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 TSA Policy and Practice Statement EN

Entaksi Solutions SpA

Table of contents

Document information

Project	Integrated Management System
Type	Manual
Document ID	MAN eIDAS 20230426 TSA Policy and 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

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") includes requirements for Trust Service Providers (TSP) providing services to the public, including those issuing electronic Time-stamps.

Time-stamps use electronic signatures techniques for incorporating the time from an accurate source in order to build a proof of existence of the data at a certain time.

Electronic signatures may be used independently or together with Time-stamps to increase the trustworthiness of electronic records and transactions.

This document is the Time-Stamp Authority Policy and Practice Statement of the Trust Service Provider (TSP) Entaksi Solutions SpA Irish Branch (in the following "Entaksi"), a branch of the Italian company with VAT-ID IT01621900479 operating in Ireland with National Trade Register number 909882.

This Policy and Practice Statement defines the operational and management practice of the Entaksi TSA so that subscribers and relying parties can evaluate their confidence in the operation of Time-stamping service.

The Entaksi TSA aims to provide time-stamping services in compliance with the eIDAS Regulation as well as with other applicable laws and regulations in EU member states.

This document does not substitute or replace the Terms and Conditions of the TSA service, of which is an attachment.

1.1. Document identification

This document is identified by the following OID:

OID	Description
1.3.6.1.4.1.57823.1.11	MAN eIDAS 20230426 TSA Policy and Practice Statement EN 1.0.0

1.2. Document maintenance

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

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

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

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

1.3. Approval and publication

This document and all the internal policies and practices mentioned in it have been approved by Entaksi's Management, published and communicated to employees and, as regards those classified as "public", published on the company website.

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.

2. 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 EN 319 421 V1.2.1 (2023-05)**, "Electronic Signatures and Infrastructures; Policy and Security Requirements for Trust Service Providers issuing Time-stamps".
- **ETSI EN 319 422 V1.1.1 (2016-03)**, "Electronic Signatures and Infrastructures; Time-stamping Protocol and Time-stamp Token Profiles".
- **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".

2.1. Certifications

Entaksi has obtained the following certifications:

UNI ISO 9001:2015

Quality Management Systems - Requirements.

ISO/IEC 20000-1:2018

Information technologies - Provision of IT services.

ISO/IEC 27001:2013

Information technology - Security techniques - Management systems of information security - Requirements.

ISO/IEC 27017:2015

Information Technology - Security Techniques - Code of Conduct for i Information security controls based on ISO/IEC 27002 for cloud services.

ISO/IEC 27018:2019

Information technology - Security techniques - Code of conduct for protection of personally identifiable information (PII) in the public clouds they serve from PII processors.

ISO/IEC 27035:2016

Information technology - Security techniques - Incident management of information security.

ISO/IEC 22301:2019

Information technology - Security and resilience - Management systems business continuity.

UNI ISO 37001:2016

Anti-Bribery Management Systems - Requirements and Guidance to use.

Sistema di conservazione dei documenti digitali

Information technology - Digital preservation - art. 24 EU Regulation no 910/2014 on digital identity.

eIDAS

Regulation (EU) no. 910/2014 of the European Parliament and of the Council, of 23 July 2014, in 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 Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

ETSI TS 119 511 v1.1.1 (2019-06)

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.

UNI ISO 9001:2015

Quality management systems - Requirements.

ISO/IEC 20000-1:2018

Information technology - Service management - Part 1: Service management system requirements.

ISO/IEC 27001:2013

Information technology — Security techniques — 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.

Long-term Preservation Service - art. 24 EU Regulation n° 910/2014 (eIDAS):

- **ETSI EN 319 401 V2.3.1 (2021-05)**:: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- **ETSI TS 119 511 v1.1.1 (2019-06)**:: 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.

3. Definition and abbreviations

3.1. Definitions

Coordinated Universal Time (UTC)

The time scale, based on the second, as defined by the International Telecommunication Radio Committee (ITU-R) TF.460-5.

Electronic Time-stamp

Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

Qualified Electronic Time-stamp

An electronic time-stamp issued by a Qualified Trust Service Provider whose Time-stamp Unit Public Key Certificate was issued by a Certification Authority operating under a ETSI EN 319 411-2 V2.3.1 (2021-05) certificate policy.

Relying party

An entity (individual or organization) which relies on a Time-stamp token provided by Entaksi TSA.

Subscriber

An entity (individual or organization) which has an agreement with Entaksi and requires the services provided by Entaksi TSA.

