ENTAKSISOLUTIONS

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 Certificate Policy and Certification Practice Statement EN

Entaksi Solutions SpA

Table of contents

Document information

Project	Integrated Management System
Type	Manual
Document ID	MAN eIDAS 20230426 Certificate Policy and Certification Practice 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 Certificate Policy and Certification Practice 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, fix the certificate attributes list, minor corrections.	Public
02/12/2025	1.3.0	Alessia Soccio	IMSM	Update to EU Regulation No. 1183/2024 – eIDAS 2, review certificate status services, key ceremony, risk analysis, idenfication procedure, minor corrections.	Public

Document approval

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

1. Introduction

This document is the **Certificate Policy (CP) and Certification Practice Statement (CPS) of qualified Certification Authority operated 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 and VAT-ID IE4101785QH.

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 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")

1.1. Purpose and scope of the document

This document specifies the practice regarding the use of CA keys for signing certificates, Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP).
It also sets out the policies, processes and procedures followed in the generation, issue, use and management of Key Pairs and Digital Certificates for the Entaksi Certification Authority Public Key Infrastructure.
Moreover, it describes the roles, responsibilities and relationships of Participants within the Entaksi's PKI, and the requirements for the use of certificate profiles.

The structure of this document is based on the IETF RFC 3647, "Certificate Policy and Certification Practices Framework".

Subject naming attributes defined in this certificate policy follow the convention defined in IETF RFC 5280, in not otherwise specified.

1.2. Document name and identification

This document is identified by the following OID:

Table 1. Document name and identification.

OID	Description	Permanent Link
`1.3.6.1.4.1.57823.1.9`	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. PKI participants

The Public Key Infrastructure participants within the framework of this policy and practice statement, as defined in the document "MAN eIDAS 20230426 PKI Disclosure Statement EN" to which this document refers, are:

- Entaksi's Public Key Infrastructure (PKI), Certification Authority and Registration Authority.
- The Local Registration Authorities in a contractual relationship with Entaksi Certification Authority.
- Subscribers to Entaksi's Trust Services.
- Relying parties.
- Other participants.

The roles and participants specifically involved in the Identity Proofing Service (IPSP), such as applicants, registration officers and subcontracted identity proofing service providers, are defined in the document "MAN eIDAS 20251125 Identity Proofing Service Policy and Practice Statement EN". These roles operate before the PKI enrollment phase and are therefore distinct from the PKI participants listed above.

Entaksi digital certificates comply with Internet standards X509v3 as set out in IETF RFC 5280.

1.3.1. Certification authorities

This policy applies to the following Certification Authorities managed by Entaksi:

- **Entaksi QTSP Root CA G1**.
- **Entaksi Qualified Time-stamps CA G1**.
- **Entaksi Qualified Electronic Signatures CA G1**.
- **Entaksi Qualified Electronic Seals CA G1**.

The "Entaksi QTSP Root CA G1", that is an internal root certification authority that act as signer of other sub CAs, is identified by the following attributes:

- CN=Entaksi QTSP Root CA G1
- C=IT
- O=Entaksi Solutions SpA
- organizationIdentifier: VATIT-01621900479
- certificatePolicies:
  - anyPolicy (OID 2.5.29.32.0)
- Fingerprints
  - SHA-256: 14 E6 BC 59 57 D8 D7 B5 D2 07 8F 36 34 52 DA 52 1E 7C 52 04 E9 5B B6 B2 5B CF 6A DE 31 B9 31 D0
  - SHA-1: 14 1D 91 D4 6A B3 28 D8 6C 31 09 EF 79 D1 10 6B 8F BF 97 0C

The "Entaksi Qualified Time-stamps CA G1", that is the certification authority that issues certificates for the Time Stamp Unit (TSU) used by the Qualified Time Stamp Service, is identified by the following attributes:

- CN=Entaksi Qualified Time-stamps CA G1
- C=IE
- O=Entaksi Solutions SpA Irish Branch
- OU=Entaksi QTSP
- organizationIdentifier: NTRIE-909882
- certificatePolicies:
  - ETSI EN 319 411-1 Enhanced Normalized Certificate Policy NCP+ (OID 0.4.0.2042.1.2)
  - Entaksi Certificate Policy and Certification Practice Statement (OID 1.3.6.1.4.1.57823.1.9)
- Fingerprints
  - SHA-256: 6B F3 0A 94 DF 57 C6 65 D2 91 AD 7E 3C 09 30 0D 06 C7 C7 CB 97 27 58 B1 85 58 CC D4 5B 27 67 B7
  - SHA-1: CD 7B FF 32 DC 13 48 DF 36 B2 7F 05 03 D2 A2 69 32 D8 23 FC

The "Entaksi Qualified Electronic Signatures CA G1", that is the certification authority used for issuing qualified certificates for electronic signature of the Entaksi's service, is identified by the following attributes:

- CN=Entaksi Qualified Electronic Signatures CA G1
- C=IE`
- O=Entaksi Solutions SpA Irish Branch
- OU=Entaksi QTSP
- organizationIdentifier: NTRIE-909882
- certificatePolicies:
  - ETSI EN 319 411-1 Enhanced Normalized Certificate Policy NCP+ (OID 0.4.0.2042.1.2)
  - Entaksi Certificate Policy and Certification Practice Statement (OID 1.3.6.1.4.1.57823.1.9)
- Fingerprints
  - SHA-256: 2D 27 0F E8 3A 08 E2 6A C3 21 05 23 1A 0E CA E2 B5 5C EB 6E CD 77 E8 80 B4 98 39 3C 6D B3 85 17
  - SHA-1: 80 53 D6 9E 0B B7 44 69 B5 F4 93 1E 8F CA FB B3 49 A7 20 23

The "Entaksi Qualified Electronic Seals CA G1", that is the certification authority used for issuing qualified certificates for electronic seal of the Entaksi's service, is identified by the following attributes:

- CN=Entaksi Qualified Electronic Seals CA G1
- C=IE
- O=Entaksi Solutions SpA Irish Branch
- OU=Entaksi QTSP
- organizationIdentifier: NTRIE-909882
- certificatePolicies:
  - ETSI EN 319 411-1 Enhanced Normalized Certificate Policy NCP+ (OID 0.4.0.2042.1.2)
  - Entaksi Certificate Policy and Certification Practice Statement (OID 1.3.6.1.4.1.57823.1.9)
- Fingerprints
  - SHA-256: 35 BA 26 14 73 05 B6 A1 4B D7 EB 67 82 C4 28 CB 0C 08 57 96 F7 E7 85 F2 82 F8 CF FC DD D2 C5 3F
  - SHA-1: 13 75 61 4F 0C 68 F7 E3 BB 47 C4 B6 B2 AD 60 4E 5A 3A F5 89

1.3.2. Registration authorities

The subscribers seeking certificates undergo a process of identification and authentication, that can be carried out directly by Entaksi CA staff, or it can be delegated to third parties, known as "Registration Authorities" (RAs) or Local Registration Authority (LRA). This delegation is sanctioned by specific agreements between Entaksi CA and the RAs.

Subscribers seeking certificates undergo an identification and authentication process that may be carried out directly by Entaksi CA personnel or delegated to third parties acting as Registration Authorities (RAs) or Local Registration Authorities (LRAs).
Such delegation is formalized through specific agreements between Entaksi and each RA, and is executed in accordance with the Identity Proofing Service Policy and Practice Statement (IPSPPS) of Entaksi, named "MAN eIDAS 20251125 Identity Proofing Service Policy and Practice Statement EN".

Entaksi's RAs are responsible for the following functions:

- identifying and authenticating certificate applicants in accordance with the IPSPPS and the applicable identity proofing use cases;
- approving or rejecting certification requests;
- processing subscriber requests to revoke, suspend, reactivate or renew certificates;
- transmitting documentation, communications and requests to the CA.

RAs, on the other hand, are not responsible for signing or issuing certificates; instead, they are delegated specific tasks on behalf of Entaksi's CA.

The individuals involved in the functions listed above are called "Registration Authority Officer (RAO)", and can perform these tasks only after having received adequate training from Entaksi.
RAOs operate via email or SaaS web services made available by Entaksi to communicate certificates data. These services are subject to the exclusive control of Entaksi.

RAOs that verify the identity shall not be the natural person to whom the certificate is issued to (as a subject).

Entaksi provides all RAOs with dedicated training and guidance for the correct execution of registration activities and has established internal documentation and operational procedures specifically designed to support them in these tasks.

1.3.3. Subscribers and subjects

A subject is the entity identified in a certificate as the holder of the private key associated with the public key contained in the certificate, in accordance with ETSI EN 319 411-1.

Within the framework of this document, the subscriber (also referred to as the "applicant") is the entity requesting the issuance of a certificate and entering into a contractual relationship with Entaksi. Depending on the type of certificate and the associated identity proofing process, the subscriber may be:

- a natural person requesting a certificate for themselves;
- a natural person identified in association with a legal person, acting within a defined organizational role;
- a legal person requesting a certificate issued to the organization.

The subscriber and the subject may coincide (e.g., a natural person applying for their own qualified signature certificate) or may be distinct entities (e.g., a legal person acting as subscriber for a qualified electronic seal certificate).

1.3.4. Relying parties

All parties relying on the information within this document or certificates issued by Entaksi CAs are referred as "relying parties". These parties may or may not be a subscriber, but can be individuals and organizations doing business with subscribers in need to verify the certificates issued by Entaksi.

The communication channels between Entaksi and the relying parties are state in the chapter Contact person.

1.3.5. Other participants

In addition to the PKI participants explicitly identified in this document, no other parties are involved in the provision or operation of Entaksi's trust services.
National supervisory bodies may interact with the PKI exclusively in their regulatory and oversight capacity, and are not considered PKI participants.

1.4. Certificate 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 OIDs (Object Identifiers) of the policies supported by this CPS, along with the corresponding reference policy specified in the ETSI EN 319 411-2 standard, are listed below.

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.

1.4.1. Appropriate certificate uses

The end-user's private keys, tied to certificates issued by Entaksi in alignment with the current Certificate Policy and Certification Practice Statement, are exclusively for creating electronic signatures, electronic seals and Time-stamps as specified in the Certificate Policy. The certificate ensures the verification of documents being signed or sealed.

Certificates issued by Entaksi Qualified Electronic Signatures CA G1 certificate authority are appropriate for generating Qualified Electronic Signatures.

Certificates issued by Entaksi Qualified Electronic Seals CA G1 certificate authority are appropriate for generating Qualified Electronic Seals.

Certificates issued by Entaksi Qualified Time-stamps CA G1 certificate authority are appropriate for generating Qualified Time-stamps.

Certificates issued shall be used only using the corresponding private key.

Certificates and private keys usage shall respect the key usage extensions as prescribed in Key usage purposes (as per X.509 v3 key usage field)

1.4.2. Prohibited certificate uses

Certificate uses other than those described in the previous paragraph are prohibited.

1.5. Policy administration

1.5.1. Organization administering the document

This Certificate Policy and Certification Practice Statement is issued under the responsibility of Entaksi's management, which ensures its adequacy, correctness, and continuous alignment with applicable legislation, standards, and operational practices.

