IDnow Trust Services.

TSA Policy
IDnow Trust Services AB
version 1.0

Table of Contents

Table of Contents **2**

1. Introduction **5**

2. General concepts **6**

2.1 Time-Stamping Authority (TSA) 6

2.2 Subscriber 6

2.3 Time-stamp policy and TSA practice statement 6

3. Introduction to time-stamp policies and general requirements **7**

3.1 Policy name and identification 7

4. Policies and practices **8**

4.1 Trust Service Practice Statement 8

4.2 Terms and conditions 8

4.3 TSA obligations 8

4.3.1 General 8

4.3.2 TSA obligations towards subscribers 8

4.4 Information for relying parties 8

5. TSA management and operation **9**

5.1 Cryptographic controls 9

5.1.1 TSU key generation 9

5.1.2 TSU private key protection 9

5.1.3 TSU public key certificate 10

5.1.4 Rekeying TSU's key 10

5.1.5 Life cycle management of signing cryptographic hardware 10

5.1.6 End of TSU key life cycle 11

5.2 Timestamping 11

5.2.1 Timestamp issuance 11

5.2.2 Clock synchronization with UTC 12

5.3 Physical and environmental security 12

5.4 Operational security 13

5.5 Network security 13

5.6 Incident management 13

5.7 Collection of evidence 13

5.8 Business continuity management 13

5.9 TSA termination and termination plans 14

5.10 Compliance 14

6. Additional requirements for qualified electronic time-stamps as per Regulation (EU) No 910/2014 15

6.1 TSU public key certificate 15

6.2 TSA issuing non-qualified and qualified electronic time-stamps as per Regulation (EU) No 910/2014 15

7. Definitions of terms, symbols, abbreviations and notation 16

7.1 Terms 16

Document Information

Version	1.0
Version date	03.07.2024
Confidentiality level	Public
Approved by	Representative of IDnow Trust Services Management
Owner of the document	Chief Security Officer
Document name	TSA Policy IDnow Trust Services AB
Relevant for	External
Document OID	1.3.6.1.4.1.61867.2.1.5.1.1

Change log

Version	Version Date	Changes	Author
1.0	03.07.2024	Version 1.0	Adam Ptasiewicz

1. Introduction

The purpose of this document is to confirm the method and implementation of requirements for the Qualified Time Stamp Authority (QTSA). IDnow Trust Services AB provides a qualified timestamping service based on this policy. This policy is a document based on the requirements specified in the Practice Statement. Timestamping is a defined qualified trust service and is compliant with the eIDAS regulation.

2. General concepts

2.1 Time-Stamping Authority (TSA)

IDnow Trust Services AB provides time-stamping services that are used only for time-stamping purposes. It is called the Time-Stamping Authority (TSA).

Timestamping is carried out based on the requests for services provided by Trust Services. Specifically, it is utilized in the signing process by the Central Component as described in the Practice Statement.

The TSA is responsible for providing timestamping services by operating one or more Timestamping Units (TSUs), which create and sign on behalf of the TSA. The TSA is responsible for issuing a timestamps that are identifiable.

The TSA may make use of other parties to provide parts of the time-stamping services. However, the TSA always maintains overall responsibility and ensures that the policy requirements identified in the present document are met.

The TSA operates one identifiable time-stamping unit.

2.2 Subscriber

Timestamping is carried out based on requests through the Signature Application described in the Practice Statement.

2.3 Time-stamp policy and TSA practice statement

A time-stamp policy is a form of Trust Service Policy as specified in ETSI EN 319 401, ETSI EN 419 231, and ETSI EN 319 421, ETSI EN 319 422 applicable to trust service providers that issue timestamps.

The present document specifies a time-stamp policy to meet general requirements for trusted time-stamping services. The TSA specifies in its practice statement how these requirements are met.

3. Introduction to time-stamp policies and general requirements

3.1 Policy name and identification

The identifier of the time-stamp policy specified in the present document is:

a) BTSP: a best practices policy for timestamp.

```
itu-t(0) identified-organization(4) etsi(0)
time-stamp-policy(2023)
policy-identifiers(1) best-practices-ts-policy (1)
```

By including this identifier object in a timestamp, the TSA claims conformance to the identified time-stamp policy.