Time Stamp Authority

A trusted authority which issues Time-stamps.

Time Stamping Unit

A set of hardware and software which is managed as a unit and has a single private signing key active at time for providing Time-stamps.

Trust Service Provider

An entity which provides one or more electronic service that enhances or establishes trust and confidence in electronic transactions.

UTC(k)

A time scale realised by a laboratory "k" as defined in Bureau International des Poids et Mesures (BIBPM) Circular T.

3.2. Abbreviations

CA

Certification Authority.

CP/CPS

Certificate Policy / Certification Practice Statement.

CRL

Certificate Revocation List.

ETSI

European Telecommunications Standards Institute.

HSM

Hardware Security Module.

PKI

Public Key Infrastructure.

QTSA

Qualified Time-Stamping Authority

TLS

Transport Layer Security

TSA

Time-Stamping Authority

TSP

Trust Service Provider.

TSU

Time Stamping Unit.

4. General Concepts

4.1. General policy requirements concepts

This document follows the requirements of the European standards ETSI EN 319 421 V1.2.1 (2023-05) and ETSI EN 319 422 V1.1.1 (2016-03), and references ETSI EN 319 401 V2.3.1 (2021-05) "General Policy Requirements for Trust Service Providers" for generic policy requirements common to all classes of TSP services, as stated in the chapter "References".

Structure and contents of this Entaksi TSA Policy and Practice Statement are laid out in accordance to ETSI EN 319 421 V1.2.1 (2023-05).

This policy is administered and approved by the Entaksi management, as stated in the chapter "Approval and publication", and should be read in conjunction with the Entaksi Certificate Policy and Practice Statement ("MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement").

4.2. Time-stamping services

Entaksi TSA services include the following components:

- **Time-stamping provision**, the component that issues Time-stamps.
- **Time-stamping management**, the component that monitors and controls the time-stamping operation, including time synchronization with the reference UTC time source.

Entaksi TSA services adheres to the international standards in section References of this document in order to increase the trustworthiness of the time-stamping services.

4.3. Time-stamping authority

The time-stamping authority is a TSP trusted by subscribers and relying parties to issue secure Time-stamps as defined in RFC 3161. Entaksi takes overall responsibility for the provision of time-stamping services identified in section Time-stamping services of this document.

Entaksi operates the Entaksi TSA as part of its own PKI.

Entaksi TSA has responsibility for the operation of the Time-stamping Unit (TSU) which creates and signs Time-stamps on behalf of the TSA.

4.3.1. Conformance

The policy identifiers in section Identification of this document are referenced in all Time-stamps issued by the Entaksi TSA to indicate the conformance with this policy.

Entaksi is subject to periodic independent internal and external audits to demonstrate that Entaksi TSA meets its obligations defined in section TSA obligations and has implemented appropriate controls according to section TSA Management and operation.

The Entaksi TSA is audited annually by a Conformity Assessment Body for qualified aspects and the assessment report is submitted to the relevant national Supervisory body.

An updated list of Entaksi accreditations is available at https://www.entaksi.eu/en/certifications.html.

Where the Conformity Assessment Body and/or Supervisory Body requires Entaksi to remedy any failure to fulfil requirements, Entaksi will act accordingly and in a timely fashion. The Supervisory Body will be informed of any change in the provision of the relevant Entaksi TSA.

4.4. Subscribers and relying parties

A subscriber is the legal or natural person bound by agreement with a service provider.

Customers can sign the Terms and Conditions of the TSA service (or "Condizioni generali del servizio") with Entaksi, in order to access the TSA service.

Relying parties are individuals or entities that rely on a Time-stamp generated by the Entaksi TSA.

A relying party may or may not be a subscriber.

If a subscriber is an organization, the organization is responsible for the activities of their associated users and relying parties

and is expected to inform them about the correct use of the Time-stamps and the condition of the TSA Policy.

Entaksi doesn't involve any external party to perform critical tasks on the TSA service. However, other third parts may be involved in the process, such as legal control bodies, authorities, and auditors.
Entaksi always requires non-disclosure agreements to any non-contractual access to the system, such as for audits, and applies anonymization and minimization of personal data wherever possible.

4.5. Time-stamp policy and TSA practice statement

This document specifies a Time-stamp policy and the practice statement to meet general requirements for trusted Time-stamping services as defined by the standards in section References.

Other internal documents define how Entaksi meets the technical, organisational and procedural requirements identified in this policy. These documents may be provided only under a non-disclosure agreement in strictly controlled conditions. All Entaksi policies and practices are under the control of the Entaksi Management.

