



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 20230426 PKI Disclosure Statement EN

Entaksi Solutions SpA

Table of contents

Document information.	1
Revisions and releases.	1
Document approval.	1
1. Introduction.	3
1.1. Document maintenance.	3
1.2. Approval and publication.	3
1.3. References.	3
1.3.1. Normative references.	3
1.3.2. Informative references.	5
2. TSP contact info.	5
2.1. Revocation or suspension request.	6
3. Certificate types, validation procedures and usage.	6
4. Reliance limits.	6
5. Obligations of subscribers.	7
6. Certificate status checking obligations of relying parties.	7
7. Limited warranty and disclaimer/Limitation of liability.	7
8. Applicable agreements, CPS, CP.	7
9. Privacy policy.	8
10. Refund policy.	8
11. Applicable law, complaints and dispute resolution.	8
12. TSP and repository licenses, trust marks, and audit.	8
12.1. Accessibility.	8

Document information

Project	Integrated Management System
Type	Manual
Document ID	MAN eIDAS 20230426 PKI Disclosure Statement EN
Version	1.3.0
Creation Date	26/04/2023
Last Revision	02/12/2025
Author	Alessia Soccio
Status	Released
Classification	Public
Translation	This document is the original version. Italian translation: "MAN eIDAS 20230426 PKI Disclosure Statement".



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
26/04/2023	0.0.1	Alessia Soccio	IMSM	Draft creation.	Internal
10/05/2023	1.0.0	Alessia Soccio	IMSM	Review and release.	Public
15/12/2023	1.1.0	Alessia Soccio	IMSM	Usage extention to qualified certificates for electronic signatures and seals.	Public
05/12/2024	1.2.0	Alessia Soccio	IMSM	Periodic update, minor corrections.	Public
02/12/2025	1.3.0	Alessia Soccio	IMSM	Update to EU Regulation No. 1183/2024 – eIDAS 2, minor corrections.	Public

Document approval

Date	Employee	Role	Signature
02/12/2025	Alessandro Geri	Sole Manager	<i>Digitally signed</i>

© 2025 Entaksi Solutions SpA

The information contained in this document is the property of Entaksi Solutions SpA, it is confidential, private, and only for the information of the intended recipient(s), and it cannot be communicated to third parties, reproduced, published or redistributed without the prior written consent of Entaksi.

1. Introduction

This is the **PKI Disclosure Statement of the Trust Service Provider (TSP) 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.

This document complies with the requirements of the European standard ETSI EN 319 411-1, and in particular is drawn up following the structure defined in Annex A of the aforementioned standard.

The Certification Authority (CA) operated by Entaksi, as part of its trust services, 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")

This document does not substitute or replace the Terms and Conditions of the CA services, of which is an attachment, nor the Certificate Policy and Certification Practice Statement, which are published on Entaksi's website (see [Applicable agreements, CPS, CP](#)).

1.1. 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.

1.2. 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.

1.3. References

1.3.1. Normative references

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.

The applicable standards for the issuance of qualified certificates for electronic signatures and the issuance of qualified certificates for electronic seals, pursuant to the EU Regulation No. 910/2014 - eIDAS, as amended by EU Regulation No. 1183/2024 - eIDAS 2 and 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 EN 319 411-2 V2.6.1 (2025-06).
- ETSI EN 319 412-1 V1.6.1 (2025-06).
- ETSI EN 319 412-2 V2.4.1 (2025-06).
- ETSI EN 319 412-3 V1.3.1 (2023-09).
- ETSI EN 319 412-5 V2.5.1 (2025-06).
- ETSI TS 119 461 V2.1.1 (2025-02).
- ETSI TS 119 495 V1.7.1 (2024-07)
- ETSI EN 301 549 V2.1.2 (2018-08).