1.5.2. Contact person

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

Entaksi Solutions SpA - Irish Branch
Suite 4.01 - Ormond Building 31 36 Ormond Quai 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/

1.5.3. Person determining CPS suitability for the policy

The suitability of this Certificate Policy and Certification Practice Statement is determined by Entaksi's management, following an internal review and an assessment performed by qualified internal and external auditors. The management ensures that the CPS remains consistent with Entaksi's governance framework, the applicable ETSI standards, and the requirements of the eIDAS Regulation.

1.5.4. CPS approval procedures

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.

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.

1.6. Definitions and acronyms

1.6.1. Definitions

Certificate

Public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it.

Certificate chain

A chain of digital certificates required to validate a holder's digital certificate back through its respective issuing certification authority to the root certification authority.

Certificate renewal

The process of issuing a new certificate duplicating all the identifying information from an old certificate, but with a different validity period.

Certificate Re-key

The process of issuing a new certificate duplication all the identifying information from an old certificate, but with a new public key and a possibly different validity period.

Certificate Revocation List (CRL)

Signed list indicating a set of certificates that have been revoked by the certificate issuer.

Certification

The process of creating a digital certificate for an entity and binding that entity's identity to the digital certificate.

Certification Authority (CA)

Authority responsible for issuing and assigning certificates to one or more users.

Certification Authority Revocation List (CARL)

A Revocation list containing a list of CA-certificates issued to certification authorities that have been revoked by the certificate issuer.

Digital Signature

Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

Digital transmission

The transmission of information in an electronic format.

Identification

The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization.

Issuing certification authority (issuing CA)

In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Participant

An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.

Registration Authority (RA)

Entity that is responsible for identification and authentication of subjects of certificates.

Relying party

A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate.

Secure Cryptographic Device

A secure software, device or utility that generates key pairs, stores cryptographic information and performs cryptographic functions.

Subscriber

A subject of a certificate who is issued a certificate.

Validation

The process of identification of certificate applicants.

1.6.2. Acronyms

CA

Certification Authority.

CP

Certificate Policy.

CPS

Certification Practice Statement.

CRL

Certificate Revocation List.

CSA

Certificate Status Authority.

eIDAS

electronic Identification, Authentication and Signature.

ETSI

European Telecommunications Standards Institute.

HSM

Hardware Security Module.

IETF

Internet Engineering Task Force.

ITU

International Telecommunication Union.

ITU-T

ITU Telecommunication Standardization Sector.

LDAP

Lightweight Directory Access Protocol.

OCSP

Online Certificate Status Protocol.

OID

Object Identifier.

PKI

Public Key Infrastructure.

QTSA

Qualified Time-stamping Authority.

QSCD

Qualified Signature Creation Device.

RA

Registration Authority.

TLS

Transport Layer Security.

TSA

Time-Stamping Authority.

TSP

Trust Service Provider.

TSU

Time Stamping Unit.

UTC

Coordinated Universal Time.

1.7. References

1.7.1. 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.

1.7.2. Informative references

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

Table 3. 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. Publication and repository responsibilities

2.1. Repositories

Entaksi maintains publicly accessible online repositories to ensure continuous availability of information necessary for the correct use and validation of certificates issued under its Public Key Infrastructure (PKI).
These repositories include:

- issued certificates (when publication is required and consent has been obtained);
- Certificate Revocation Lists (CRLs);
- the Online Certificate Status Protocol (OCSP) service;
- policies, practice statements, and disclosure statements relevant to Entaksi's Trust Services.

All repositories are available online 24 hours a day, 7 days a week, subject only to maintenance or circumstances beyond Entaksi's control. In such situations, Entaksi undertakes best efforts to restore availability as quickly as possible.

The CRL profile is described in CRL and CRL entry extensions, and the OCSP service profile is specified in OCSP profile.

2.2. Publication of certification information

Entaksi publishes its Trust Service documentation—such as Certificate Policies, Certification Practice Statements, the PKI Disclosure Statement, and related documents—in PDF format at:

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

Documents are kept up to date and are replaced whenever modifications, improvements, or regulatory updates occur. Each publication is versioned to ensure traceability.

2.3. Time or frequency of publication

Updates to published documents occur whenever changes affecting policies, practices or certificate profiles are approved by Entaksi.

CRLs are issued and published at regular intervals, with frequency detailed in CRL issuance frequency.

OCSP responses are available continuously, with real-time status information.

2.4. Access controls on repositories

All information intended for public use—such as published certificates, CRLs, Trust Service documents, and status information—is accessible without restrictions.

Only Entaksi is authorized to modify, update, or publish content within these repositories.
Write access is strictly controlled through internal security measures to ensure integrity and prevent unauthorized modifications.

3. Identification and authentication

3.1. Naming

Naming in certificate issued by the Certification Authorities under this policy follows the IETF RFC 5280 standard, "Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile (2008)", the Recommendation ITU-T X.509 and the appropriate controls from ETSI EN 319 412-1,2,3,5.

3.1.1. Types of names

Certificate holder is identified by the Distinguished Name in compliance with the X.509 standard.

Certificates issued under this policy are compliant with the following standards:

- 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.

3.1.2. Need for names to be meaningful

Certificate holders require a distinguished name in compliance with the X.500 standard for Distinguished Names.

The Subject Name of all digital certificates issued to legal persons includes at least the common name (`commonName`, OID 2.5.4.3) of the legal person and the organization identifier (`organizationIdentifier`, OID 2.5.4.97).

The Distinguished Name may include the following fields:

- `commonName` (OID 2.5.4.3).
- `givenName` (OID 2.5.4.42).
- `surname` (OID 2.5.4.4).
- `serialNumber` (OID 2.5.4.5).
- `countryName` (OID 2.5.4.6).
- `organizationName` (OID 2.5.4.10).
- `organizationalUnitName` (OID 2.5.4.11).
- `localityName` (OID 2.5.4.7).
- `stateOrProvinceName` (OID 2.5.4.8).
- `organizationIdentifier` (OID 2.5.4.97).
- `title` (OID 2.5.4.12).
- `dnQualifier` (OID 2.5.4.46).

3.1.3. Anonymity or pseudonymity of subscribers

Entaksi does not allow the use of pseudonym on the certificates.

3.1.4. Rules for interpreting various name forms

Rules for interpreting name forms can be found in ITU-T standards X.500 and applicable IEFT RFCs.

3.1.5. Uniqueness of names

For certificate issued by "Entaksi Qualified Electronic Signatures CA G1" and "Entaksi Qualified Electronic Seals CA G1" the uniqueness is granted by the combination of Subject attributes.

For certificates issued to natural persons:

- `givenName` (OID 2.5.4.42).
- `surname` (OID 2.5.4.4).
- `serialNumber` (OID 2.5.4.5).
- `dnQualifier` (OID 2.5.4.46).

For certificates issued to legal persons:

- `organizationName` (OID 2.5.4.10).
- `organizationIdentifier` (OID 2.5.4.97).
- `dnQualifier` (OID 2.5.4.46).

The subject name of each digital certificate issued by the "Entaksi Qualified Time-stamps CA G1" certification authority is unique within each class of digital certificate issued by the same certification authority, as granted by Entaksi's internal procedures.

The `serialNumber` field (for certificates issued by Entaksi Qualified Electronic Signatures CA G1) and the `organizationIdentifier` field (for certificates issued by Entaksi Qualified Electronic Seals CA G1) avoid any subject name collisions using the following structure:

- 3 character identity type reference
- 2 character ISO 3166-1 country code
- hyphen-minus "-"
- identifier (according to country and identity type reference)

For natural person, the three initial characters shall have one of the following values:

- PAS for identification based on passport number.
- `IDC` for identification based on national identity card number.
- `PNO` for identification based on (national) personal number (national civic registration number).
- `TIN` Tax Identification Number, according to the European Commission - Tax and Customs Union.

For legal person, the three initial characters shall have one of the following values:

- `VAT` for identification based on a national value added tax identification number.
- `NTR` for identification based on an identifier from a national trade register.
- `PSD` for identification based on the national authorization number of a payment service provider under Payments Services Directive (EU) 2015/2366.

3.1.6. Recognition, authentication, and role of trademarks

Entaksi is not obliged to seek evidence of trademark usage by any organization or individual.
When a client requests a certificate and seeks to include a brand name or trademark indication, the client must furnish evidence of the usage's legitimacy.
Certificate applicants assert and ensure that their interactions with the CA, as well as the utilization of information pertaining to certificate requests, do not infringe upon or adversely affect the rights of any third party in any jurisdiction.

3.2. Initial identity validation

The initial identity validation is performed in accordance with the **Identity Proofing Service Policy and Practice Statement (IPSPPS)** issued by Entaksi: "MAN eIDAS 20251125 Identity Proofing Service Policy and Practice Statement EN".
All identity proofing activities, including evidence collection, validation, binding, and issuance of the identity proofing result, follow the processes, assurance levels and requirements defined in the IPSPPS, which implements ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI TS 119 461 and the applicable provisions of eIDAS.

3.2.1. Method to prove possession of private key

The issuing certification authority uses the IETF PKIX Certificate Management Protocol PKCS#10 to prove the private key's possession of the certificate applicant.

3.2.2. Authentication of organization identity

The authentication of the identity of a legal person follows the procedures defined in the IPSPPS. Entaksi validates the legal existence, registration data and organization identifiers using trusted national registers or authoritative sources, and verifies the authority of the representative acting on behalf of the organization in accordance with ETSI TS 119 461 and the applicable identity proofing use cases.

3.2.3. Authentication of individual identity

The authentication of natural persons—whether acting as individuals or on behalf of a legal person—is carried out in accordance with the IPSPPS.
Identity proofing may occur through physical presence, attended or unattended remote identity proofing, authentication using an eID, or validation of a qualified electronic signature, as permitted by eIDAS Regulation.
All operational steps, evidence requirements, validation procedures and RAO responsibilities are defined in the IPSPPS.

3.2.4. Non-verified subscriber information

Certain pre-contractual information, such as address or telephone number, may not undergo verification by appointed RAOs. Entaksi bears no responsibility for the accuracy of these details.

3.2.5. Validation of authority

The validation of the authority of a natural person acting on behalf of a legal person is performed in accordance with the IPSPPS.
Entaksi verifies representation rights using authoritative registers, corporate documentation, electronic attestations of attributes, or other trusted evidence, following the procedures required for the applicable identity proofing use case under eIDAS Regulation.

3.2.6. Criteria for interoperation

Entaksi can interoperate with other Trust Service Providers, through specific agreements.

3.3. Identification and authentication for re-key requests

Entaksi does not perform re-keys on certificates.

3.3.1. Identification and authentication for routine re-key

Entaksi does not perform routine re-keys on certificates.

3.3.2. Identification and authentication for re-key after revocation

Entaksi does not perform re-keys on certificates.

3.4. Identification and authentication for renewal requests

Certificate renewal refers to the issuance of a new certificate to a subject who has previously been issued a certificate by Entaksi, without modifying the subject's certificate information.

Identity verification for certificate renewal requires the subject to provide a proof of ownership of the private key of the previously issued certificate and the previously issued certificate to be valid (i.e. not revoked nor suspended) and not expired.

