ENTAKSI SOLUTIONS

CERTIFIED MANAGEMENT SYSTEM
ISO 9001| ISO 20000-1 | ISO 22301
ISO 27001| ISO 27017| ISO 27018 | ISO 27035
CERTIFIED PRESERVATION SYSTEM
ETSI 319 401| ETSI 119 511
FOR 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	1.0.0
Creation Date	26/04/2023
Last Revision	10/05/2023
Author	Alessia Soccio
Status	Released
Classification	Internal

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

Revisions and releases

Date	Version	Name	Mansion	Action	Release
26/04/2023	0.0.1	Alessia Soccio	RSIG	Draft creation.	Public
10/05/2023	1.0.0	Alessia Soccio	RSIG	Review and release.	Public

Document approval

Date	Employee	Role	Signature
10/05/2023	Alessandro Geri	Amministratore Unico	*Digitally signed*

1. Introduction

This document is the Certificate Policy and Certification Practice Statement of qualified certification authority operated by Entaksi Solutions SpA (hereinafter "Entaksi").

Entaksi provides trust services such the Time-Stamp Authority Service and Long Term Preservation Service for Electronic Signature and Seals to its customers under contractual relationship.

This document complies with the 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 (hereinafter "eIDAS Regulation").

The service provided according to eIDAS Regulation is an EU qualified trust service.

Entaksi is registered as a trust service provider by DCCAE – Department of Communications, Climate Action and Environment.

1.1. Purpose and scope of the document

This document 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.

It also describes the roles, responsibilities and relationships of Participants within the Entaksi PKI.

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

1.2. Document name and identification

This document is identified by the following OID:

OID	Description
1.3.6.1.4.1.57823.1.9	MAN eIDAS 20230101 Certificate Policy and Certification Practice Statement 1.0.0

1.3. PKI participants

The Public Key Infrastructure participants within the framework of this policy and practice statement are:

- Entaksi Public Key Infrastructure (PKI), Certification Authority and Registration Authority.
- Subscribers to the Entaksi Time-stamp Service.
- Relying parties.
- Other participants.

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

1.3.1. Certification authorities

This policy applies to the following two Certification Authorities managed by Entaksi.

- The "Entaksi QTSP Root CA G1", that is an internal root certification authority that act as signer of other sub CAs.
- The "Entaksi Qualified Time-stamps CA G1", that is the certification authority used for signing TSU certificates of the Entaksi TSA service.

The "Entaksi QTSP Root CA G1" certification authority is identified by the following attributes:

- `CN=Entaksi QTSP Root CA G1`
- `C=IT`
- `O=Entaksi Solutions SpA`
- `organizationIdentifier: VATIT-01621900479`
- `certificatePolicies:`

    - anyPolicy (2.5.29.32.0)

The "Entaksi Qualified Time-stamps CA G1", that is the Certification Authorities that issues certificate for the Time-stamp Unit used by the Qualified Time Stamp Service.

- 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 Enhanced Normalized Certificate Policy NCP+ (0.4.0.2042.1.2)
    - Entaksi Certificate Policy and Certification Practice Statement (1.3.6.1.4.1.57823.1.9)

1.3.2. Registration authorities

Under this policy and practice statement certificates are not issued to external subscribers, therefore there is no public registration authority operating under this policy except for the internal registration authority that issues Time-stamp Unit certificates.

1.3.3. Subscribers

Not applicable to this policy since the certification authority only provides certificate for the Entaksi TSA Time-stamp Unit.

1.3.4. Relying parties

Relying Parties are individuals or legal entities that rely on digital signatures, including Time-stamps, generated with a private key whose integrity and authenticity is guaranteed by public key certificate signed by the Entaksi Certification Authority.

In the context of the Entaksi TSA, a Relying party may or may not be a Subscriber. Subscribers are responsible for the activities of their associated users and Relying parties and are expected to inform them about the correct use of Time-stamps.