The TSA embeds the identifier for the supported time-stamp policy in its disclosure statement, which is accessible to subscribers and those relying on the service, to evaluate its compliance.

4. Policies and practices

4.1 Trust Service Practice Statement

IDnow Trust Services AB has a publicly available Practise Statement which describes general rules applicable to the qualified, trusted services. These practices also cover time stamp services; this document describes areas specific to timestamp services.

IDnow Trust Services AB declares the use of the SHA-512 hashing algorithm with RSA and the 3072-bit key algorithm used to represent the data being time-stamped.

4.2 Terms and conditions

Before using the service described in this document, the User will be required to read the Terms & Conditions.

4.3 TSA obligations

4.3.1 General

The TSA adheres to every additional obligation indicated in the timestamp either directly or incorporated by reference.

4.3.2 TSA obligations towards subscribers

The present document places no specific obligations on the subscriber beyond the TSA-specific requirements stated in the TSA's terms and conditions.

4.4 Information for relying parties

The TSA ensures the integrity of the timestamp. It is the obligation of relying party to 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.

5. TSA management and operation

Management along with operational and physical controls are described in the Practice Statement. This chapter contains additional practices that IDnow Trust Services AB implements regarding its timestamping service.

5.1 Cryptographic controls

5.1.1 TSU key generation

The creation of the TSU's signing keys takes place in a secure physical environment, involving personnel who hold trusted roles and operate under dual control.

Only those individuals deemed necessary according to the TSA's operational practices are authorized to generate the TSU's signing keys.

The process of generating the TSU's signing keys occurs within a secure cryptographic device that either:

Achieves a trustworthiness level of EAL 4 or higher as per ISO/IEC 15408 or an equivalent standard, tailored to a security target or protection profile that aligns with this document's requirements and a comprehensive risk analysis, including physical and other security measures.

Fulfills the criteria set by ISO/IEC 19790, FIPS PUB 140-2 level 3, or FIPS PUB 140-3 level 3.

The selection of the TSU key generation algorithm, the resulting signing key length, and the signature algorithm for timestamp keys adhere to the standards specified in ETSI TS 119 312. A TSU's signing key remains exclusive to a single cryptographic module and cannot be transferred between different modules.

5.1.2 TSU private key protection

The integrity and confidentiality of the TSU private keys are preserved through specific measures specified below.

The TSU private signing key is securely managed within a cryptographic module that:

Is recognized as a reliable system, confirmed to EAL 4 or above according to ISO/IEC 15408 or an equivalent standard, crafted to a security target or protection profile that fulfills the requirements of this document, with a risk analysis that considers both physical and other security aspects.

Complies with the standards set in ISO/IEC 19790, FIPS PUB 140-2 level 3, or FIPS PUB 140-3 level 3.

In instances where TSU private keys are backed up, the procedure of copying, storing, and recovering these keys is exclusively performed by trusted personnel, utilizing dual control within a secure physical setting. Only individuals deemed necessary by the TSA's operational protocols are authorized to execute the backup operations. The cryptographic module adequately safeguards any backup copies of the TSU private signing keys to maintain their integrity and confidentiality prior to being stored externally, in line with the additional requirements for private key protection outlined in the timestamping protection profile EN 419 231.

5.1.3 TSU public key certificate

The (public) TSU signature verification keys are provided to relying parties through a public key certificate, ensuring transparency and accessibility.

The TSU does not issue timestamps until the certificate for its signature verification (public key) has been properly integrated into the TSU or its associated cryptographic device, ensuring a secure and verified starting point for time-stamp issuance.

5.1.4 Rekeying TSU's key

The procedure of rekey based on the current key pair is not allowed.

A new key pair will be securely generated as described in section 5.1.1, and a new certificate will be issued.