The renewal requests involves the signature of a data object cryptographically bound to the certificate application for issuing the new certificate. Such signature shall be a valid signature at the time of the renewal request.

3.5. Identification and authentication for revocation request

The revocation or suspension of a certificate can be requested by sending the 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.

The completed request must:

- be submitted using the same email address indicated during the certificate application phase;
- include the reason for the request;
- contain a valid identification document of the requester.

Requests for revocation or suspension must also include all elements necessary for Entaksi to verify the identity and/or authority of the requester. Identity verification for revocation follows the methods defined in the IPSPPS, which specify the applicable procedures according to the requester's role (subject, subscriber, or an authorized representative of a legal person).

If any of the required elements are missing or incomplete, Entaksi will not proceed with the request.

4. Certificate life-cycle operational requirements

4.1. Certificate Application

n the context of this CP and CPS, Entaksi defines the relationships and responsibilities of the parties involved in a certificate application, in accordance with chapter PKI participants and the applicable provisions of ETSI EN 319 411-1 and ETSI EN 319 411-2.

An electronic signature is data in electronic form attached to or logically associated with other electronic data and used by a signatory, who is always a natural person.
An electronic seal is data in electronic form attached to or logically associated with other electronic data to ensure its origin and integrity, where the creator of the seal is a legal person.

The subject is the entity identified in the certificate as the holder of the private key corresponding to the public key certified by the CA.
Depending on the certificate type, the subject may be:

- a natural person;
- a natural person identified in association with a legal person;
- a legal person (including an organisation, unit, or department).

When the subscriber and the subject coincide, the subscriber is directly responsible for meeting all obligations.
When the subscriber acts on behalf of one or more subjects—for example, a company requesting certificates for its employees—the respective responsibilities of subscriber and subject are defined in the applicable Terms and Conditions.

The relationship between subscriber and subject follows these rules:

- For certificates issued to natural persons, the subscriber may be:
    - the natural person themself;
    - a natural person authorised to represent the subject;
    - an entity with which the natural person is associated (e.g., their employer).
- For certificates issued to legal persons, the subscriber may be:
    - any entity legally authorised to represent the legal person;
    - a natural person holding verified representation rights, requesting certificates for the legal person or its sub-entities.

4.1.1. Who can submit a certificate application

A qualified certificate may be requested directly from Entaksi CA or through one of its RAs.

For natural persons, the applicant may be the individual themself or, where applicable, a third party authorised to request the certificate (e.g., an employer requesting a certificate with an organisational attribute).

For legal persons, the application must be submitted by a natural person legally representing the entity.

Applicants must be at least 18 years old.

Certificates for Time-Stamp Units may only be requested by Entaksi internal Certification Authority Officers.

4.1.2. Enrollment process and responsibilities

After the authentication and identification phase the RAO must have collected all the documents that make up the contractual arrangement necessary for processing the certificate request.

The contractual arrangement comprises:

- Service contract ("Condizioni generali del servizio" or "General Terms and Conditions").
- Certificate issuance request form with attached identification document.
- 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".

The subscriber must read and accept all the documents composing the contractual arrangement.

Entaksi, having received and validated the documentation, communicates to the RAO and the subscriber the procedure for the certificate issuance.

To request a qualified certificate, the subject or subscriber must furnish the following obligatory details:

- full name;
- date, city, State, and country of birth;
- country of residence;
- mobile phone number;
- email address;
- ID code, tax registration code or equivalent;
- organization name (if legal person);
- organization tax code or VAT code (if legal person);
- organization full address (if legal person);
- organization contact email and phone number (if legal person).

All these details are required in the application form, that is available on Entaksi's website: https://www.entaksi.eu/en/documentation.html.

4.2. Certificate issuance

4.2.1. Certification Authority actions during certificate issuance

The Registration Authority Officer directly generates the pair of cryptographic keys on the secure signature devices, utilizing applications provided by the CA and following secure authentication procedures.

Subsequently, the RAO generates a certificate signing request for the public key in PKCS#10 format and submits this request to the CA using the Certificate Management Protocol (CMP) as described in RFC 4210.

The CMP request is authenticated either with a shared secret assigned to the RAO or signed with a certificate assigned to the RAO for this purpose. Entaksi, after confirming the validity of the request and ensuring the subject's capability to make the request, proceeds to generate the qualified certificate. The qualified certificate is then transmitted securely via a dedicated channel within the device.

The "Entaksi Qualified Time-stamps CA G1", Entaksi Qualified Electronic Signatures CA G1 and Entaksi Qualified Electronic Seals CA G1 certification authorities are signed by the "Entaksi QTSP Root CA G1", which is self generated and self-signed.

Time-stamp unit certificate provision

Certificate signing requests from the Entaksi TSA are submitted to the "Entaksi Qualified Time-stamps CA G1" certification authority for signing and a new certificate is generated for the Time-stamp Unit.

The certificate signing request is generated in the Time-stamp Unit and passed to the certification authority in the form of a PKCS#10 (RFC 2314) data object.

The issued X.509 certificate is passed back to the Time-stamp Unit for deploying.

4.2.2. Notification to subscriber by the CA of issuance of certificate

A notification is always sent to the subscriber at the end of the certificate issuance process, while there is no need to send any notification to the subject, as the certificate issuance occurs only in their presence.

4.3. Certificate acceptance

4.3.1. Conduct constituting certificate acceptance

Upon receiving a certificate, the subscriber is obligated to review its contents. If the certificate exhibits any defects or error deemed unacceptable by the subscriber, the Registration Authority Officer must promptly notify Entaksi, that subsequently will initiate the revocation process and take necessary steps to reissue a corrected certificate.

If the subscriber fails to reject the certificate within 7 days of its receipt, the certificate will be considered accepted.

4.3.2. Publication of the certificate by the CA

The certificate becomes publicly accessible immediately after the registration phase is completed, and the keys are issued by the Entaksi on the signature device.

4.3.3. Notification of certificate issuance by the CA to other entities

A confirmation email containing a confirmation message is sent exclusively to the subscriber. No notification is sent for TSA certificates.

4.4. Key pair and certificate usage

Key pair 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.

4.4.1. Subscriber private key and certificate usage

By using the private key the certificate holder unconditionally agrees to use the digital certificate in a manner consistent with the Key-Usage field extension included in the digital certificate profile.

4.4.2. Relying party public key and certificate usage

Relying parties must assess:

- The appropriateness of the use of the digital certificate for any given purpose and that the use is not prohibited by this policy (see Prohibited certificate uses).
- That the digital certificate is being used in accordance with its Key-Usage field extension.
- That the digital certificate is valid at the time of reliance by reference to Online Certificate Status Protocol or Certificate Revocation List checks.

4.5. Certificate renewal

4.5.1. Circumstance for certificate renewal

The certificate renewal process can be initiated only if the certificate has not expired, is not revoked or suspended.

Upon a renewal request a new certificate is issued, that is the process involves the generation of a new key pair.

For TSA certificates, a new certificate is issued quarterly by the Certification Authority Officer under the supervision of a Security Officer, following the internal procedures of Entaksi.

4.5.2. Who may request renewal

The certificate renewal process can be initiated by the subscriber.

See Identification and authentication for renewal requests.

4.5.3. Processing certificate renewal requests

The renewal request proceeds as follows:

1. The subscriber issues a renewal request using the service dashboard or one of the tools provided for managing the previously issued certificate.
2. The RAO verifies the condition for processing the request.
3. The subscriber uses one of the tools provided for managing the previously issued certificate to perform the technical operation that leads to the issuance of the new certificate to replace the previously issued one.

4.5.4. Notification of new certificate issuance to subscriber

A confirmation email containing a confirmation message is sent exclusively to the subscriber.

4.5.5. Conduct constituting acceptance of a renewal certificate

Thus key generation is not involved in a renewal process, Entaksi does not require any further acceptance process.
The subject installs the certificate into the device and accepts it through its usage without the need for additional declarations.

4.5.6. Publication of the renewal certificate by the CA

The certificate becomes publicly accessible immediately after the renewal phase is completed, and the keys are issued by the Entaksi on the signature device.

4.5.7. Notification of certificate issuance by the CA to other entities

See Notification of new certificate issuance to subscriber.

4.6. Certificate re-key

Entaksi does not perform re-keys on certificates.

4.6.1. Circumstance for certificate re-key

Entaksi does not perform re-keys on certificates.

4.6.2. Who may request certification of a new public key

Entaksi does not perform re-keys on certificates.

4.6.3. Processing certificate re-keying requests

Entaksi does not perform re-keys on certificates.

4.6.4. Notification of new certificate issuance to subscriber

Entaksi does not perform re-keys on certificates.

4.6.5. Conduct constituting acceptance of a re-keyed certificate

Entaksi does not perform re-keys on certificates.

4.6.6. Publication of the re-keyed certificate by the CA

Entaksi does not perform re-keys on certificates.

4.6.7. Notification of certificate issuance by the CA to other entities

Entaksi does not perform re-keys on certificates.

4.7. Certificate modification

Entaksi does not allow modification on certificates.

4.7.1. Circumstance for certificate modification

Entaksi does not allow modification on certificates.

4.7.2. Who may request certificate modification

Entaksi does not allow modification on certificates.

4.7.3. Processing certificate modification requests

Entaksi does not allow modification on certificates.

4.7.4. Notification of new certificate issuance to subscriber

Entaksi does not allow modification on certificates.

4.7.5. Conduct constituting acceptance of modified certificate

Entaksi does not allow modification on certificates.

4.7.6. Publication of the modified certificate by the CA

Entaksi does not allow modification on certificates.

4.7.7. Notification of certificate issuance by the CA to other entities

Entaksi does not allow modification on certificates.

4.8. Certificate revocation and suspension

The revocation or the suspension of a certificate can be requested by sending a specific form, at ca@entaksi.eu.
The form is available on Entaksi’s website at the following link: https://www.entaksi.eu/en/documentation.html.

4.8.1. Circumstances for revocation

Digital certificates are revoked when any of the information on a digital certificate changes or becomes obsolete or when the private key associated with the digital certificate is compromised or suspected to be compromised.

The subject may request the revocation of the certificate for one of the following reasons:

- the private key has been compromised;
- the secure signature device containing the key has been lost or damaged;
- the key or its activation code (PIN) is no longer secret;
- any other event has occurred that compromised the reliability level of the key.

4.8.2. Who can request revocation

A request to revoke or suspend keys and digital certificates may be submitted by persons authorized to do so under relevant contractual documentation.

Digital certificates issued by the "Entaksi Qualified Time-stamps CA G1" certification authority are only used of the Entaksi TSA, therefore certificate revocation requests can be issued only by the Entaksi TSA.

4.8.3. Procedure for revocation request

The revocation or suspension request proceed as follows:

The RAO:

1. Receives the revocation or suspension request request via email.
2. Verifies the presence of all required documents for follow up on the request.
3. Examines the documentation and ensure its compliance.
4. Provides any necessary clarifications or corrections via email.
5. Evaluates whether the applicant meets the requirements for the request of revocation or suspension.
6. In the case of a positive outcome, confirms the take in charge of the request, indicating the timeline.
7. In the case of a negative outcome, suspends the process and notifies the Certification Authority.
8. In the case of a positive outcome, transmits the collected documentation to the Certification Authority that updates the CRL list.