1.3.5. Other participants

There are no other participants to the PKI.

1.4. Certificate usage

The CA issues certificates for the Entaksi TSA Time-stamp Unit (TSU). Certificates types issued by the CA contains the QcStatements field (OID 1.3.6.1.5.5.7.1.3) specifying `esi4-qtstStatement-1` as specified in clause 9.1 of ETSI EN 319 422 V1.1.1 (2016-03).

1.4.1. Appropriate certificate uses

Certificates issued for the TSU shall be used only for signing Time-stamps using the corresponding private key.

1.4.2. Prohibited certificate uses

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

1.5. Policy administration

1.5.1. Organization administering the document

This policy is issued under the responsibility of Entaksi Management.

1.5.2. Contact person

The TSP can be contacted at the following addresses:

Entaksi Solutions SpA - Irish Branch
Suite 4.01 - Ormond Building 31 36 Ormond Quai Upper - D07F6DC Dublino 7 - Ireland

Entaksi Solutions SpA - Italian Headquarter
via la Piana 76, fraz. Pontepetri, 51028 San Marcello Piteglio (PT)

Entaksi Solutions SpA - Business office
Re.work, Via G. Porzio, 4 - Centro Direzionale Isola E2 - 80143 Napoli

Info: info@entaksi.eu
Help Desk: assistenza@entaksi.eu
Data Protection: privacy@entaksi.eu
DPO: dpo@entaksi.eu

Phone: +39 0573 171 6484
Website: http://www.entaksi.eu

1.5.3. Person determining CPS suitability for the policy

This Certificate Policy and Certification Practice Statement has been approved by Entaksi management following a review by internal and external auditors.

1.5.4. CPS approval procedures

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.

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.

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

1.6. Definitions and acronyms

1.6.1. Definitions

- **Certification**: The process of creating a digital certificate for an entity and binding that entity's identity to the digital certificate.
- **Certification Authority**: An entity trusted by one or more entities to create, assign o revoke digital certificates.
- **Certificate Policy and Certification Practice Statement**: A publicly available document that details the Entaksi Public Key Infrastructure and describes the practices employed in issuing digital certificates.
- **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**: A list of digital certificates signed by the issuing certification authority that have been revoked.
- **Cryptographic module**: A secure software, device or utility that generates key pairs, stores cryptographic information and performs cryptographic functions.
- **Digital signature**: A set of data appended to a data unit that allows a recipient of the data to prove the source and integrity of the data unit.
- **Digital transmission**: The transmission of information in an electronic format.

1.6.2. Acronyms

- **CP/CPS**: Certificate Policy / Certification Practice Statement.
- **CRL**: Certificate Revocation List.
- **ETSI**: European Telecommunications Standards Institute.
- **HSM**: Hardware Security Module.
- **PKI**: Public Key Infrastructure.
- **TSP**: Trust Service Provider.
- **ITU**: International Telecommunication Union
- **ITU-T**: ITU Telecommunication Standardization Sector
- **IETF**: Internet Engineering Task Force

1.7. References

The following documents contain provisions which are relevant to the Entaksi TSA:

- **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.
- **ETSI EN 319 401 V2.3.1 (2021-05)**, "Electronic Signatures and Infrastructure; General Policy Requirements for Trust Service Providers".
- **ETSI EN 319 411-1 V1.3.1 (2021-05)**, "Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
- **ETSI EN 319 411-2 V2.3.1 (2021-05)**, "Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".
- **ETSI EN 319 412-3 V1.2.1 (2020-07)**, "Electronic Signatures and Infrastructure; Certificate Profiles: Part 3: Certificate profile for certificates issued to legal persons".
- **ETSI EN 319 412-5 V2.3.1 (2020-04)**, "Electronic Signatures and Infrastructures; Certificate Profiles; Part 5: QCStatements".
- **ETSI TS 119 312 V1.4.1 (2021-08)**, "Electronic Signatures and Infrastructures; Cryptographic Suites".
- "MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement"
- **RFC 3161**, "Internet X.509 Public Key Infrastructure Time-stamp Protocol".
- **RFC 5280**, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

2. Publication and repository responsibilities

2.1. Repositories

Published certificates, the Certificate Revocation List (CRL) and the OCSP service are available on line, 24 hours a day.

