 18170:2025**: Functional requirements for the electronic archiving services.

3.1.2. Long-Term Preservation

The applicable standards for the qualified preservation service for qualified electronic signatures and the qualified preservation service for qualified electronic seals, pursuant to the "Commission Implementing Regulation (EU) n° 2025/2162 of 27 October 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the accreditation of conformity assessment bodies performing the assessment of qualified trust service providers and the qualified trust services they provide, the conformity assessment report and the conformity assessment scheme", are:

- ETSI EN 319 401 V3.1.1 (2024-06).
- ETSI TS 119 172-4 V1.1.1 (2021-05).
- ETSI TS 119 511 V1.2.1 (2025-10).
- ETSI TS 119 512 V1.2.1 (2023-05).
- ETSI EN 301 549 V2.1.2 (2018-08).

3.1.3. Italian Digital Preservation Regulation

Codice dell'Amministrazione Digitale (CAD)

Codice dell'Amministrazione Digitale (Decreto Legislativo del 7 marzo 2005, n. 82, e successive modifiche).

"Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"

"Guidelines on the creation, management and preservation of IT documents", issued on 09 September 2020 by the Agenzia dell'Italia Digitale (AgID).

AgID Preservation Service Providers Regulation

"Determinazione" No 455/2021 of the Agenzia dell'Italia Digitale (AgID) of 25 June 2021 on the adoption of ""Regulation on the criteria for the provision of IT document preservation services"".

3.1.4. Data Protection

General Data Protection Regulation (EU) 2016/679

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Decreto Legislativo 10 agosto 2018, n. 101

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

3.1.5. Other provisions

The eCON digital preservation system also conforms to the following standards:

UNI 11386:2020

Supporting interoperability in preservation and retrieval of digital objects.

ISO 15489-1:2016

Information and documentation - Records management - Part 1: Concepts and principles.

ISO 15836-1:2017

Information and documentation - The Dublin Core metadata element set - Part 1: Core elements.

ISO 16363:2025

Space data and information transfer systems - Audit and certification of trustworthy digital repositories.

ISAD(G)

General International Standard Archival Description, description standard for archives intended for the registration of documents produced by organizations, individuals and families.

3.2. Informative references

Entaksi's Qualified Long-Term Preservation Service is supported by the following policies, practice statements and manuals:

Table 2. LTP documents name and identification.

OID	Description	Permanent Link
`1.3.6.1.4.1.57823.1.1`	MAN eIDAS 20210628 Preservation Service Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.1
`1.3.6.1.4.1.57823.1.4`	MAN eIDAS 20210628 Signature Validation Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.4
`1.3.6.1.4.1.57823.1.3`	MAN eIDAS 20210628 Preservation Evidence Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.3
`1.3.6.1.4.1.57823.1.2`	MAN eIDAS 20210628 Preservation Service Practice Statement EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.2

The italian conformity document is "MAN eCON 20151222 Digital Preservation Manual".

All the previous enlisted documents are classified as "public" and disclosed to the relying parties on the company website: https://www.entaksi.eu/en/

Furthermore, the subsequent documents illustrate some confidential topics about the eCON Preservation Service, mostly related to system security procedures and technical questions.

Table 3. eCON Preservation Service Confidential Documents

Document name	Document version	Valid from
MAN eCON 20190918 Termination Plan	1.4.0	01/12/2021
MAN eCON 20151222 Security Plan	1.5.0	01/12/2021

Entaksi, due to their confidential content, doesn't disclose these documents and any of its other internal manuals, procedures and security documents. However, according to the company's availability and commitment, it is available to undergo audits by its subscribers or other interested parties, upon signing an un-disclosure agreement.

4. Roles and responsibilities

The **designated community of eCON Digital Preservation Service**, as required by the Open Archival Information System (OAIS) Standard ISO/IEC 14721:2025, is described in the eCON User Manuals, and also are enlisted the roles and activities for each Entaksi's staff member.

Entaksi is appointed as Trust Service Provider for the eCON Long-Term Preservation Service.

The eCON Preservation Service is administrated by various "**Managers**", each of whom covers a very specific role in the company and in the service in particular, in order to better ensure the reliability of the system without overlapping activities and with compartmentalization of roles:

- **Preservation Service Manager (PSM)**.
- **Deputy Preservation Service Manager (DPSM)**.
- **Archival Function Manager (AFM)**.
- **Data Protection Manager (DPM)**.
- **Preservation System Security Manager (PSSM)**.
- **Preservation Information System Manager (PISM)**.
- **Preservation System Development and Maintenance Manager (PSDMM)**.

All the data relating to the persons and specific roles covered by the various managers of the Preservation Service eCON are available in the eCON preservation manual, published both on the Agenzia per l'Italia Digitale website and on the Entaksi Website: https://www.entaksi.eu/en/

Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification, or misuse of the Entaksi's assets.