4.8.4. Revocation request grace period

The CRL's grace period extends from the CA's publication of the next CRL to the expiration of the current one. To prevent any disruptions for those involved, this duration exceeds the time it takes for the CA to generate and release a new CRL. Consequently, the current CRL remains valid until it is replaced by the new one, ensuring a seamless transition.

A new CRL is generated when a certificate is revoked.

4.8.5. Time within which CA must process the revocation request

The maximum delay between receiving a revocation or suspension request and making the status change available to all relying parties should not exceed 24 hours. If not Entaksi will record the actions taken along with justifications, and make them available to the relying parties.

Any exception procedures in case revocation requests cannot be confirmed within 24 hours is stated in the Terms and Condition of the service.

Entaksi does not provide faster process times. The revocation can be performed at a future date (e.g. subject's planned cessation from his/her duties at a certain date), then the scheduled date will be considered as the time at which receipt of the request has occurred. The future date should be indicated in the reason for the request.

The time module used for the provision of revocation or suspension services is synchronized with UTC at least once every 24 hours.

4.8.6. Revocation checking requirement for relying parties

Digital certificate revocation information is provided via the Certificate Revocation List for digital certificates in their current validity period.

Online Certificate Status Protocol can be used to check the revocation status of a certificate at a specific date in time up to the retention period of the certificate information.

To uphold the security standards established by Entaksi, PKI participants must verify the information outlined in the certificate.
This verification process should encompass the validation of Certificate validity, adherence to policy requirements and key usage, and confirmation of referenced Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) revocation information.

4.8.7. CRL issuance frequency

Certificate Revocation List is valid for 24 hours and is updated every 8 hours.

4.8.8. Maximum latency for CRLs (if applicable)

The time between the request for revocation or suspension and the confirmation with the issuance of a new CRL is at maximum 24 hours.

4.8.9. On-line revocation/status checking availability

The OCSP service is available 24 hours a day.

4.8.10. On-line revocation checking requirements

The validity of a digital certificate issued by the "Entaksi Qualified Time-stamps CA G1" certification authority must be checked online using the Certificate Revocation List or the Online Certificate Status Protocol responder by relying parties.

Failure to do so negates the ability of the relaying party to claim that it acted on the digital certificate with reasonable reliance.

4.8.11. Other forms of revocation advertisements available

Entaksi does not support any other form of revocation advertisement.

4.8.12. Special requirements regarding key compromise

Not applicable.

4.8.13. Circumstances for suspension

See Circumstances for revocation.

4.8.14. Who can request suspension

See Who can request revocation.

4.8.15. Procedure for suspension request

See Procedure for revocation request.

4.8.16. Limits on suspension period

After a predetermined 120-day period from the suspension date, a suspended certificate is automatically revoked by Entaksi. In this scenario, Entaksi also sends revocation notifications to the subject and the subscriber.

4.9. Certificate status services

Services for checking the status of the certificates are publicly available for relying parties.

4.9.1. Operational characteristics

The status of certificates can be checked through both Certificate Revocation List (CRL) and the Online Certificate Status Protocol (OCSP) service.

CRLs are signed by the CA they refer to.

Any updates to revocation status of a certificate cause the on-line certificate status service to reply with the updated status and the certificate revocation list to be upgraded with the updated status.

When an update to the revocation status of a certificate occurs, responses from the on-line certificate status service provide the updated revocation status immediately. The certificate revocation list is updated every 8 hours and lasts 24 hours before expiring. Relying parties may find differences in the revocation status obtained from the on-line certificate status service and the revocation status checked against a valid CRL downloaded up to 8 hours before the check operation, until the CRL expires.

CRLs can be retrieved with the HTTP protocol at the URLs specified the following table.

Table 4. CRLs.

CA	CRL's address
Entaksi QTSP Root CA G1	https://va.entaksi.eu/crls/Entaksi_QTSP_Root_CA_G1.crl
Entaksi Qualified Time-stamps CA G1	https://va.entaksi.eu/crls/Entaksi_Qualified_Time-stamps_CA_G1.crl
Entaksi Qualified Electronic Signatures CA G1	https://va.entaksi.eu/crls/Entaksi_Qualified_Electronic_Signatures_CA_G1.crl
Entaksi Qualified Electronic Seals CA G1	https://va.entaksi.eu/crls/Entaksi_Qualified_Electronic_Seals_CA_G1.crl

The OCSP responder endpoint is available at the following URL: https://va.entaksi.eu/ocsp.

4.9.2. Validity assurance for short-term certificates

Short-term certificates don't include neither the CRL distribution point nor access location of an on-line certificate status service.

Short-term certificates contain a validity assured extension for short-term certificates as specified in RFC 9608.

For certificates issued with the validity assured extension for short-term certificates, the time as indicated in the certificate attribute from `notBefore` through `notAfter`, inclusive, is shorter than 24 hours.

4.9.3. Service availability

Both CRLs and OCSP are available 24 hours per day, 7 days per week.

4.10. End of subscription

A subscriber may end a subscription with Entaksi's CA services allowing the certificate to expire or revoking the certificate.

4.11. Key escrow and recovery

Key escrow is allowed only for Entaksi CA and TSU keys in order to allow redundancy of the key-pairs among hardware security modules and for backup purposes.

The recovery process adheres to HSM procedures and operates under dual operator control.

Entaksi does not support any other form of key escrow.

4.11.1. Key escrow and recovery policy and practices

See Key escrow and recovery.

4.11.2. Session key encapsulation and recovery policy and practices

See Key escrow and recovery.

5. Facility, management, and operational controls

The Entaksi Solutions SpA organization is designed around these principles:

- The servers hosting the Certification Authority and the company’s trusted services are housed in data centers operated by specialized providers. Contracts between Entaksi and these providers are regularly reviewed to ensure optimal performance and market-competitive value. The same approach applies to general network services—such as domain names and DNS—which are also managed by external providers.
- All employees and collaborators has a contract that favors remote working.

The result of these statements is that the company operates entirely on the network, not relying on physical headquarters and facilities. Therefore, Entaksi does not regulate directly the control of physical access to the infrastructures, instead it checks the suppliers during the qualification phase, monitors the SLA defined by the contracts and, if necessary, conducts audits.

Hence Entaksi guarantees the compliance with the requirements about physical security management of the central infrastructure through an accurate qualification process and by monitoring the suppliers, who are selected on the basis of market convenience and on the quality standard guaranteed in terms of security, such as, for example, the certification ISO/IEC 27001:2022.
Entaksi also requires, according the limits of the contract, the possibility for the supplier to be subjected to audits and inspections, in order to identify any elements not sufficiently covered by the contractual conditions or by the certifications themselves.

Entaksi keeps the PKI devices, including Hardware Security Modules and servers used for the PKI management, in selected datacenters where a secure area is dedicated for this purpose and is accessible only to authorized personnel.

Facility management, physical security and operational controls are part of the datacenter services and are delegated to the entity that manages the datacenter.

5.1. Physical controls

Entaksi defines a list of physical and environmental security controls in order to protect the CA hardware resources.

5.1.1. Site location and construction

Three secure areas are located in three different datacenters for redundancy and business continuity.

Datacenters are built with state-of-the-art security measures.

5.1.2. Physical access

Entaksi does not directly regulate the control of physical access to infrastructures, but applies controls on the qualification phase of the suppliers.

The CA management facilities are operated in a secure environment which is physically and logically protected from unauthorized access to systems or data.

Every entry to the secure area is subject to independent oversight. Non authorized persons can access the secure area only accompanied by an authorized person. Every entry and exit to or from the secure area is logged.

The CA management facilities are inside a defined security perimeter made of a server rack with a locker that can be opened only by authorized persons so that other organizations are not allowed to enter into this security perimeter.

The secure area is inside a datacenter facility with adequate protection for system resources, including state-of-the-art measures for access control, natural disaster protection, fire safety, power failures, communication interruptions, structure collapse, leaks, theft, breaking.

The CA services cannot be taken off-site without authorization.

5.1.3. Power and air conditioning

The secure area hosting the PKI facilities has redundant power supply and controlled air temperature.

5.1.4. Water exposures

The datacenters are protected from water exposure.

5.1.5. Fire prevention and protection

The datacenters implement adequate fire prevention and protection counter measure.

5.1.6. Media storage

Any media containing sensible information, including backup media, are stored in containers, cabinets or safes with fire protection capabilities and are located within the secure area.

5.1.7. Waste disposal

Entaksi implements operational procedures for secure destruction of data before disposing electronic devices.

5.1.8. Off-site backup

Off-site backup of the PKI facilities, including software and data, is stored in strongly encrypted form in the Entaksi object storage service.

5.2. Procedural controls

Administrative procedures related to personnel and procedura requirements are maintained in accordance with this Certificate Policy and Practice Statement and other relevant documents.

Entaksi does not outsource any of its PKI operation to other organizations.

5.2.1. Trusted roles

In order to ensure that one person acting alone cannot circumvent security safeguards, responsibilities are shared by multiple roles and individuals. This is accomplished by creating separate roles and accounts on various components of the CA system, and each role has a limited amount of capability.

Defined roles are:

- **Certification Authority Officers**, who are responsible for Certification Authority hardware and software, and the generation and signing of issuing Certification Authority keys.
- **Registration Authority Officers**, who are appointed by Registration Authorities and given responsibility for the operation of the Registration Authority functions.
- **Security Officer**, who is responsible for verifying the integrity of the Certification Authority, its functions and procedures.
- **Backup Officer**, who is responsible for backup and restore of Certification Authority keys.

5.2.2. Number of persons required per task

Key-pairs generation and initialization of Certification Authority requires the participation of at least two individuals.

5.2.3. Identification and authentication for each role

For the identification and authentication of trusted roles digital keys and cryptographic tokens assigned to individuals in role are used.

Personnel authenticate as person in role by using such assigned digital keys and cryptographic tokens.

Upon assigning a role to a person the corresponding digital key or cryptographic token is made available to that person.

5.2.4. Roles requiring separation of duties

For roles requiring separation of duties, like the cryptographic device Master Backup Key management, cryptographic techniques are used so that the key is split in three parts and at least two of them are needed in order to authorize the operation.

5.3. Personnel controls

Entaksi employs a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide CA services.

5.3.1. Qualifications, experience, and clearance requirements

Entaksi commits to employ qualified staff who possess the necessary expertise, reliability, experience, and qualifications to work on the qualified trust services.

Security roles and responsibilities are clearly identified in job descriptions and in the internal documents, persistently available to all concerned personnel.
The roles are differentiated between general functions and QTSP specific functions.
Entaksi defines the minimum requirements to fill the roles: all the personnel shall possess experience or training with respect to the service provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

All Entaksi's personnel involved in trusted roles shall be free from conflict of interest that might prejudice the impartiality of Entaksi's operations.

5.3.2. Background check procedures

All personnel involved in a trusted role is checked for conflict of interests and other malicious interferences, applying UNI ISO 37001:2016 controls.