2.2. Publication of certification information

Entaksi publishes all the TSP documents in PDF format at the following link: https://www.entaksi.eu/en/eidas.html

The PKI Disclosure statement (MAN eIDAS 20230426 PKI Disclosure Statement) is available at https://r.entaksi.net/oids/1.3.6.1.4.1.57823.1.10.

This Certificate Policy and Certification Practice Statement document (MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement) is available at https://r.entaksi.net/oids/1.3.6.1.4.1.57823.1.9.

The Certification Authority "Entaksi QTSP Root CA G1" is available at https://s.entaksi.net/pki/Entaksi QTSP Root CA G1.pem.

The Certification Authority "Entaksi Qualified Time-stamps CA G1" that signs the Time Stamp Unit certificates is available at https://s.entaksi.net/pki/Entaksi Qualified Time-stamps CA G1.pem.

2.3. Time or frequency of publication

Frequency of publication of the Certificate Policy and Certification Practice Statement varies to reflect any changes that have occurred.

CRL update frequency is specified in chapter CRL issuance frequency (if applicable).

2.4. Access controls on repositories

Information on issued certificates, CRL, Certificate Policy and Certification Practice Statements and the PKI Disclosure Statement are publicly available and accessible without restrictions.

Entaksi is the only entity that has write access to repositories.

3. Identification and authentication

3.1. Naming

Naming in certificate issued by the Certification Authorities under this policy follows the ITU-T X .509v3 specifications, the IETF RFC 5280 and the appropriate part of ETSI EN 319 412-2 V2.2.1 (2020-07) and ETSI EN 319 412-3 V1.2.1 (2020-07).

3.1.1. Types of names

Certificate holder is identified by the Distinguished Name in compliance with X.550 standard.

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

- ETSI EN 319 411-1 V1.3.1 (2021-05): Electronic Signatures and Infrastructures; Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 V2.3.1 (2021-05): Electronic Signatures and Infrastructures; 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 V1.4.4 (2021-05): Electronic Signatures and Infrastructures; Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-3 V1.2.1 (2020-07): Electronic Signatures and Infrastructures; Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-5 V2.3.1 (2020-04): Electronic Signatures and Infrastructures; Certificate Profiles; Part 5: QCStatements

3.1.2. Need for names to be meaningful

Certificate holders require a distinguished name that is 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)
- `organizationUnitName` (OID 2.5.4.11)
- `localityName` (OID 2.5.4.7)
- `stateOrProvinceName` (OID 2.5.4.8)
- `organizationIdentifier` (OID 2.5.4.97)

3.1.3. Anonymity or pseudonymity of subscribers

Not applicable.

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

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.

3.1.6. Recognition, authentication, and role of trademarks

Entaksi is not obliged to seek evidence of trademark usage by any organization or individual.

3.2. Initial identity validation

Identity validation is in compliance with this Certificate Policy as far as the only validated identity is the Time-stamp Unit managed by Entaksi TSA.

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 possession of the private key of the certificate applicant.

3.2.2. Authentication of organization identity

Not applicable.

3.2.3. Authentication of individual identity

Not applicable.

3.2.4. Non-verified subscriber information

Not applicable.

3.2.5. Validation of authority

Not applicable.

3.2.6. Criteria for interoperation

Not applicable.

3.3. Identification and authentication for re-key requests

Not applicable.

3.3.1. Identification and authentication for routine re-key

Not applicable.

3.3.2. Identification and authentication for re-key after revocation

Not applicable.