Entaksi Solutions SpA is responsible for the provision of the service, and the Preservation Service Manager (PSM) is the role appointed for service delivery tasks.

In accordance with art. 38 of the "Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013" (Prime Minister's Decree), the following individuals are appointed in addition to those listed above:

- Security Manager.
- Qualified Service Manager;
- Responsible for the technical management of the systems.
- Responsible for technical and logistical services.
- Responsible for audits and inspections (auditing).

In this context the Preservation Service Manager is also responsible for the design, maintenance and monitoring of the Signature Validation Policies, the correct operation of the Signature Validation Service, and the conformity of the SVS with applicable standards and regulations.

Supported by the Preservation System Security Manager (PSSM) and the Preservation Information System Manager (PISM), is responsible for:

- ensuring that the signature validation policies and the corresponding XML policy files are implemented and deployed correctly;
- ensuring that validation results are produced only under identified and approved policies;
- ensuring that logs of validation operations are generated, protected and retained for at least the period required by applicable legislation;
- coordinating incident handling related to signature validation processes.

Other roles are defined in "MAN eIDAS 20210628 Preservation Service Policy EN" and "MAN eIDAS 20210628 Preservation Service Practice Statement EN".

5. eCON Preservation Service Signature Validation Policies

The signature validation policies used in the eCON Preservation Service are provided in a machine-readable format.

eCON Preservation Service supports the automatic interpretation of a machine-readable signature validation policy description language according to technical specifications described in ETSI EN 319 102-1.

Signature validation policies are described by an XML file that states rules and policies applied during the validation process.

The Signature Validation Service is operated under Entaksi’s control. It is only used internally by the eCON Preservation Service and is not exposed as a stand-alone public validation web service. Relying Parties obtain the validation result indirectly through the preservation evidence and associated validation report.

5.1. Validation strategy

Signature validation operates according to ETSI EN 319 102-1 chapter "5.6 Validation process for Signatures providing Long-Term Availability and Integrity of Validation Material".

During the validation procedure all materials needed for long-term validation of the signature are collected resulting in a signature validation report that contains all collected materials and a set of proof of existence of the signature at the time of validation.

The Signature Validation Service applies the following general strategy:

- Validation is always performed under a clearly identified Signature Validation Policy.
- The Signature Validation Service supports AdES, AdES/QC and QES signatures and seals in the formats XAdES, CAdES, PAdES and ASiC containers, as described in the applicable XML policy.
- Validation uses evidence from certificates, CRLs, OCSP responses, time-stamps, and, where applicable, prior preservation evidences, in accordance with ETSI EN 319 102-1.
- The validation process determines the status of the signature at an appropriate control time (best-signature-time or validation time) and records this in the validation report, which is subsequently embedded or linked in the preservation evidence created.

5.2. Validation policies

The Entaksi Signature Validation Policies are identified by the following OIDs:

Table 4. Signature Validation Policies' OIDs.

OID	Description
`1.3.6.1.4.1.57823.2.3.1`	eCON Signature Validation Policy 2022-01
`1.3.6.1.4.1.57823.2.3.2`	eCON Signature Validation Policy 2024-01

Each validation policy:

- is specified by a machine-readable XML file compliant with ETSI EN 319 102-1 and ETSI TS 119 172-4;
- defines one or more validation constraint sets (e.g. for QES, AdES/QC) covering algorithm constraints, certificate and revocation status handling, and trust anchor configurations in accordance with ETSI TS 119 312;
- refers explicitly to the use of EU Member States’ Trusted Lists;
- is versioned and controlled under Entaksi’s configuration management system;
- is uniquely referenced in validation reports and in preservation evidences using an OID, so that the relying party can identify the policy used.

5.3. Policies description

The policies describe a process that validates electronic signatures and indicates whether they are Advanced electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a Qualified electronic Signature (QES). All certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes signer’s certificate and certificates used to validate certificate validity status services, CRLs, OCSP, and time-stamps).

The policies contain rules and validation parameters that might change over time following the recommendations in updated versions of ETSI TS 119 312.

5.3.1. Signature Validation Policy 2022-01

The "Signature Validation Policy 2022-01" identified by OID `1.3.6.1.4.1.57823.2.3.1` contains rules and validation parameters as of January 2022.

The XML file describing the signature validation policy is available at the following address: https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.2.3.1.

The policy implements the controls defined in the ETSI TS 119 312 V1.4.1 (2021-08) standard.

This Signature Validation Policy XML file follows ETSI EN 319 102-1 V1.2.1 (2018-08) requirements. The validation procedure takes this file as input for applying defined rules and validation parameters from this file, and it produces a validation report according to the format defined in ETSI TS 119 102-2.