5.1.5 Life cycle management of signing cryptographic hardware

The cryptographic hardware used to sign timestamps is secured and intact throughout the shipping process, ensuring its integrity upon arrival. During storage, the cryptographic hardware designated for timestamp signing is safeguarded against any form of tampering, thereby maintaining its security and reliability. The tasks of installing, activating, and duplicating the TSU's signing keys within cryptographic hardware are exclusively carried out by authorized personnel

who occupy trusted roles. This process requires a dual control at a minimum and takes place within a secure physical environment, ensuring a high level of security and oversight.

When a cryptographic device used by the TSU is retired, all private signing keys stored on the module are thoroughly erased. This deletion process ensures that the keys become practically irretrievable, preserving the confidentiality and integrity of the cryptographic operations previously performed by the device.

5.1.6 End of TSU key life cycle

The TSA sets an expiration date for TSU keys for 8 years to ensure security and ease of management. The expiration date of TSU keys may not exceed the validity period of the corresponding public key certificate, ensuring that the key lifecycle is consistent with the certificate duration.

Operational or technical measures have been implemented to transition to a new key upon expiration of the TSU key without interruptions, ensuring the continuity of services without compromising security. Within 1 year before the expiration of TSU key, the new key pair is generated as described in 5.1.1.

Upon expiry or when no longer needed, TSU private signing keys, including any parts or copies thereof, are irreversibly destroyed to prevent recovery, thereby ensuring the confidentiality of the information they were used to protect.

5.2 Timestamping

5.2.1 Timestamp issuance

Issued timestamps comply with the specifications set out in the ETSI EN 319 422 timestamp profile, ensuring consistency and standardization. Issuing time stamps is conducted securely, preventing unauthorized access and ensuring the authenticity of the time stamps. The generated timestamps accurately reflect the correct time, providing the reliability of timestamping services.

Specifically, the time values utilized by the TSU in timestamps are verifiably linked to one of the real time values provided by a UTC(k) laboratory, as recognized by the Bureau International des Poids et Mesures (BIPM), ensuring an authoritative source of time. The time contained in timestamps is synchronized with Coordinated Universal Time (UTC) in accordance with the Recommendation ITU-R TF.460-6.

If a TSA's clock deviates from its stated accuracy, the issuance of timestamps will be suspended to maintain the integrity and reliability of the timestamping service. The digital signature on each timestamp is generated using a dedicated key, ensuring the security and authenticity of the timestamp. The timestamp generation system automatically rejects any attempt to issue timestamps after the TSU private key has expired, thereby protecting against the use of invalid or compromised keys.

5.2.2 Clock synchronization with UTC

The TSU clock synchronizes with Universal Time (UTC), maintaining synchronization within a specified accuracy range and complying with additional requirements. TSU clocks are calibrated to prevent deviations beyond the stated accuracy, ensuring consistent and reliable timekeeping.

The accuracy of TSU clocks is under one second, setting a high standard for time precision.

Measures are in place to protect TSU clocks from potential threats that may lead to unauthorized changes or interference, thereby maintaining their calibration and accuracy. The TSA is responsible for monitoring and identifying any discrepancy where the time indicated on the timestamp may deviate from UTC, ensuring the integrity of the timestamps. If a discrepancy or offset from UTC synchronization is detected, the TSU is programmed to stop issuing timestamps to prevent the dissemination of erroneous or unreliable timestamps.

In the event of a leap second, as announced by the relevant authority, the clock synchronization process is intended to smoothly adapt to this regulation. The leap second correction is scheduled in the last minute of the day on which the leap second is scheduled, ensuring a smooth transition. A detailed record is kept of the exact moment (within the declared accuracy) of the leap second adjustment, providing a transparent and verifiable description of the synchronization process. This protocol follows the practice of adding or omitting a second at the end of specific UTC months, with a preference for late December and June and a second preference for March and September.

5.3 Physical and environmental security

Access control measures are used to ensure that the cryptographic module is in a secure environment. Timestamp management operations occur in an environment with physical and logical safeguards to prevent unauthorized access to the system or data.

A meticulous record is kept of each person's entry and exit from the protected area. The integrity of timestamping management is ensured by establishing clear security boundaries, indicated by physical barriers.