3.4. Identification and authentication for revocation request

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

4. Certificate life-cycle operational requirements

4.1. Certificate Application

4.1.1. Who can submit a certificate application

Certificate application can only be submitted by the Entaksi TSA for the Time-stamp Unit that signs Time-stamps.

4.2. Certificate issuance

4.2.1. Certification Authority actions during certificate issuance

The "Entaksi Qualified Time-stamps CA G1" certification authority has been self generated, and it is signed by the "Entaksi QTSP Root CA G1", which is also 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

Not applicable.

4.3. Certificate acceptance

Not applicable.

4.3.1. Conduct constituting certificate acceptance

Not applicable.

4.3.2. Publication of the certificate by the CA

Not applicable.

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

Not applicable.

4.4. Key pair and certificate usage

A certificate holder may only use the private key and corresponding public key in the digital certificate for their lawful and intended use.

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 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

Not applicable.

4.5.1. Circumstance for certificate renewal

Not applicable.

4.5.2. Who may request renewal

Not applicable.

4.5.3. Processing certificate renewal requests

Not applicable.

4.5.4. Notification of new certificate issuance to subscriber

Not applicable.

4.5.5. Conduct constituting acceptance of a renewal certificate

Not applicable.

4.5.6. Publication of the renewal certificate by the CA

Not applicable.

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

Not applicable.

4.6. Certificate re-key

Certificate re-key consists in the duplication of all the identifying information from an old valid certificate in a new certificate with different public key and validity period.

4.6.1. Circumstance for certificate re-key

Digital certificates may be re-keyed upon request.

4.6.2. Who may request certification of a new public key

Certificate holders may request digital certificate re-keys.

4.6.3. Processing certificate re-keying requests

Digital certificate re-key requests are processed in the same manner as requests for new digital certificates and in accordance with provisions of this Certificate Policy and Practice Statement.

4.6.4. Notification of new certificate issuance to subscriber

Not applicable.

4.6.5. Conduct constituting acceptance of a re-keyed certificate

Downloading, installing or otherwise taking delivery of a re-keyed digital certificate constitutes acceptance of the digital certificate re-key.

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

Not applicable.

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

Not applicable.

4.7. Certificate modification

Certificate modification are not allowed.

4.7.1. Circumstance for certificate modification

Not applicable.

4.7.2. Who may request certificate modification

Not applicable.

4.7.3. Processing certificate modification requests

Not applicable.

4.7.4. Notification of new certificate issuance to subscriber

Not applicable.

4.7.5. Conduct constituting acceptance of modified certificate

Not applicable.

4.7.6. Publication of the modified certificate by the CA

Not applicable.

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

Not applicable.

4.8. Certificate revocation and suspension

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.

4.8.2. Who can request revocation

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 "Entaksi Qualified Time-stamps CA G1" applies the certification revocation upon receipt of a valid revocation request.

4.8.4. Revocation request grace period

Not applicable.

4.8.5. Time within which CA must process the revocation request

Not applicable.

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.

4.8.7. CRL issuance frequency (if applicable)

Certificate Revocation List is updated every 24 hours.

4.8.8. Maximum latency for CRLs (if applicable)

Not applicable.

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

Not applicable.

4.8.12. Special requirements re key compromise

Not applicable.

4.8.13. Circumstances for suspension

Not applicable.

4.8.14. Who can request suspension

Not applicable.

4.8.15. Procedure for suspension request

Not applicable.

4.8.16. Limits on suspension period

Not applicable.

4.9. Certificate status services

4.9.1. Operational characteristics

The status of digital certificates issued by the "Entaksi Qualified Time-stamps CA G1" is published in a Certificate Revocation List or is made available via Online Certificate Status Protocol.

CRL can be found at https://va.entaksi.eu/crls/Entaksi_Qualified_TSA_CA_G1.crl.

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

4.9.2. Service availability

Certificate Revocation List is available for download any time.