Entaksi does not issue qualified certificates for Payment Service Providers and does not operate a PSD2/Open Banking trust service. Therefore, ETSI TS 119 495 ("Electronic Signatures and Trust Infrastructures (ESI) - Sector Specific Requirements - Certificate Profiles and TSP Policy Requirements for Open Banking") is not applicable to the trust services provided by Entaksi.

1.3.2. Informative references

Entaksi's Certification Authority is supported by the following policies, practice statements and manuals:

Table 1. CA documents name and identification.

OID	Description	Permanent Link
1.3.6.1.4.1.57823.1.9	MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.9
1.3.6.1.4.1.57823.1.10	MAN eIDAS 20230426 PKI Disclosure Statement EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.10
1.3.6.1.4.1.57823.1.13	MAN eIDAS 20251125 Identity Proofing Service Policy and Practice Statement EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.13

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

2. TSP contact info

The Trust Service Provider can be contacted at the following addresses:

Entaksi Solutions SpA - Irish Branch

Suite 4.01 - Ormond Building 31 36 Ormond Quay Upper - D07F6DC Dublin 7 - Ireland

Entaksi Solutions SpA - Italian Head Office

via la Piana 76, fraz. Pontepetri, 51028 San Marcello Piteglio (PT), Italy

Entaksi Solutions SpA - Operational office

re.working, Viale della Costituzione - Centro Direzionale Isola E2 - 80143 Napoli, Italy

Info: info@entaksi.eu

Help Desk: helpdesk@entaksi.eu

Data Protection Info: privacy@entaksi.eu

Data Protection Officer: dpo@entaksi.eu

Anti-Bribery: antibribery@entaksi.eu

Certification Authority: ca@entaksi.eu

Phone: +39 0573 171 6484

Website: <https://www.entaksi.eu/en/>

2.1. Revocation or suspension request

The revocation or the suspension of a certificate can be requested by sending a specific form to ca@entaksi.eu.

The form is available on Entaksi's website at the following link: <https://www.entaksi.eu/en/documentation.html>.

3. Certificate types, validation procedures and usage

Entaksi issues qualified certificates for the following usages:

- Qualified certificates for electronic signatures;
- Qualified certificates for electronic seals;
- Qualified certificates for Time-stamping Units issuing qualified Time-stamps.

The applicability is described in [References](#).

The algorithm used for signing certificates can be one of the following:

- sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11);
- sha384WithRSAEncryption (OID 1.2.840.113549.1.1.12);
- sha512WithRSAEncryption (OID 1.2.840.113549.1.1.13);
- ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2);
- ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3);
- ecdsa-with-SHA512 (OID 1.2.840.10045.4.3.4);

Entaksi implements the following certificate policies.

Table 2. Certificate policies.

Policy	OID	Description
QCP-n-qscd	0.4.0.194112.1.2	Certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD.
QCP-l-qscd	0.4.0.194112.1.3	Certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD.

The Entaksi CA also issues certificates for the Entaksi TSA Time-stamping Unit (TSU). Certificate type issued by the CA for the TSU contains the QcStatements field (OID 1.3.6.1.5.5.7.1.3) specifying esi4-qtstStatement-1 as defined in clause 9.1 of ETSI EN 319 422.

4. Reliance limits

Entaksi does not set reliance limits for certificates issued by the Certification Authority, however reliance limits may be set by applicable laws in the EU country where the service is used or by customer agreement.

5. Obligations of subscribers

Key pairs shall be used in accordance with the limitation notified to the subscriber.

Unauthorized use of the private key is prohibited.

Use of the private key for cryptographic functions shall occur within the secure cryptographic device.

The subscriber is responsible for:

- providing the TSP accurate and complete information during the registration;
- using the key pair only in accordance with any limitations notified in the Certificate Policy and Certification Practice Statement;
- preventing any unauthorized use of the private key;
- maintaining the sole control of the private key;
- not attempting to use private key for cryptographic functions outside the secure cryptographic device;
- performing subject's keys generation within the secure cryptographic device in every procedure where the key generation is under control of the subscriber (for instance during certificate renewal);
- notifying Entaksi without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
 - private key has been lost, stolen, potentially compromised;
 - control over the private key has been lost due to compromise of activation data or other reasons;
 - inaccuracy or changes to the certificate content;
- immediately and permanently discontinuing the use of a compromised key, except for key decipherment;
- in the case of being informed that the certificate has been revoked by Entaksi, or that the issuing CA has been compromised, ensuring that the private key is no longer used.