Comprehensive physical and environmental security measures are used to protect the facility containing system resources and the infrastructure supporting their functionality.

5.4 Operational security

The TSA actively monitors capacity demands and forecasts future requirements to guarantee that sufficient processing power and storage capacity are always available.

5.5 Network security

TSA ensures that all TSU systems are secured by removing or deactivating any unnecessary accounts, applications, services, protocols, and ports that are not essential to TSA operation.

Only people in trusted roles within the TSA have access to secure and high-security zones.

5.6 Incident management

The scope related to this item is addressed in the Practice Statement.

5.7 Collection of evidence

TSU key management

The TSA maintains records of every event related to the lifecycle of TSU keys. It maintains detailed records of all TSU certificate lifecycle events, where applicable.

Clock Synchronization

The TSA records and logs all events related to the TSU clock synchronization with UTC time. Any event where a loss of synchronization is detected is logged by TSA.

The detailed scope related to this item is addressed in the Practice Statement.

5.8 Business continuity management

The TSA's disaster recovery plan addresses scenarios in which the TSU's private signing keys might be compromised or suspected of being compromised, as well as any loss of calibration of the TSU clock that could affect issued timestamps.

In any case of operational compromise of the TSU, such as a key compromise, suspected compromise, or loss of clock calibration, the TSU will halt the issuance of timestamps until the necessary recovery actions are executed.

IDnow Trust Services AB maintains a business continuity plan (BCP). The detailed scope related to this item is addressed in the Practice Statement.

5.9 TSA termination and termination plans

Upon cessation of its services, the TSA will revoke all TSU certificates that have not yet expired.

The detailed scope related to this item is addressed in the Practice Statement.

5.10 Compliance

The scope related to this item is addressed in the Practice Statement.

Additional requirements for qualified electronic time-stamps as per Regulation (EU) No 910/2014

5.11 TSU public key certificate

- The Trust Service policy document complies with the relevant standards, including ETSI EN 319 411-2. When a timestamp is claimed as a qualified electronic timestamp in accordance with Regulation (EU) No 910/2014, the TSU signature verification (public) key certificate is issued by a certification authority that operates under the ETSI EN 319 411-2 certificate policy, which encompasses the requirements of ETSI EN 319 411-1.

The policy document supports the reliance on a Trusted List for determining the qualification of the timestamping service and the timestamps issued. If the public key of the TSU is listed on the Trusted List, representing a qualified timestamping service, the timestamps from this TSU are recognized as qualified.

Additionally, for a TSA operating multiple TSUs, if the public key is listed in the Trusted List as per ETSI TS 119 612 and includes "qualified timestamping" service, the timestamps issued are regarded as qualified when the TSU is properly identified in its certificate within the TSA's context. The inclusion of the qcStatement "esi4-qtstStatement-1" as outlined in ETSI EN 319 422, clause 9.1, is an indication of the timestamp's status as a claimed qualified electronic timestamp.

5.12 TSA issuing non-qualified and qualified electronic time-stamps as per Regulation (EU) No 910/2014

The TSU is exclusively dedicated to qualified electronic timestamps. This ensures the integrity and distinctiveness of our qualified electronic time-stamping service. Since non-qualified timestamps are excluded, there is no need for differentiation between TSUs with separate subject names in their public key certificates or distinct service access points. Our adherence to these protocols affirms our commitment to delivering qualified time-stamping services that meet the regulatory standards and technical specifications set forth, including those detailed in ETSI TS 119 612.

6. Definitions of terms, symbols, abbreviations and notation

6.1 Terms

Central Component - application responsible for orchestrating signing related operations on the backend system. Compliant with the CSC API V2.0 specification.

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6.

time-stamp policy: a named set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with standard security requirements.

Time-Stamping Authority (TSA): IDnow Trust Services AB providing time-stamping services using one or more time-stamping units.

Time-Stamping Unit (TSU): a set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.

UTC(k): time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns.

IDnow Trust Services AB
Box 16285
103 25 Stockholm
Sweden

info@trust-services.io
www.trust-services.io