The Online Certificate Status Protocol responder is available 24 hours a day.

4.9.3. Optional features

Void.

4.10. End of subscription

A subscriber may end a subscription with the Certification Authority service allowing the certificate to expire or revoking the certificate.

4.11. Key escrow and recovery

Key escrow is not available.

4.11.1. Key escrow and recovery policy and practices

Not applicable.

4.11.2. Session key encapsulation and recovery policy and practices

Not applicable.

5. Facility, management, and operational controls

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 persons.

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

Secure area access is allowed only to authorized persons. Every entry and exit is logged.

5.1.1. Site location and construction

Two secure areas are located in two different datacenters for redundancy and business continuity. Datacenter are built with state of the art security measures.

5.1.2. Physical access

Every entry and exit is logged.

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

Identification and authentication of trusted roles use digital keys and cryptographic tokens assigned to individuals in role.

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

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 or them are needed in order to authorize the operation.

5.3. Personnel controls

All personnel involved in trusted role is checked for conflict of interests and other malicious interferences.

5.3.1. Qualifications, experience, and clearance requirements

All personnel involved in trusted role is qualified and approved for the role.

5.3.2. Background check procedures

Entaksi maintains records of personnel activities.

5.3.3. Training requirements

All personnel involved in trusted role is subject to adequate training.

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. A full skill assessment is performed annually.

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

Appropriate disciplinary actions are taken for unauthorised actions.

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 PKI uses 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 a specific preservation object identifier;
- 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.

5.4.2. Frequency of processing log

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

Log retention is set to 6 months. The retention period may be shortened or lengthened according to contract terms, law and regulations.

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.

5.4.5. Audit log backup procedures

Logs are sent for digital preservation daily.

5.4.6. Audit collection system (internal vs. external)

The security audit process of each certification authority runs independently of the certification authority software.

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

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

Vulnerability assessments are performed internally every three months and externally every year.

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.
- Evidence of Digital Certificate acceptance and signed (electronically or otherwise) Certificate Holder Agreements.
- Revocation 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 v1.1.1 (2019-06) specifications.

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

Incident management procedures are defined in the business continuity plan.

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

Incident that involve a private key compromise is addressed according to a specific procedure described in the business continuity plan.

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 two redundant site is available.

5.8. 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 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 TSA 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 notice of the termination of the service is published on the company's website "www.entaksi.eu".
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.

6.1.1. Private key delivery to subscriber

Private key for subscriber certificates are always generated by 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.500 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/.

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 uses 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)

6.2. Private Key Protection and Cryptographic Module Engineering Controls

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

6.2.1. Cryptographic module standards and controls

Cryptographic modules used by Entaksi are Common Criteria certified and meet the requirements of EAL 4 augmented with AVA_VAN.5. A such the devices are conformant to:

- 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

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 security module 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

Private key escrow is not allowed.

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.

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 cryptographic module using the encrypted backup and provided that all cryptographic modules use the same Master Backup Key.

6.2.7. Private key storage on cryptographic module

Private keys stored in a cryptographic module 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 security module where they reside.

6.2.11. Cryptographic Module 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

Void.

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, organisation, or device.

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

6.4. Activation data

Private keys activation requires the activation key that was used in initialized the private key.

6.4.1. Activation data generation and installation

Activation data is generated with cryptographic module application interface.

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

Void.

6.5. Computer security controls

Entaksi implements a set of security controls as part of its implementation of the ISO/IEC 27001:2013 specification.

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 UNI 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 V1.3.1 (2021-05).

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

Void.

7. Certificate, CRL, and OCPS profiles

7.1. Certificate profile

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 contains 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)
- `QcRetentionPeriod` (OID 0.4.0.1862.1.3) with value set to 30 years
- `QcSSCD` (0.4.0.1862.1.4)
- `QcPDS` (OID 0.4.0.1862.1.5) with URL to the Entaksi PKI Disclosure Statement as value.