This policy and practice statement (MAN eIDAS 20230426 TSA Policy and Practice Statement) as well as the Certificate Policy and Practice Statement (MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement) are public and are available at https://www.entaksi.eu.

5. Time-stamp policy

5.1. General

As a TSP, Entaksi defines a set of processes for the trustworthy creation of Time-stamps according to ETSI EN 319 421 V1.2.1 (2023-05).

The private keys and the TSU meet the technical specifications of ETSI EN 319 422 V1.1.1 (2016-03) and RFC 3161.

Time-stamps are signed using private keys that are reserved specifically for this purpose.

Each Time-stamp contains identifiers to the applicable policies that consist in the following OIDs:

- `0.4.0.2023.1.1`: The ETSI best practices Time-stamp policy defined in ETSI EN 319 421 V1.2.1 (2023-05).
- `1.3.6.1.4.1.57823.1.11`: The Entaksi TSA Policy and Practice Statement defined in the present document "MAN eIDAS 20230426 TSA Policy and Practice Statement".

Time-stamps are issued with time accurate to 1 second or better of UTC, as described in Accuracy of the time.

Time-stamps are requested by means of the Hypertext Transfer Protocol (HTTP) as described by RFC 3161.

5.2. Identification

This Entaksi TSA Policy is identified by the following OID: `1.3.6.1.4.1.57823.1.11`.

Such OID is referenced in every issued Time-stamp and this Entaksi TSA Policy is available for both subscriber and relying parties.

This Entaksi TSA Policy is based on the ETSI best practices Time-stamp policy defined in ETSI EN 319 421 V1.2.1 (2023-05) (OID `0.4.0.2023.1.1`).

5.3. User community and applicability

The user community for Entaksi TSA includes subscribers and their relying parties.

The Time-stamp service is not provided for public access, and it is available only to subscribers.

Entaksi does not impose restrictions on the applicability of Time-stamps issued by the Entaksi TSA.

Time-stamps issued by the Entaksi TSA may be applied to any application requiring proof that a data object existed before a certain time.

6. Policies and practices

6.1. Risk assessment

Entaksi performs periodic risk assessments according to ETSI EN 319 401 V2.3.1 (2021-05) section 5.

Entaksi applies all security controls and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the Information Security Policy, publicly available at https://www.entaksi.eu/en/ispd.html.

6.2. Trust service practice statement

6.2.1. Time-stamp format

Time-stamps issued by the Entaksi TSA are compliant with RFC 3161 (including support for `reqPolicy`, `nonce` and `certReq`).

The cryptographic algorithms and key lengths used by the TSU comply with ETSI EN 319 422 V1.1.1 (2016-03):

- Acceptable Time-stamp request hashes: SHA-256, SHA-384, SHA-512.
- Signature: `sha256WithRSAEncryption` (4096 bit).

6.2.2. Accuracy of the time

Entaksi TSA provides time accurancy of 1 second or better of UTC.

Time is synchronized with the following NTP servers provided by the Italian "Istituto Nazionale di Ricerca Metrologica", a body appointed by the Bureau International des Poid et Mesures:

- `ntp1.inrim.it`
- `ntp2.inrim.it`
- `time.inrim.it`

The time included in a Time-stamp is the time of processing by the TSU, not the time of submission nor of acceptance.

6.2.3. Limitations of the service

The service can only be used by subscribers with a prior service contract.

6.2.4. Obligations of the subscriber

Subscribers must verify that the Time-stamp has been correctly signed and check that the private key used to sign the Time-stamp has not been compromised.

Subscribers must use secure cryptographic functions for issuing time-stamping requests.

Subscribers must inform their relying parties about the Entaksi TSA Policy and Practice Statement.

6.2.5. Relying party obligations

Relying parties must verify that the Time-stamp has been correctly signed and that the private key used to sign the Time-stamp has not been compromised.

Long term verification of time-stamp

As per ETSI EN 319 421 V1.2.1 (2023-05) Annex D, verification of a Time-stamp can still be performed after the end of the validity period of the TSU certificate, if at the time of verification:

- The TSU private key has not been compromised.
- The hash algorithm, signature algorithm and signature key size are still supported by Entaksi TSA Policy and Practice Statement.

6.2.6. Verification of the time-stamp

Time-stamp verification includes the following steps:

- Verification of the Time-stamp issuer.
- Verification of the revocation status of the TSU certificate in the Time-stamp.