Personnel have access to the trusted functions only after the management completes the necessary checks.

Entaksi maintains records of personnel activities.

5.3.3. Training requirements

Entaksi provides constant training regarding security and personal data protection rules as appropriate for the offered services and the job function.

5.3.4. Retraining frequency and requirements

Entaksi training and self-training session are scheduled regularly and every time a change occurs in systems or requirements.

The reviewing process of the training scopes and of the experience gained by the staff takes place periodically, on an annual basis at least. Accrued skills are recorded in the Entaksi databases.

5.3.5. Job rotation frequency and sequence

Entaksi provides and maintains a program of job rotation in order to maintain appropriate and required level of competency across key roles.

5.3.6. Sanctions for unauthorized actions

Entaksi foresees in its documentation, formally accepted by the employee, that adequate disciplinary sanctions can be put in place to personnel who violate the security policies or procedures. Personnel shall exercise administrative and management procedures and processes that are in line with Entaksi's management procedures.

The acceptance procedure involves a reviewing from the management and the signature of the employee on the appointment document.

5.3.7. Independent contractor requirements

Entaksi doesn't delegate trusted roles to external contractors.

5.3.8. Documentation supplied to personnel

Entaksi provides personnel with all required materials and documentations for their job function.

5.4. Audit logging procedures

Entaksi’s systems are constantly monitored: this activity includes regularly monitoring or reviewing audit logs to identify evidence of malicious activity, implementing automated mechanisms to process audit logs and alerting staff of possible security-critical events.

Entaksi PKI uses an event log collection and review as part of its information security management system.

5.4.1. Types of events recorded

Events recorded in logs are:

- failed and successful logins;
- modification of security settings;
- privileged use or escalation of privileges;
- system events;
- modification of system-level objects;
- all operations related to the performing of a qualified trust service;
- session activity;
- account management activities including password changes (success and failure).

Each log reports the following information:

- date and time of activity;
- peer IP address (for connection logs);
- user ID;
- description of attempted or completed activity;
- client requests and server responses;
- abnormal usage, e.g. number of transactions, usage spikes, etc.;
- abnormal application behavior, including repeated application restart;
- data modification where required for regulatory compliance.

Each log contains the exact time of the event, a reference to the user and a description of the operation. Logs are recorded in chronological order, and the time used to record events as required in the audit log is synchronised with UTC time at least once a day.

5.4.2. Frequency of processing log

Each log contains the exact time of the event, a reference to the user and a description of the operation. Logs are recorded in chronological order, and the time used to record events as required in the audit log is synchronised with UTC time at least once a day.

Entaksi ensures an appropriate log monitoring, and review logs in response to suspected or reported security problems.

5.4.3. Retention period for audit log

Entaksi records and stores in its eCON Preservation Service the event logs produced by its systems for at least 6 months. These logs are fully archived as confidential, and may provide evidence in legal proceedings and in order to guarantee continuity of service.
The log preservation policy is the same as for documents, digital signatures and seals, in order to maintain the confidentiality and integrity of records relating to the operation of the service.

CA audit log retention period is 20 years.

5.4.4. Protection of audit log

Logs are accessed, secured and protected according to the nature of the information they may contain. Except for Entaksi any activity of logging review, such as auditing or inspection, is recorded.

CA audit log is subject to integrity protection.

5.4.5. Audit log backup procedures

Logs are sent for digital preservation daily.

5.4.6. Audit collection system (internal vs. external)

Security audit processes are invoked at system startup and cease only at system shutdown.

These processes collect events that happens during the CA operations.

5.4.7. Notification to event-causing subject

Where an event is logged, no notice is required to be given to the individual, organization, device or application that caused the event.

5.4.8. Vulnerability assessments

Entaksi regularly undergoes a Vulnerability Assessment and Penetration Test.
The vulnerability scan is done on public and private IP addresses identified by Entaksi's Technical Manager, and is performed by an external body with the necessary skills, tools, proficiency, code of ethics, and independence to provide a reliable report.

Vulnerability and penetration tests on Entaksi's systems are set up at least yearly or after significant upgrades or changes to the infrastructure or application.

Entaksi archives in its systems the records, evaluations and minutes of all tests performed.

5.5. Records archival

5.5.1. Types of records archived

For each digital certificate, the records contain information related to creation, issuance, intended use, revocation and expiration.

These records will include all relevant evidence in the issuing certification authority possession, including:

- Audit logs.
- Digital certificate requests and all related actions.
- Contents of issued digital certificates.
- All the contractual arrangement components enlisted in Enrollment process and responsibilities.
- Revocation / suspension requests and all related actions.
- Renewal requests and all related actions.
- Archive and retrieval requests.
- Digital Certificate Revocation Lists posted.

5.5.2. Retention period for archive

Audit logs relating to the certificate lifecycle are retained for 20 years.

5.5.3. Protection of archive

Archives are stored in the Entaksi eCON Digital Preservation System, which is a Qualified Preservation System for digital signatures and seals operating under the provisions of the ETSI TS 119 511 specifications.

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.

5.5.4. Archive backup procedures

Archive backup procedures are demanded to the digital preservation system.

5.5.5. Requirements for time-stamping of records

Records are time-stamped as part of the process of storing in the digital preservation system.

5.5.6. Archive collection system (internal or external)

Archive collection system is internal only.

5.5.7. Procedures to obtain and verify archive information

Procedures for obtaining and verifying archive information are defined in the digital preservation system.

5.6. Key changeover

Key changeover is performed manually by the Certification Authority Officer. A key ceremony takes place for generation and activation of the new keys.

5.7. Compromise and disaster recovery

Entaksi PKI is subject to the same disaster recovery procedure of the Entaksi integrated management system. Business continuity and disaster recovery procedure are defined and compliant with the provisions of the ISO/IEC 22301:2019 specifications.

5.7.1. Incident and compromise handling procedures

Entaksi defines a "security incident" as any event that compromises or threatens the correct functioning of the organization's systems and/or networks or the integrity and/or confidentiality of the information stored in the systems or in transit, or that violates the defined security policies or laws in force, with particular reference to General Data Protection Regulation (EU) 2016/679.

The Incident Response Team (IRT) is a group of suitably qualified and trusted members of the organization that manages incidents throughout their lifecycle.

Incident management procedures are based on adherence to ISO/IEC 27035:2016 standard.

The incident management process defined by Entaksi is divided into the following phases:

- **Plan and prepare**: establish an information security incident management policy, form an Incident Response Team, prepare the organization to respond to any malicious event.
- **Detection and reporting**: one or more security events need to be recognized as an incident, and each incident is assigned a severity level.
- **Assessment and decision**: the IRT makes an assessment that determinate whether it is in fact an incident and qualifies it.
- **Response**: implementation of countermeasures to minimize the damage caused by the accident, and, if necessary, adjustment of the resources and restoration if needed.
- **Subsequent activities**: the update of the risk analysis and the adequacy of the accident management procedures.
- **Lessons learned**: Entaksi's management reviews the incident and identifies possible points for improvement.

More details and the disaster recovery plans are described in Entaksi's internal procedures.
Disaster recovery infrastructure and procedures are fully tested yearly.

5.7.2. Computing resources, software, and/or data are corrupted

Corruption of computing resources, data and/or software are managed using a backup site.

5.7.3. Entity private key compromise procedures

Incidents that involve a private key compromise are addressed according to a specific procedure described in the Entaksi's business continuity plan.

A compromise of the CA private key(s) necessitates an immediate revocation of the affected certificate(s). To address the situation effectively, Entaksi will undertake the following actions:

- Cease the operation of any qualified services impacted by the compromise.
- Revoke all certificates that have become unreliable due to the identified event.
- Promptly publish a Certificate Revocation List (CRL) containing updated revocation information.
- Notify PKI participants of the compromised key, ensuring transparent communication.
- Inform the Conformity Assessment Body about the security incident.

After the remediation of the cause(s) of the incident Entaksi will proceed to generate a new key pair and a new CA certificate. This updated set of credentials will be securely distributed to relevant PKI participants.

5.7.4. Business continuity capabilities after a disaster

The Entaksi PKI continues to operate with full capability as far as at least one of the three redundant site is available.

5.8. Cybersecurity risk management

Entaksi establishes, implements, maintains and continually improves a documented cybersecurity risk-management process to ensure that all risks affecting the security, availability, integrity, authenticity and confidentiality of its trust services, networks and information systems are systematically identified, analysed, evaluated, treated, monitored and reviewed.

This process is an integral part of the Integrated Management System and is fully aligned with the methodology based on ISO/IEC 31000:2018 and ISO/IEC 31010:2019 models and adapted to Entaksi's organisational context—ensures a unified approach to the assessment and treatment of risks across all domains covered by the IMS (information security, business continuity, service management, anti-corruption, data protection and trust service provision).

Entaksi performs regular, systematic and documented risk assessments covering all trust service operations, infrastructures, processes and supporting assets.
The risk assessment applies the corporate methodology, structured around asset–threat relationships, and uses the consolidated quantitative/qualitative scales for Probability (P), Impact (I) and Vulnerability (V).
The risk assessment includes:

- identification of assets / Configuration Items (CIs) using the CMDB platform;
- evaluation of assets according to the impact domains relevant to their classification (critical, vital, sensitive) as defined in the Business Continuity criteria;
- identification of threats, covering all the topics related to IMS's management;
- attribution of Probability, Impact and Vulnerability, using the calibrated scales maintained in the CMDB and automatically updated when incident data is available;

- calculation of the risk level through the methodology's defined correlation matrices.

Risk assessments are carried out at least annually, and whenever significant changes to operations, infrastructure, technologies, or threat landscape occur, or after significant security incidents.

All risk-assessment results are documented and archived within Entaksi preservation system.

5.8.1. Risk management process

Entaksi maintains a documented cybersecurity risk-management process based on an all-hazards approach.

The process includes:

- definition of scope, scenarios and boundaries;
- identification and classification of assets and CIs;
- identification and documentation of threats, including:
  - physical threats;
  - cyber threats;
  - supply-chain and third-party risks;
  - corruption-related threats;
- analysis of the relationships between threats, vulnerabilities, asset value and impacts;
- evaluation of risks against the defined risk criteria and thresholds for acceptable risk;
- selection of appropriate treatment measures based on cost/benefit and operational feasibility;
- assignment of responsibilities for control implementation;
- continuous monitoring and periodic improvement.

Entaksi also considers threats specific to the provision of eIDAS trust services, affecting processes such as identity verification, certificate issuance, device management (QSCD), signature creation, time-stamping, and preservation of evidence.

This process is reviewed at least annually and approved by Entaksi management.

5.8.2. Risk criteria, risk appetite and risk tolerance

Entaksi defines and documents risk criteria, including impact categories (availability, integrity, authenticity, confidentiality, compliance and service continuity).

Entaksi's risk appetite is expressed as a high-level statement by management indicating the degree of risk the organisation is willing to accept in achieving its trust-service objectives.

From this, Entaksi defines risk tolerance levels specifying the maximum acceptable residual risk for each category or process, using quantifiable thresholds where possible (e.g., downtime, data-loss thresholds, acceptable monetary impact).