7.1.3. Algorithm object identifiers

Certificates are signed with the following algorithm:

- `sha256WithRSAEncryption` (OID 1.2.840.113549.1.1.11)

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 2 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 contains the extension that indicates the reason for certificate revocation.

CRLs are available at:

- https://va.entaksi.eu/crls/Entaksi_QTSP_Root_CA_G1.crl.
- https://va.entaksi.eu/crls/Entaksi_Qualified_Time-stamps_CA_G1.crl.

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.

7.3.1. Version number(s)

OCSP version number is 1.

7.3.2. OCSP extensions

Not applicable.

8. Compliance audit and other assessments

The applicable legal system is declared in References.

The configuration of the Entaksi PKI is regularly checked by the management to avoid any change which violate Entaksi security policies.

Entaksi PKI is checked by an accredited certification body.

Audit working papers and inspection documents are classified as confidential.
The conformity certificates and their updates are published on the Entaksi website in accordance with the assessment results.

8.1. Frequency or circumstances of assessment

Assessment are conducted yearly.

8.2. Identity/qualifications of assessor

The conformity checks (audits) on the Entaksi PKI 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 V2.3.1 (2020-06) 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 the Entaksi PKI have no relationship with Entaksi.

The internal auditor does not belong to the structure that deals with Entaksi PKI 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 of 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 in order 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

Not applicable.

9.1. Fees

Not applicable.

9.1.1. Certificate issuance or renewal fees

Not applicable.

9.1.2. Certificate access fees

Not applicable.

9.1.3. Revocation or status information access fees

Not applicable.

9.1.4. Fees for other services

Not applicable.

9.1.5. Refund policy

Not applicable.

9.2. Financial responsibility

Not applicable.

9.2.1. Insurance coverage

Not applicable.

9.2.2. Other assets

Not applicable.

9.2.3. Insurance or warranty coverage for end-entities

Not applicable.

9.3. Confidentiality of business information

Not applicable.

9.3.1. Scope of confidential information

Not applicable.

9.3.2. Information not within the scope of confidential information

Not applicable.

9.3.3. Responsibility to protect confidential information

Not applicable.

9.4. Privacy of personal information

Not applicable.

9.4.1. Privacy plan

Not applicable.

9.4.2. Information treated as private

Not applicable.

9.4.3. Information not deemed private

Not applicable.

9.4.4. Responsibility to protect private information

Not applicable.

9.4.5. Notice and consent to use private information

Not applicable.

9.4.6. Disclosure pursuant to judicial or administrative process

Not applicable.

9.4.7. Other information disclosure circumstances

Not applicable.

9.5. Intellectual property rights

Not applicable.

9.6. Representations and warranties

Not applicable.

9.6.1. CA representations and warranties

Not applicable.

9.6.2. RA representations and warranties

Not applicable.

9.6.3. Subscriber representations and warranties

Not applicable.

9.6.4. Relying party representations and warranties

Not applicable.

9.6.5. Representations and warranties of other participants

Not applicable.

9.7. Disclaimers of warranties

Not applicable.

9.8. Limitations of liability

Not applicable.

9.9. Indemnities

Not applicable.

9.10. Term and termination

Not applicable.

9.10.1. Term

Not applicable.

9.10.2. Termination

See section CA or RA termination.

9.10.3. Effect of termination and survival

Not applicable.

9.11. Individual notices and communications with participants

Not applicable.

9.12. Amendments

Not applicable.

9.12.1. Procedure for amendment

Not applicable.

9.12.2. Notification mechanism and period

Not applicable.

9.12.3. Circumstances under which OID must be changed

Not applicable.

9.13. Dispute resolution provisions

Not applicable.

9.14. Governing law

Not applicable.

9.15. Compliance with applicable law

Not applicable.

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

Not applicable.

9.17. Other provisions

Not applicable.