6.2.7. Availability

Entaksi operates the Time-stamp service implementing business continuity measures to guarantee 24 hours a day, 7 days a week.

Service Level Agreement of minimum uptime of the service is specified in the subscriber agreement.

The Entaksi TSA Disclosure Statement (MAN eIDAS 20230426 TSA Disclosure Statement) is available at https://www.entaksi.eu.

6.3. Terms and conditions

Entaksi provides a service agreement ("Condizioni generali del servizio") to interested subscribers to be informed about terms and conditions of the TSA Service, before entering into a contractual relationship.

The service agreement contains:

- general terms and conditions of the service;
- limitation on the use of the service;
- subscriber's obligations;
- information for parties relying on the trust service;
- the period of time during which Entaksi's event logs are retained;
- limitations of liability;
- limitations on the use of the services provided including the limitation for damages arising from the use of services exceeding such limitations;
- procedures for complaints and dispute settlement;
- whether the Entaksi trust service has been assessed to be compliant with the trust service policy, and through which conformity assessment scheme;
- Entaksi contact information;
- any undertaking regarding availability and Service Level Agreements;
- the reference to this document and other relevant policies;
- a reference to the user manual;
- the technical specification of time-stamps.

Entaksi makes the terms and conditions available to all subscribers and relying parties, and can transmit the document in paper form or electronically.

Entaksi does not currently employ subcontractors or outsourcing for the provision of critical service functions. Any third party involved would be named in the contract.

Entaksi automatically preserves the signed digital document of the service agreement both on its and the customer preservation system. If the contract is signed in paper form proceeds to digitize it and archives both the copies.

Terms and conditions are available in two languages, Italian and English.

6.4. Information security policy

The Entaksi information security policy is available at https://www.entaksi.eu/en/ispd.html.

6.5. TSA obligations

6.5.1. General

Void.

6.5.2. TSA obligation towards subscribers

Entaksi undertakes the following obligations towards subscribers:

- To operate in accordance with this policy and practice statement.
- To ensure that the TSU maintains a minimum UTC time accuracy of 1 second.
- Undergo internal and external reviews to assure compliance with relevant legislation and policies.

6.6. Information for relying parties

When relying upon a Time-stamp issued by the Entaksi TSA, relying parties must verify that the Time-stamp has been correctly signed and that the private key used to sign the Time-stamp has not been compromised until the time of the verification.

See also section Relying party obligations and section Verification of the time-stamp.

7. TSA Management and operation

7.1. Introduction

Entaksi has implemented the policies and operational procedures to maintain the security of the TSA service and aims to meet the requirements of ETSI EN 319 401 V2.3.1 (2021-05).

7.2. Internal organization

Entaksi's management is constantly committed to guarantee the reliability of the entire organization and in particular of Entaksi Time-stamp Authority service provided to customers.

Entaksi undertakes to be non-discriminatory and to guarantee access to the service to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the terms and conditions.

The Time-stamp Authority described in this document is designed for the European marketplace under the eIDAS regulation and is operated by the Irish Branch of the Italian company Entaksi Solutions SpA.

Entaksi TSA services are provided from datacenters located within the EU, in Germany.

The Integrated Management System implemented by Entaksi has certified compliance with the standards listed in Certifications.

Entaksi Integrated Management System defines the capacity planning procedures to provide personnel and facilities needed for operating the Time-stamp Authority service.

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 the time-stamping service.

7.3. Personnel security

Entaksi commits to employ qualified staff who possess the necessary expertise, reliability, experience, and qualifications to work on the Time-stamp Authority Service. It also provides constant training regarding security and personal data protection rules as appropriate for the offered services and the job function.

7.4. Asset management

Entaksi ensures an appropriate level of protection of its assets, including information assets, and it is responsible for the commitment of all the personnel to handle all the media securely, in accordance with its policies and procedures.

Entaksi uses its own software to manage all the resources, a Configuration Management Data Base (CMDB) that constitutes an inventory of all information assets, and declares for each object a classification consistent with the risk assessment.

7.5. Access control

All users accessing the Entaksi TSA are assigned to a specific user group in order to protect the segregation of roles and information.

Access is restricted to authorised individuals.

All access controls are defined to protect Entaksi's internal network from unauthorized intrusion.
Access security controls include the separation of trusted roles, logs, the separation of security administration and operation functions, controlled use of system utility programs.
Firewalls are configured to prevent all protocols and accesses not required for the operation on the Time-stamp Authority Service.