These parameters guide risk evaluation, prioritisation and treatment decisions.

5.8.3. Risk treatment plan

Based on the results of the risk assessment, Entaksi establishes, implements and maintains a Risk Treatment Plan (RTP) describing:

- selected treatment options (avoid, mitigate, transfer, accept);
- technical, organisational and procedural controls mapped to IMS controls;
- justification for selected measures, including cost-benefit considerations;
- responsibilities, implementation timelines and dependencies;
- performance and effectiveness metrics aligned with control objectives from IMS;
- vulnerability and incident monitoring criteria from the CMDB.

Residual risks remaining after treatment are explicitly documented and formally accepted by Entaksi's management bodies or persons delegated with risk-management authority.

The RTP is monitored continuously and reviewed at least annually.

5.8.4. Monitoring, Measurement and Evaluation

Entaksi establishes and applies policies and procedures for continuous monitoring and measurement of cybersecurity risk-management measures. These procedures incorporate the monitoring rules included in the IMS and the dynamic update mechanisms of the CMDB.

These procedures define:

- the controls, processes and treatment measures subject to monitoring;
- methods and tools used (vulnerability assessments, penetration tests, system logs, supplier monitoring, continuous availability checks);
- monitoring frequencies (aligned with control categories and incident statistics);
- roles and responsibilities;
- criteria for evaluating effectiveness and triggering re-assessment;
- escalation and reporting mechanisms based on the SIG incident-management process.

Monitoring activities include, but are not limited to: vulnerability assessments, penetration testing, configuration audits, log reviews, service-availability measurements, integrity checks and continuous performance monitoring of critical components.

5.8.5. Review and update of the risk management process

Entaksi reviews the cybersecurity risk-management process, the Risk Assessment and the Risk Treatment Plan at least once per year and after any significant incident or significant changes to technologies, procedures, personnel, infrastructure or external conditions.

5.8.6. Management approval and governance

Entaksi's Management must approve the risk-assessment framework and the cybersecurity risk-management process, the Risk Treatment Plan and formally accept residual risks.

Entaksi Management also reviews risk-management outputs during management-review activities.

5.9. CA or RA termination

The decision of terminate the certification authority service can be taken only by the Entaksi management.

The CEO, hearing the opinion of shareholders, will formalize the termination of service and the activation of the termination plan.

A specific document describes the termination plan and the procedure to apply for each termination step. The plan is constantly kept up-to-date by Entaksi Management.

The termination plan describes all the activities summarized in the following list:

1. **Decision to terminate the service**: the management of Entaksi, having heard the opinion of the shareholders, can declare the termination of the CA service. Contextually the management drafts a special report in which the reason for the termination is detailed, the termination is scheduled, and the termination program is started.
   At the same time, the acquisition of new customers is ceased.
2. **Communication to interested parties**: during the termination procedure, the interested parties, are notified of the ceasing of the service. Communication takes place at least 60 days before the actual termination of the service. All parts must be notified without delay.
   Responsibility for communication is entrusted to Entaksi Management, which approves the content of the e-mail. The database of third-party e-mails is kept updated on the system.
   In addition to sending e-mail communications, a termination notice for the service is published on the company's website https://www.entaksi.eu/en/.
3. **Termination of subcontractors**: Entaksi does not currently use subcontractors, but it has a specific internal procedure that regulates relations with suppliers and other subcontractors.
4. **Communication with the authority and transfer of documentation**: the termination is communicated also to the relevant authority, that can acquire the documentation proving the management of CA service (technical documentation, service manuals, system, SLA template, certificates).
5. **Termination**: after 6 months from the ceasing of the service, once the termination period has ended, the IT management proceeds to permanently delete any personal data from the systems (such as registration informations). The deletion is extended to all backup copies and it is done using the most up-to-date secure cancellation technology available. All the documents are kept by Entaksi until the end of their validity.

6. Technical security controls

The Entaksi certification authority private keys are protected within a hardware security modules which are Common Criteria certified according to the EN 419 221-5 Protection Profile.

Access to the modules within the Entaksi environment are restricted by the use of token and smart cards and associated pass phrases. These smart cards and pass phrases are allocated among the multiple members of the Entaksi Management team and defined trusted roles.

6.1. Key pair generation and installation

Key pair generation and installation for certification authorities follows a specific key ceremony and happens inside the hardware security module under the provisions and the specific requirements of EN 419 221-5 Protection Profile.

The same procedure and security controls also apply to key pairs generated for the Time-stamping Unit.

6.1.1. Private key delivery to subscriber

Private key for subscriber certificates are always generated inside the QSCD assigned to the subscriber.

6.1.2. Public key delivery to certificate issuer

Public key is delivered to certificate issuer inside a digital certificate signed by the certification authority as an X.509 v3 certificate.

6.1.3. CA public key delivery to relying parties

Certification authority certificate containing the public key is available for download to subscribers and relying parties in the Entaksi web site at https://www.entaksi.eu/en/documentation.html.

Certification authority certificate is also available in the EU Trusted List.

6.1.4. Key sizes

Key size for RSA keys is 4096 bits.

6.1.5. Public key parameters generation and quality checking

Certification Authorities use different key pairs for signing and encrypting.

Public keys associated to private keys used for signing have parameters that allow to use the public key for verifying and not for decrypting.

Public keys associated to private keys used for encrypting have parameters that allow to use the public key for decrypting and not for verifying.

6.1.6. Key usage purposes (as per X.509 v3 key usage field)

Key usage extension is used as per X.509v3 specification:

- Bit 0: `digitalSignature`
- Bit 1: `nonRepudiation` (or `contentCommitment`)
- Bit 2: `keyEncipherment`
- Bit 3: `dataEncipherment`
- Bit 4: `keyAgreement`
- Bit 5: `keyCertSign`
- Bit 6: `cRLSign`
- Bit 7: `encipherOnly`
- Bit 8: `decipherOnly`

Certification authority certificates use the following KeyUsage bits marked as critical:

- Bit 0: `digitalSignature`.
- Bit 5: `keyCertSign`.
- Bit 6: `cRLSign`.

Certificates issued to the Entaksi Time-stamp Unit use the following KeyUsage bits marked as critical:

- Bit 0: `digitalSignature`.
- Extended KeyUsage: Timestamping (OID `1.3.6.1.5.5.7.3.8`)

Certificates issued to natural person for the creation of digital signatures and certificates issued to legal person for the creation digital seals uses the following KeyUsage bit marked as critical:

- Bit 1: `nonRepudiation` (or `contentCommitment`)

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Private keys are generated and stored in the secure cryptographic device and cannot be exported.

6.2.1. Cryptographic device standards and controls

Secure cryptographic devices used by Entaksi are Common Criteria certified and meet the requirements of EAL 4 augmented with AVA_VAN.5. As such, the devices are compliant with the following technical specification and protection profiles:

- EN 419 221-5 Protection profiles for TSP Cryptographic Modules; Part 5: Cryptographic Modules for Trust Services.
- EN 419 241-1 Trustworthy Systems Supporting Server Signing; Part 1: Security requirements.
- EN 419 241-2 Trustworthy Systems Supporting Server Signing; Part 2: Protection Profile for Qualified Signature Creation Device (QSCD) for Server Signing.
- EN 419 231 Protection profile for trustworthy systems supporting time stamping.

6.2.2. Private key (n out of m) multi-person control

Master Backup Key used for getting an encrypted copy of the cryptographic material inside the hardware secure cryptographic device is split in three parts so that two of them are needed for multi-person control of the Master Backup Key usage.

6.2.3. Private key escrow

See Key escrow and recovery.

6.2.4. Private key backup

Private key backup is possibile in encrypted form using the Master Backup Key with two out of three multi-person control.

See Key escrow and recovery.

6.2.5. Private key archival

Private keys are archived in secondary hardware security modules for redundancy and in the backup storage encrypted with the Master Backup Key.

6.2.6. Private key transfer into or from a cryptographic module

Private keys can be transferred into or from a secure cryptographic device using the encrypted backup and provided that all secure cryptographic device use the same Master Backup Key.

6.2.7. Private key storage on cryptographic module

Private keys stored in a secure cryptographic device can be use only by the cryptographic module itself performing cryptographic functions.

6.2.8. Method of activating private key

Private keys must be activated using the application interface of the hardware security module and the activation key with which the private key was initialized.

6.2.9. Method of deactivating private key

Private keys can be deactivated using the application interface of the hardware security module.

6.2.10. Method of destroying private key

Private keys can be destroyed deleting them from the hardware secure cryptographic device where they reside.

6.2.11. Secure cryptographic device rating

Cryptographic modules used in the Entaksi PKI implement are Common Criteria certified and meet the requirements of EAL 4 augmented with AVA_VAN.5.

6.3. Other aspects of key pair management

6.3.1. Public key archival

Public key are archived in the database managed by the Entaksi PKI software.

6.3.2. Certificate operational periods and key pair usage periods

Usage periods for public keys and private keys match the usage periods for the Digital Certificate that binds the Public Key to an individual, organization, or device.

- "Entaksi QTSP Root CA G1" is valid for 30 years.
- "Entaksi Qualified Time-stamps CA G1" is valid for 20 years.
- "Entaksi Qualified Electronic Signatures CA G1" is valid for 20 years.
- "Entaksi Qualified Electronic Seals CA G1" is valid for 20 years.

A new generation of Certification Authority is set on "Gx" value and will be performed every 10 years.

6.4. Activation data

Private keys activation requires the activation key that has been used when initializing the private key.

6.4.1. Activation data generation and installation

Activation data is generated within the secure cryptographic device.

6.4.2. Activation data protection

Activation data is protected in the database of the Entaksi PKI software.

6.4.3. Other aspects of activation data

There are no other relevant aspects regarding activation data.

6.5. Computer security controls

Entaksi implements a set of security controls as part of its implementation of the ISO/IEC 27001:2022 specification.

Detailed descriptions of implemented computer security controls are available as internal document(s).

6.5.1. Specific computer security technical requirements

Void.

6.5.2. Computer security rating

Void.

6.6. Life cycle technical controls

Entaksi implements a set of life cycle technical controls as part of its implementation of the ISO 9001:2015 specification.

6.6.1. System development controls

Void.

6.6.2. Security management controls

Void.

6.6.3. Life cycle security controls

Void.

6.7. Network security controls

Networks and systems are protected against attack using firewalls and network segmentation in order to logically separate different trustworthy systems and services. Network security measures apply to all systems in the same network segment.

Communications among different network segments are restricted to those actually needed for function provided by each network segment and all other communication are forbidden. The rule set in the firewall configuration is reviewed every time a change occurs in the network or in the services.

Systems that are critical for the Certification Authority management and operation, such as the hardware security modules and the servers used to create and manage the life cycle of certificates, generate, sign and publish the Certificate Revocation List and to provide the certificate status service are located in a secure area according to the technical requirements specified in ETSI EN 319 411-1.

The administration of IT systems uses a network segment separated from the network segments used for service operation and this network segment is used only for this purpose.

Production system are separated from systems used for testing and other non production goals.

All communication among systems are encrypted in order to prevent any information disclosure and to ensure the integrity of data.