6. Certificate status checking obligations of relying parties

Before placing any reliance on a digital signature that uses a certificate issued by the Certification Authority, including Time-stamps, relying parties must verify that the signature is correct and that the private key used to sign the document has not been revoked verifying the status of the public key certificate.

The relying party should take into account any limitation on usage indicated in the Certificate Practice Statement and any other reasonable precautions.

The public key certificate status can be verified using the Certificate Revocation List (CRL) reported in the TSU certificate CRLDistributionPoints extension (OID 2.5.29.31) or querying the Online Certificate Status Protocol responder reported in the AuthorityInformationAccess (OID 1.3.6.1.5.5.7.1.1) of the same certificate.

Revocation status of the certificate can be verified after the expiration of the certificate according to the QcRetentionPeriod statement (OID 0.4.0.1862.1.3) specified in the QcStatements field of the certificate (OID 1.3.6.1.5.5.7.1.3).

7. Limited warranty and disclaimer/Limitation of liability

Warranty and liability limitations are specified in the Terms and Conditions of the Qualified Certification Authority service.

The Certification Authority service Terms and Conditions are available in the Entaksi web site at the following link:

<https://www.entaksi.eu/en/documentation.html>.

8. Applicable agreements, CPS, CP

Applicable agreements are composed by the following documents:

- Service contract ("Condizioni generali del servizio" or "General Terms and Conditions").
- Personal data processing information.
- "MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement EN".
- "MAN eIDAS 20230426 PKI Disclosure Statement EN".
- "MAN eIDAS 20251125 Identity Proofing Service Policy and Practice Statement EN".

- Any additional document within the aforementioned.

All the TSP documents are available at the following link: <https://www.entaksi.eu/en/documentation.html>.

9. Privacy policy

Entaksi PKI complies with applicable regulation and legal requirements (including GDPR and eIDAS Regulation) as well as the requirements of the Entaksi Privacy Policy (see <https://www.entaksi.eu/en/privacy.html>).

The complete set of provisions relating to the processing of personal data and information security is reported on the Entaksi website (see <https://www.entaksi.eu/en/ispd.html>).

Entaksi Management operates to guarantee that appropriate technical and organizational measures will be constantly taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

10. Refund policy

The primary reference for Entaksi refund policy is the general Terms and Condition of the Qualified CA service. This document form is publicly available on Entaksi's website at the following link: <https://www.entaksi.eu/en/documentation.html>.

Entaksi does not refund fees for Certification Authority services that have already been paid.

11. Applicable law, complaints and dispute resolution

Certificates issued to clients located in Ireland are provided in accordance with Irish laws. Certificate issued outside Ireland are provided in accordance with Italian laws.

Entaksi looks for a peaceful and negotiated settlement of any disputes that may arise from its operation of the Certification Authority.

For any controversy the exclusive competent court will be Pistoia (Italy), except for subscribers located in Ireland that can submit the controversy to the competent court of Ireland.

12. TSP and repository licenses, trust marks, and audit

Entaksi has several certifications, whose full and updated list of is available at <https://www.entaksi.eu/en/certifications.html>.

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.

Entaksi TSP services are subject to conformity assessment every year by an accredited certification body, according to ETSI Standards as required by the eIDAS Regulation.

Audit working papers and inspection documents are classified as confidential, but the conformity certificates and their updates are published on the previously mentioned website page.

The trusted list of TSP can be checked at the following link: <https://eidas.ec.europa.eu/efda/tl-browser/>.

12.1. 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.