This Signature Validation Policy uses the shell validation model in that all certificates must be valid at validation time.

5.3.2. Signature Validation Policy 2024-01

The "Signature Validation Policy 2022-01" identified by OID `1.3.6.1.4.1.57823.2.3.2` contains rules and validation parameters as of January 2024.

The XML file describing the signature validation policy is available at the following address: https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.2.3.2.

The policy implements the controls defined in the ETSI TS 119 312 V1.4.3 (2023-08) standard.

This Signature Validation Policy XML file follows ETSI EN 319 102-1 V1.3.1 (2021-11) requirements. The validation procedure takes this file as input for applying defined rules and validation parameters from this file, and it produces a validation report according to the format defined in ETSI TS 119 102-2.

This Signature Validation Policy uses the shell validation model in that all certificates must be valid at validation time.

5.4. Signature Validation Service

The Signature Validation Service is operated by Entaksi as an internal component supporting the eCON qualified preservation services for electronic signatures, electronic seals and general data. The service validates signatures and seals created in accordance with ETSI EN 319 102-1 and ETSI TS 119 312, using the XML validation policies referenced in Policies description and produces validation reports compliant with ETSI TS 119 102-2.
These reports are stored or referenced within the preservation evidence generated under ETSI TS 119 511.

5.4.1. Inputs

To perform validation, the Signature Validation Service requires the signed data object or container together with its associated electronic signature(s) or seal(s), including any embedded time-stamps or validation material.

The Signature Validation Policy to be applied is identified by its OID.
Additional validation material not embedded in the signature — such as external CRLs, OCSP responses, certificates or time-stamps — is supplied as described in the eCON Preservation Service Practice Statement ("MAN eIDAS 20210628 Preservation Service Practice Statement EN").

5.4.2. Validation process

For a comprehensive description of the validation workflow, reference should be made to "MAN eIDAS 20210628 Preservation Service Policy EN", "MAN eIDAS 20210628 Preservation Service Practice Statement EN" and "MAN eIDAS 20210628 Preservation Evidence Policy EN". These documents describe in detail the validation architecture, the applicable Signature Validation Policies, the associated processing rules, and the integration of validation results into the preservation evidence produced by the service.

5.4.3. Outputs

The primary output of the validation process is a validation report compliant with the requirements of ETSI TS 119 102-2. The structure, mandatory fields and encoding of this report are fully described in "MAN eIDAS 20210628 Preservation Evidence Policy EN".

The report includes:

- validation status;
- diagnostic data;
- details of the validation policy applied;
- time indications;
- trust paths and revocation data used.

Once generated, the validation report is stored within the preservation system itself, either embedded in or referenced by the preservation evidence. This ensures long-term verifiability, traceability and reproducibility of the validation process.

6. Other provisions

6.1. Compliance and Audit

The applicable legal system is declared in References.

The configuration of the eCON Preservation Service is regularly checked by the management to avoid any change which violate Entaksi's security policies.

Entaksi's eCON Preservation Service is supervised by the Agenzia dell'Italia Digitale (AgID), which has the responsibility of regularly checking and revising the compliance of the system at the requirements defined in accordance with the Italian regulations on digital preservation.

Moreover, the system is checked at least yearly by an accredited certification body, recognized by Accredia, the Italian Accreditation Body.

Audit working papers and inspection documents are classified as confidentials.
The conformity certificates and their updates are published on the Entaksi website] in accordance with the assessment results: https://www.entaksi.eu/en/certifications.html

Entaksi's qualified service for the long-term preservation of signatures, seals and general data is outlined by the following documents:

Table 5. LTP documents name and identification.

OID	Description	Permanent Link
`1.3.6.1.4.1.57823.1.1`	MAN eIDAS 20210628 Preservation Service Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.1
`1.3.6.1.4.1.57823.1.2`	MAN eIDAS 20210628 Preservation Service Practice Statement EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.2
`1.3.6.1.4.1.57823.1.3`	MAN eIDAS 20210628 Preservation Evidence Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.3
`1.3.6.1.4.1.57823.1.4`	MAN eIDAS 20210628 Signature Validation Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.4

All Entaksi's qualified trust services documents are available at the following link:
https://www.entaksi.eu/en/documentation.html.

6.2. Accessibility

Entaksi provides its documentation, contract forms, and web-based interfaces for Trust Services management through channels designed to be accessible to persons with disabilities and users with accessibility needs, in accordance with the requirements of ETSI EN 301 549 and applicable national legislation.

Where a subscriber or relying party cannot reasonably use the standard online channels due to an accessibility need or disability, Entaksi will provide alternative accessible means (like assisted support via email or telephone) to guarantee access to identical information and services without discrimination.

Entaksi takes into account feedbacks that involve accessibility issues from users and is committed to continually improving the accessibility of its services.