All systems are replicated for high availability.

Vulnerability assessment are performed on regular basis on internal and external endpoint.

Networks and systems are subject to a penetration test operated by a certified, external and independent entity once a year. Penetration test results are collected in a report and analyzed for addressing any critical outcome that should arise.

Firewalls are configured for each network segment so that only needed connections is allowed.

6.8. Time-stamping

Entaksi uses its own TSA service.

NTP protocol guarantees system time accuracy. The time included in Time-stamps is traceable to the real time value distributed by the Italian "Istituto Nazionale di Ricerca Metrologica", a laboratory of the Bureau International des Poids et Mesures (BIPM).

Entaksi’s Qualified Time Stamp Service is supported by the following policies, practice statements and manuals:

Table 6. TSA documents name and identification.

OID	Description	Permanent Link
`1.3.6.1.4.1.57823.1.12`	MAN eIDAS 20230426 TSA Disclosure Statement EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.12
`1.3.6.1.4.1.57823.1.11`	MAN eIDAS 20230426 TSA Policy and Practice Statement EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.11

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

7. Certificate, CRL, and OCPS profiles

7.1. Certificate profile

The applicable certificatePolicies OIDs and semantics identifiers (QCP-n-qscd / QCP-l-qscd) are specified in Certificate usage.

Digital certificates issued under this policy conform to Digital Certificate and Certificate Revocation List profiles as described in RFC 5280 and utilise the ITU-T X.509 version 3 Digital Certificate standard.

Digital certificates issued under this policy conform to the Normalized Certificate Policy requiring a secure cryptographic device (NCP+) identified by OID `0.4.0.2042.1.2`.

7.1.1. Version number(s)

X.509 version number is 3.

7.1.2. Certificate extensions

Certificates issued under this policy contain the following certificate extensions:

- `KeyUsage` (OID 2.5.29.15) marked as critical.
- `CertificatePolicies` (OID 2.5.29.32).
- `CRLDistributionPoints` (OID 2.5.29.31).
- `AuthorityKeyIdentifier` (OID 2.5.29.35).
- `SubjectKeyIdentifier` (OID 2.5.29.14).
- `AuthorityInformationAccess` (OID 1.3.6.1.5.5.7.1.1).
- `qCStatements` (OID 1.3.6.1.5.5.7.1.3).

`KeyUsage` extension content is specified in section Key usage purposes (as per X.509 v3 key usage field).

`CertificatePolicies` extension content is specified in section Certificate policy object identifier.

`CRLDistributionPoints` extension content is specified in CRL and CRL entry extensions.

`AuthorityInformationAccess` extension content is specified in OCSP profile.

`qCStatements` extensions contains the following items:

- `QcCompliance` (OID 0.4.0.1862.1.1), a statement claiming qualified certificate compliance.
- `QcRetentionPeriod` (OID 0.4.0.1862.1.3), a statement that set retention period to 20 years.
- `QcSSCD` (OID 0.4.0.1862.1.4), a statement claiming that the private key related to the certified public key resides in a qualified electronic Signature/Seal Creation Device.
- `QcType` (OID 0.4.0.1862.1.6), a statement claiming that the certificate is a European Union qualified certificate of a particular type.
- QcPDS (OID 0.4.0.1862.1.5), a statement that specifies the URL to the Entaksi PKI Disclosure Statement.

7.1.3. Algorithm object identifiers

Hash functions are:

- `id-sha256/sha256` (OID 2.16.840.1.101.3.4.2.1)
- `id-sha512/sha512` (OID 2.16.840.1.101.3.4.2.3)

Key generation algorithms are:

- `RSA-3072`
- `RSA-4096`
- `secp256r1/prime256v1` (OID 1.2.840.10045.3.1.7)

- `secp384r1/ansip384r1` (OID 1.3.132.0.34)

Certificates are signed with the following algorithms:

- `sha256WithRSAEncryption` (OID 1.2.840.113549.1.1.11).
- `sha512WithRSAEncryption` (OID 1.2.840.113549.1.1.13).
- `ecdsa-with-SHA256` (OID 1.2.840.10045.4.3.2)
- `ecdsa-with-SHA512` (OID 1.2.840.10045.4.3.4)

7.1.4. Name forms

See section Types of names.

7.1.5. Name constraints

See section Types of names.

7.1.6. Certificate policy object identifier

The OID assigned to this Certificate Policy and Certification Practice Statement is: 1.3.6.1.4.1.57823.1.9.

7.1.7. Usage of Policy Constraints extension

Policy constraints extension is not used.

7.1.8. Policy qualifiers syntax and semantics

Digital Certificates issued under this policy contain the object identifier (OID) for this Certificate Policy and Certification Practice Statement (OID 1.3.6.1.4.1.57823.1.9) in the `CertificatePolicies` extension (OID 2.5.29.32) with a "CPS URI" qualifier containing a link to the publicly available version of this document.

7.1.9. Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2. CRL profile

Certificate Revocation Lists are issued in the X.509 version 3 format in accordance with RFC 5280.

7.2.1. Version number(s)

CRL version number is 2.

7.2.2. CRL and CRL entry extensions

CRL entries contain the extension that indicates the reason for certificate revocation.

CRLs are available as described in Operational characteristics.

7.3. OCSP profile

Online Certificate Status Protocol profile is as defined in RFC 6960.

OCSP responder is available at https://va.entaksi.eu/ocsp.

The OCSP responder doesn't respond with "good" for a certificate that doesn't exist.

7.3.1. Version number(s)

OCSP version number is 1.

7.3.2. OCSP extensions

The OCSP responder uses the following extension:

- Archive Cutoff (OID 1.3.6.1.5.5.7.48.1.6).

The OCSP responder uses the issuer’s `notBefore` date as the archive cutoff date in OCSP responses.

8. Compliance audit and other assessments

The applicable legal system is declared in References.

The configuration of the Entaksi's Integrated Management System is regularly checked by the management to avoid any change which violate Entaksi's security policies.
The system is checked by at least yearly by an accredited certification body, recognized by Accredia, the Italian Accreditation Body.

Audit working papers and inspection documents are classified as confidential.

The conformity certificates and their updates are published in accordance with the assessment results on the Entaksi's website at the following link: https://www.entaksi.eu/en/certifications.html

8.1. Frequency or circumstances of assessment

Assessments are conducted yearly.

8.2. Identity/qualifications of assessor

The conformity checks (audits) on Entaksi are conducted by an assessment body accredited in accordance with Regulation (EC) no. 765/2008, through qualified and competent personnel on the subject of conformity assessments, according to the ETSI EN 319 403-1 standard, of Trust Service Providers and related trust services provided pursuant to the eIDAS Regulation.

8.3. Assessor's relationship to assessed entity

The assessment bodies that conduct audits on Entaksi have no relationship with Entaksi.

The internal auditor does not belong to the structure that deals with Entaksi activities.

8.4. Topics covered by assessment

Assessment concern in particular the correct operation of the Entaksi PKI such as:

- identification and authentication of the subjects requesting the certificates;
- management of related documentation;
- issue of the certificate;
- key management;
- revocation of certificates;
- updating the list of revoked certificates (CRL).

Physical, technical and operational security measures are also verified to verify the compliance with this Certificate Policy and Certification Practice Statement and other relevant documents.

8.5. Actions taken as a result of deficiency

The actions resulting from any issue found during the audits, (e.g., failure to meet the requirements defined in the applicable regulations, standards, procedures) depend on the nature and severity of the issue.

Entaksi commits to produce a remediation plan to address deviations from relevant standards and regulations.

8.6. Communication of results

The assessment body report is communicated to the Entaksi Management.

9. Other business and legal matters

9.1. Fees

Economic conditions may vary and can be negotiated on a personalized basis, contingent on the volumes requested and SLAs, so fees associated with the issuance, renewal, revocation, and suspension of certificates will be determined during the first contact with the applicant.

These fees, influenced by the quantities processed and market dynamics, are not publicly disclosed on Entaksi’s website.

9.1.1. Certificate access fees

Access to published certificates is freely available and unrestricted, with no associated fees.

9.1.2. Revocation or status information access fees

Access to revocation or status information is freely available and unrestricted, with no associated fees.

9.1.3. Fees for other services

Entaksi’s qualified services can be provided in modular combinations with other services, and the fees will adjust according to the parameters outlined in the Fees section.

9.1.4. Refund policy

The primary reference for Entaksi refund policy is the general Terms and conditions of the Qualified CA service ("Condizioni Generali del Servizio").
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.
Even though reimbursements are not foreseen can be performed a replacement of the physical device (smart card, token) in the case of proven inborn defects.

9.2. Financial responsibility

9.2.1. Insurance coverage

The maximum compensation for any damage resulting from non-compliance or negligence of Entaksi performing its services is fixed at € 2,500,000 per incident and € 2,500,000 per year.

9.2.2. Other assets

Not applicable.

9.2.3. Insurance or warranty coverage for end-entities

See Insurance coverage.

9.3. Confidentiality of business information

As stated in the terms and conditions and in the privacy policy, all the following information are considered confidential:

- data provided by subscribers and subjects, excluding information required for certificates or deemed non-confidential for other reasons;
- all the requests arriving from subscribers and subjects;
- communications exchanged among PKI participants;
- technical and operational information provided to the certificate holder (e.g., authentication credentials, private keys

activation data, etc.) generated by Entaksi or managed by Entaksi’s systems;

- private keys;
- system logs;
- contracts with external Registration Authoritys and all information exchanged with RAs and Registration Authority Officers.

9.3.1. Scope of confidential information

Entaksi, acting as data controller, processes personal data in full compliance with the provisions of General Data Protection Regulation (EU) 2016/679.

All data provided by the customers will be used solely for the purpose of executing the contract and fulfilling legal obligations.

9.3.2. Information not within the scope of confidential information

Information not deemed confidential includes:

- certificates and the information they contain;
- lists of suspended or revoked certificates (CRLs);
- information on the status of certificates issued online (e.g., via OCSP).

Any information required to be public by law, certification services technical standards (e.g., RFC 5280), or explicit request of the certificate holder is not considered confidential.

9.3.3. Responsibility to protect confidential information

The QTSP processes all confidential information in compliance with applicable data protection and privacy laws, ensuring it is physically and/or logically protected from unauthorized access (even if read-only) and the risk of loss due to disasters.

9.4. Privacy of personal information

Any information pertaining to Subjects or Subscribers obtained by the Certification Authority (CA) during its routine activities shall be treated as confidential and non-publishable. This includes personal data, which will be processed in accordance with General Data Protection Regulation (EU) 2016/679.

Information specifically intended for public use, such as the public key, information contained in the certificate (if requested by the Subject), in the certificate revocation, and suspension dates, may be exceptions to this confidentiality rule.

9.4.1. Privacy plan

As part of the processing of personal data related to the performance of the activities provided for qualified trust services, Entaksi acts as a Processor, by virtue of by specific legal delegation conferred by the Customer.

The complete set of provisions relating to the processing of personal data is reported in the document "Condizioni Generali del Servizio", chapter "Trattamento dei dati personali".

The complete set of provisions relating to the processing of personal data performed by Entaksi is reported at the following link: https://www.entaksi.eu/en/privacy.html.