7.6. Cryptographic controls

7.6.1. General

Entaksi ensures that appropriate security controls are in place for the management of cryptographic devices and private keys.

Certificates used in the Time-stamp Unit are issued by the Entaksi CA.

7.6.2. TSU key generation

Entaksi generates the TSU key under dual control within a secure cryptographic device which is Common Criteria certified according to the EN 419 221-5 Protection Profile.

The TSU key generation algorithm is RSA with a key length of 4096 bit as per recommendations defined in ETSI TS 119 312 V1.4.1 (2021-08).

The generated TSU key and its corresponding public key and certificate are imported in all cryptographic devices that form the TSU cluster for redundancy.

The TSU uses a single signing key at a time.

7.6.3. TSU private key protection

The TSU private key is held and used inside secure cryptographic devices which 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

The device fulfills the requirements for a cryptographic module according to EN 419 231 "Protection profile for trustworthy system supporting time stamping".

Backup of the private key are stored in encrypted form so that they can only be used in a cryptographic device with the same Master Backup Key. The Master Backup Key is split in three secure tokens so that at least two of them are needed in order to rebuild the whole key. The three parts of the Master Backup Key are assigned only to the personnel authorized to carry out the backup function.

7.6.4. TSU public key certificate

Entaksi TSA guarantee the integrity and authenticity of the TSU signature verification (public) keys by signing the public key certificate with the "Entaksi Qualified Time-stamps CA G1", which is a certification authority operating under ETSI EN 319 411-1 V1.3.1 (2021-05) and the additional provisions of ETSI EN 319 411-2 V2.3.1 (2021-05).

The public key certificate is published in the Entaksi web site and included in the Time-stamp.

The TSU validates that the certificate has been correctly signed before issuing Time-stamps using the corresponding private key.

7.6.5. Rekeying TSU'key

The validity period of the TSU certificate is no longer than the period of time that the algorithm and key size specified in section Time-stamp format are fit for the purpose according to ETSI TS 119 312 V1.4.1 (2021-08).

If the TSU private key is compromised the TSU certificate is revoked by the CA and the TSU private key and certificate replaced with a new one.

7.6.6. Life cycle management of signing cryptographic hardware

Entaksi implements a specific procedure to manage the life cycle of the cryptographic hardware.

Under provision of the EN 419 221-5 Protection Profile compliance the cryptographic hardware ships with a sealed package that guarantee the integrity of the device during shipment and while stored.

The device also implements a builtin security configuration that requires dual control for installation, activation and duplication of the signing keys.

The cryptographic hardware defines an erase procedure that can be activated before disposal or retirement in a way that its practically impossibile to recover the keys.

7.6.7. End of TSU key life cycle

TSU public keys and certificates are valid for 5 years, while the corresponding private keys are valid for 3 months. Expired TSU private keys are not used beyond the end of their validity period and they are destroyed.

The Entaksi TSA implements operational and technical procedures to ensure that a new key is put in place when the TSU key expires.

7.7. Time-stamping

7.7.1. Time-stamp issuance

Time-stamps conform to the profile as defined in ETSI EN 319 422 V1.1.1 (2016-03). Time-stamps are issued upon request from a subscriber in a secure manner and they include the correct time.

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).

If the clock is detected to be out of the stated accuracy of 1 second then Time-stamp is not issued.

The issued Time-stamps are signed using the TSU private key generated exclusively for this purpose.

The Time-stamp generation system reject any attempt to issue Time-stamps if the end of the TSU private key validity has been reached.

7.7.2. Clock synchronization with UTC

The TSU clock is synchronized with the time source provider by mean of a set of NTP servers as specified in section Accuracy of the time. The calibration of the TSU clock is maintained so that the clock does not drift outside the accuracy of 1 second. The TSU clock is protected against threats which could result in undetected time drifts.

If a time drift of the TSU clock is detected the TSU stops issuing Time-stamps.

When the BIPM notifies the occurrence of a leap second, this iss applied in the last minute of the day the leap second is scheduled to occur. A record is maintained with the exact time when the leap second was applied to the TSU clock.

7.8. Physical and environmental security

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

The Time-stamping 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 Time-stamping 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 Time-stamping services cannot be taken off-site without authorization.

7.9. Operational security

Entaksi implements a capacity planning procedure monitoring the system resources usage to make sure that adequate processing power and storage are available.

Entaksi uses trustworthy systems and products that are protected against modification, and guarantees the technical security and reliability of the processes supported by them.