9.4.2. Information treated as private

The complete set of provisions relating to the processing of personal data is reported in the document "Condizioni Generali del Servizio", chapter "Trattamento dei dati personali".

9.4.3. Information not deemed private

The complete set of provisions relating to the processing of personal data is reported in the document "Condizioni Generali del Servizio", chapter "Trattamento dei dati personali".

9.4.4. Responsibility to protect private information

The complete set of provisions relating to the processing of personal data is reported in the document "Condizioni Generali del Servizio", chapter "Trattamento dei dati personali".

9.4.5. Notice and consent to use private information

The complete set of provisions relating to the processing of personal data is reported in the document "Condizioni Generali del Servizio", chapter "Trattamento dei dati personali".

9.4.6. Disclosure pursuant to judicial or administrative process

The complete set of provisions relating to the processing of personal data is reported in the document "Condizioni Generali del Servizio", chapter "Trattamento dei dati personali".

9.4.7. Other information disclosure circumstances

The complete set of provisions relating to the processing of personal data is reported in the document "Condizioni Generali del Servizio", chapter "Trattamento dei dati personali".

9.5. Intellectual property rights

Entaksi retains ownership of all intellectual and industrial property rights, along with any other rights associated with its Trust Services (including trademarks, patents, designs, know-how, etc.), unless expressly indicated otherwise by third-party ownership. Utilization rights for the Services and their related technological solutions are exclusively reserved for Entaksi.

The subscriber is granted permission to use the service(s) within the specified limits and conditions outlined in this document.

9.6. Representations and warranties

9.6.1. CA representations and warranties

CA representation and warranties are defined in general terms and conditions of the qualified CA service ("Condizioni Generali del Servizio").

Entaksi, as a QTSP and CA, shall:

1. Act in accordance with the CP, CPS, and the operational manual.
2. Operate, ensuring that its reference clock is synchronized with Coordinated Universal Time within declared accuracy limits of one second.
3. Undergo internal and external audits to ensure compliance with relevant regulations and Entaksi’s internal policies and procedures.
4. Grant access to competent authorities and oversight bodies to its systems for the aforementioned audits, excluding cases of system maintenance, unavailability, planned technical interruptions, and loss of time synchronization.
5. Ensure the provision of trust services, excluding cases of system maintenance, unavailability, planned interruptions (with prior communication to the subscriber), and loss of time synchronization.
6. Inform the subscriber in case of service cessation. Entaksi will retain information and documentation related to terminated services according to its cessation plans.

9.6.2. RA representations and warranties

RA representation and warranties are defined in general terms and conditions document stated between Entaksi and the Local Registration Authoritys.

9.6.3. Subscriber representations and warranties

Subscriber representations and warranties are defined in general terms and conditions of the qualified CA service ("Condizioni Generali del Servizio").

The subscriber's obligations include all those stated in these conditions and in the current legislation regarding digital administration.

The subscriber:

- is obliged to use certified services in accordance with these conditions, the user manual, CP, and CPS;
- must provide Entaksi with all necessary information to enable the correct provision of Trust Services, provide proof of identity, and ensure the accuracy and periodic update of such information;
- must provide a physical address and an email address for contact purposes;
- must activate the services within the defined terms in the commercial offer;
- is required to exercise the utmost diligence in the use, storage, and protection of authentication credentials and any devices provided for service delivery, following the guidelines in the operational manual, CP, and CPS. In particular, the subscriber must take all suitable and necessary measures to prevent harm to third parties when requesting or using the services. Authentication credentials are strictly personal and cannot be transferred or used, directly or indirectly, by any means, by third parties. Otherwise, the legitimate recipient remains solely responsible for their correct use, as per legal effects.

In case the subscriber is different from the certificate holder (subject), the subscriber must:

- inform the certificate holder about the content of these general conditions and communicate any violations committed by the certificate holder to Entaksi;
- communicate to the Certificate holder the methods and limits related to its use.

9.6.4. Relying party representations and warranties

Before accepting a certificate, those relying on the information within, known as relying parties, must adhere to the following obligations:

- verify the completeness and authenticity of the certificate under consideration;
- ensure that the certificate in question is neither suspended, revoked, nor expired on the reference date of the check;
- give due consideration to specific information present in the certificate, including the holder's title or qualifications, the organization to which the holder belongs, and any limitations on use or value;
- confirm that the certificate in question meets the criteria for being a qualified certificate.

9.6.5. Representations and warranties of other participants

Any other participant is asked to promptly inform Entaksi if recognize inappropriate use of the certificates.

9.7. Disclaimers of warranties

In the case of supplying physical devices, Entaksi ensures compliance of the device with the specifications outlined in this document, as well as their suitability for the intended use in accordance with current laws.

All the applicable warranties are defined in the document "Condizioni Generali del Servizio".

9.8. Limitations of liability

Entaksi limits its liability to the issuance of the certificates, the management of the Certification Authority and the administration of the key pairs provided to subscribers.

9.9. Indemnities

Indemnities are defined in general terms and conditions of the qualified CA service ("Condizioni Generali del Servizio").

The subscriber, if:

- provides false, inaccurate, incomplete, or outdated information regarding identity and/or personal data, including the use of untruthful identity documents;
- improperly uses qualified trust services, violating current regulations, these general conditions, CP, and CPS, or in a manner that causes harm to others;
- engages in technical interventions or tampering personally or through unauthorized third parties not approved by Entaksi;

- fails to adopt the necessary measures to prevent the illegitimate use of qualified trust services by third parties;
- fails to immediately report to Entaksi the theft or attempted theft of authentication credentials to allow Entaksi to block the services;
- fails to observe, in general, the obligations imposed by this contract or the law;

will be deemed personally responsible for all the aforementioned violations and undertakes to indemnify and hold harmless Entaksi and its delegates from any liability, expense, prejudice, or direct or indirect damage arising from claims or actions by third parties against which Entaksi and/or its delegates have been called to respond for acts attributable to the subscriber.

9.10. Term and termination

Terms and termination are defined in general terms and conditions of the qualified CA service ("Condizioni Generali del Servizio").

9.10.1. Term

The contract will have the duration specified in general terms and conditions of the qualified CA service ("Condizioni Generali del Servizio").

The client will have the option, before the certificates expire, to request their renewal as outlined in this document.

9.10.2. Termination

Entaksi has the authority to terminate the contract, resulting in the revocation of certificates issued to the subscriber without any prior notice if the latter violates, in whole or in part, the provisions outlined in the contract.

In the event of contract termination, Entaksi will promptly revoke the provision of qualified services.

See section CA or RA termination.

9.10.3. Effect of termination and survival

In the event of the cessation of Entaksi’s activity as a qualified trust service provider, the latter commits to transmitting the necessary information for the continuation of the service to another equivalent QTSP. If this is not feasible, Entaksi undertakes to ensure the operation of the provided services in accordance with the cessation plan.

9.11. Individual notices and communications with participants

Refer to Contact person.

9.12. Amendments

Entaksi retains the right to modify its documents in response to modifications in regulatory standards, safety requirements, market conditions, or other relevant circumstances.

9.12.1. Procedure for amendment

Any amendment is registered in the "Revisions and releases" paragraph at the start of each document.

See also CPS approval procedures.

9.12.2. Notification mechanism and period

See CPS approval procedures.

9.12.3. Circumstances under which OID must be changed

Entaksi maintains the OID assigned to this document as long as changes to the document are minor, editorial or backwards-compatible.
Whenever changes materially affect the certificate policy semantics, the assurance level, or introduce non-backwards-compatible modifications to certificate usage or relying-party obligations, Entaksi will assign a new OID under its private OID

arc and update all affected certificates and documentation accordingly.

9.13. Dispute resolution provisions

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.

9.14. Governing law

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.

9.15. Compliance with applicable law

The main applicable framework is:

EU Regulation No. 910/2014 of the European Parliament and of the Council - eIDAS

> 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

EU Regulation No. 1183/2024 – eIDAS 2

> Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

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).

9.16. Miscellaneous provisions

Not applicable.

9.16.1. Entire agreement

Not applicable.

9.16.2. Assignment

Not applicable.

9.16.3. Severability

Not applicable.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5. Force Majeure

Are considered "force majeure", unforeseen events, and catastrophic events (including, by way of example and not exhaustively: wars, fires, floods, explosions, earthquakes, blocks on internet and electrical networks, etc.).

9.17. 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.

9.17.1. User interface accessibility

Entaksi delivers its Qualified Trust Services through a web-based interface (Entaksi’s Console).
Entaksi develops the user interface using Angular, an open-source, TypeScript-based framework and platform developed by Google. While accessibility is not automatic, Angular provides a structured, component-based architecture that supports the correct implementation of accessibility features; in particular, it facilitates the use of semantic HTML, consistent form-handling patterns, keyboard event management, and reusable interface components, providing a stable technical basis for meeting the ETSI EN 301 549 clause 9 (*WCAG 2.1 Level AA*) requirements.
The user interface currently supports:

- text alternatives for non-text elements;
- structured and semantic HTML with programmatic headings and landmarks;
- keyboard operability for core functions;
- programmatically associated labels for buttons and input fields;
- compatibility with assistive technologies such as screen readers;
- responsive layouts supporting zoom, viewport resizing, and text scaling.

Periodic accessibility reviews are carried out as part of Entaksi’s quality and maintenance processes. These reviews include both automated evaluations—using recognized accessibility testing tools—and manual checks such as keyboard navigation testing, screen-reader verification, and visual inspection of contrast and layout behaviour. The objective of these activities is to identify potential accessibility barriers and ensure continuing alignment with the requirements of ETSI EN 301 549.

Entaksi monitors and evaluates all accessibility-related requests, feedback, and defect reports received from users, customers, or internal teams. Once the issue has been verified, it is addressed in the maintenance improvement cycle to further enhance the accessibility features.

9.17.2. Documentation accessibility

All service documentation is provided in accessible electronic PDF format. These PDFs are produced with accessibility considerations in accordance with the requirements of ETSI EN 301 549 clause 10 for non-web documents. In particular, documentation includes:

- alternative text for images and non-text elements;
- a tagged and logical reading order;
- semantic and properly structured headings and lists;
- accessible tables with correctly defined headers;
- visual elements with adequate colour contrast.

All these measures support the readability and usability of the documentation for persons with disabilities and users with accessibility needs.

Upon request documentation can be provided in the HTML alternative accessible format, where reasonably practicable.

9.17.3. Support for accessibility

Entaksi’s Help Desk, accessible at helpdesk@entaksi.eu, provides information on the accessibility and compatibility features of the service portal and its documentation, and ensures effective communication with persons with disabilities and users with accessibility needs.

Support services can be accessed through the channels described in the service’s Terms and Conditions, including:

- accessible email communication channels;
- telephone support;
- alternative communication methods upon request.

Any documentation or information supplied through the support service is provided in accessible formats consistent with Entaksi’s documentation accessibility practices.

9.18. Other provisions

Please refer to the general terms and conditions of the qualified CA service ("Condizioni Generali del Servizio") for any other detail about the guarantees and responsibilities incumbent on each party.