All these organisational procedures are established and implemented for all trusted and administrative roles that impact on the provision of service.

A security requirements analysis is carried out in the design and requirements specification phase for each system development project undertaken by the ICT management to ensure that security is implemented within the IT systems.

Change control procedures are applied for software releases, modifications and emergency fixes of any operational software or configuration change that are affected by Entaksi's safety policy. The procedures include documentation and record of changes. Any change that could impact the established security level must be approved by Entaksi's management.

The integrity of the services provided and of the organisation's information is strongly protected against viruses, malicious and unauthorized software.

Precise procedures are defined by Entaksi to ensure that the media used within the organization's systems are managed securely to protect them from damage, theft, unauthorized access, and obsolescence.

Regarding the service management operational controls, specific procedures ensure that:

- security patches are applied within a reasonable time after they come available;
- security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and
- the reasons for not applying any security patches are documented.

7.10. Network security

Entaksi applies appropriate network security controls to protect its network and systems from any attack.

ICT management has identified critical networks aimed to supply the service, based on risk assessment and considering functional, logical, and physical (including location) relationship between trustworthy systems and services.
Security controls are executed on all networks.

All TSU systems are maintained in a secure area and all accounts, applications, services, protocols and ports that are not used in the TSA's operations are disabled.

Access to the secure area is granted only to trusted roles.

Entaksi states that:

- production environment shall be separated from development and test environments;
- although separation of environments is enforced, the highest levels of security checks on connections are still applied in any configuration;
- the communication between clients and the service shall take place only through trusted channels;
- any not needed connections or service shall be explicitly forbid or deactivate;
- shall not use systems used for administration of the security policy implementation for other purposes;
- communication between distinct trustworthy systems is established only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure;

- the external network connection shall be redundant to ensure availability of the services in case of a single failure.

The policy and the network technical features are review at least yearly, or after any significant change.

7.11. Incident management

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.

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.

7.12. Collection of evidence

Entaksi maintains records of relevant information concerning the Entaksi TSA that includes:

- Events related to the life-cycle of the TSU keys.
- Events related to the clock synchronization and recalibration.

Records are time-stamped to protect data integrity and moved to a protected storage on daily base.

Records are maintained for 20 years.

7.13. Business continuity management

Entaksi implements a business continuity management system as part of its Integrate Management System certified under the scope of ISO/IEC 22301:2019.

The business continuity plan address the following two specific events regarding the Entaksi TSA operations:

- The compromise or suspected compromise of TSU's private signing key.
- The loss of calibration of the TSU clock.

For both these events Entaksi will make available a description of the compromise that occurred to subscribers and relying parties.

In the case of compromise of TSU private keys or loss of calibration of the TSU clock, the TSU will stop issuing Time-stamps until steps are taken to recover.

7.14. TSA termination and termination plans

The decision of terminate the TSA service can be taken only by the Entaksi Solution SpA 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 Solutions SpA, 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's 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 TSA 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. When Entaksi TSA terminates its services, all non-expired TSU certificates will be revoked.

7.15. Compliance

The applicable legal system is declared in References.

Entaksi TSA complies with applicable regulations and legal requirements, including the eIDAS Regulation, and with the Entaksi Privace Policy available at https://www.entaksi.eu/en/privacy.html

7.15.1. Data protection

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

Entaksi operates in the European Union, and follow the Regulation (EU) 2016/679 that repeals the Directive 95/46/EC.

The complete set of provisions relating to the processing of personal data is reported in the Terms and Conditions of the TSA service (or "Condizioni generali del servizio") document, and also on the Entaksi website.

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

8. Additional requirements for eIDAS Regulation

8.1. TSU public key certificate

Time-stamps issued by the Entaksi TSA are Qualified Time-stamps under the provisions of ETSI EN 319 422 V1.1.1 (2016-03) . The TSU public key certificate is issued by Entaksi CA, that is a certification authority operating under ETSI EN 319 411-2 V2.3.1 (2021-05) certificate policy.

Subscribers and relying parties can verify the validity of the Time-stamp using the CA certificates published in the EU Trusted List as defined in ETSI TS 119 612 V2.2.1 (2016-04).

Time-stamps issued by the Entaksi TSA contains the `qcStatements` with value `esi-4-qtstStatement-1` as defined in ETSI EN 319 422 V1.1.1 (2016-03) as an indication that the Time-stamp claims to be a Qualified Electronic Time-stamp.