Gjaldstovan Timestamping Practice Statement

Version 1.0 - 09 Oct 2023

Gjaldstovan
Kvíggjartún 1,
FO-160 Argir
Faroe Islands
EAN 5797100000010

Or:

gjaldstovan@gjaldstovan.fo

Table of contents

Version history

Version	Author	Comment
1.0	Janus Læarsson	Approved and effective version.

1 Introduction

1.1 Scope

This practice statement specifies policy and security requirements relating to the operation and management practices of the official Gjaldstovan Timestamp Authorities issuing timestamps.

These requirements are only applicable to TSPs issuing timestamps. Such timestamps can be used in support of any application requiring to prove that a datum existed before a particular time.

The practise statement can be used by independent bodies as the basis for confirming that a TSP can be trusted for issuing timestamps.

2 References

2.1 Normative References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

The following referenced documents are necessary for the application of the present document:

- [1] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
- [2] ISO/IEC 19790:2012: "Information technology – Security techniques – Security requirements for cryptographic modules".
- [3] ISO/IEC 15408 (parts 1 to 3): "Information technology – Security techniques – Evaluation criteria for IT security".
- [4] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
- [5] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Timestamping protocol and time-stamp token profiles".
- [6] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

2.2 Informative References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

The following referenced documents are not necessary for the application of the present document but they assist the reader with regard to a particular subject area:

- [i.1] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".
- [i.2] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".
- [i.3] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".
- [i.4] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- [i.5] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
- [i.6] BIPM Circular T.
- [i.7] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".
- [i.8] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for timestamping authorities".
- [i.9] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".
- [i.10] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

- [i.11] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".
- [i.12] CEN EN 419 231: "Protection profile for trustworthy systems supporting time stamping".
- [i.13] CEN EN 419 221-2: "Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup".
- [i.14] CEN EN 419 221-3: "Protection profiles for TSP Cryptographic modules - Part 3: Cryptographic module for Cryptographic module for CSP key generation services".
- [i.15] CEN EN 419 221-4: "Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup".
- [i.16] CEN EN 419 221-5: "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services".

3 Definitions and Abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given ETSI EN 319 401 [4] and the following apply:

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6 [1]

Relying party: recipient of a timestamp who relies on that time-stamp

Subscriber: legal or natural person to whom a timestamp is issued and who is bound to any subscriber obligations

Timestamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

Timestamping Authority (TSA): TSP providing timestamping services using one or more timestamping units

Timestamping service: trust service for issuing timestamps

Timestamping Unit (TSU): set of hardware and software which is managed as a unit and has a single timestamp signing key active at a time

Trust service: electronic service that enhances trust and confidence in electronic transactions

Trust Service Provider (TSP): entity which provides one or more trust services

TSA Disclosure statement: set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements

TSA practice statement: statement of the practices that a TSA employs in issuing timestamp in relation to a timestamp policy

TSA system: composition of IT products and components organized to support the provision of timestamping services

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

3.2 Abbreviations

For the purposes of this policy, the abbreviations given in ETSI EN 319 401 [4] and the following apply:
BIPM: Bureau International des Poids et Mesures
BTSP: Best practices Time-Stamp Policy
CA: Certification Authority
GMT: Greenwich Mean Time
IERS: International Earth Rotation and Reference System Service
TAI: International Atomic Time
TSA: Timestamping Authority
TSP: Trust Service Provider
TSU: Timestamping Unit
UTC: Coordinated Universal Time

4 General Concepts

4.1 General Policy Requirements Concepts

The policy references ETSI EN 319 401 [4] for generic policy requirements common to all classes of trust service providers service. These policy requirements are based upon the use of public key cryptography, public key certificates and reliable time sources. Subscriber and relying parties are expected to consult the TSA's practice statement to obtain further details of precisely how this time-stamp policy is implemented by the particular TSA (e.g. protocols used in providing this service).

4.2 Timestamping Services

The provision of timestamping services is broken down in the present document into the following component services for the purposes of classifying requirements:

- Timestamping provision: This service component generates time-stamps.
- Timestamping management: This service component monitors and controls the operation of the timestamping services to ensure that the service provided is as specified by the TSA. This service component has responsibility for the installation and de-installation of the timestamping provision service.

This subdivision of services is only for the purposes of clarifying the requirements specified in the policy and places no restrictions on any subdivision of an implementation of timestamping services.

4.3 Timestamping Authority (TSA)

A Trust Service Provider (TSP) providing timestamping services to the public, is called the Timestamping Authority (TSA).

Gjaldstovan has overall responsibility for the provision of the timestamping services identified in clause 4.2. Gjaldstovan has responsibility for the operation of one or more TSUs which creates and signs on behalf of a Gjaldstovan TSA.

Gjaldstovan may make use of other parties to provide parts of the timestamping services. However, Gjaldstovan always maintains overall responsibility and ensures that the policy requirements identified in this document are met. Gjaldstovan may operate several identifiable timestamping units.

Gjaldstovan is a trust service provider as described in ETSI EN 319 401 [4] which issues time-stamps.

4.4 Subscriber

A Subscriber, as used herein, refers to both the subject of the certificate issued by Gjaldstovan and the entity that is contracted with Gjaldstovan for the use of the Timestamping Service

4.5 Timestamp Policy and TSA Practice Statement

This section explains the relative roles of Timestamp policy and TSA practice statement.

A Timestamp policy is a form of trust service policy as specified in ETSI EN 319 401 [3] applicable to Trust Service Providers issuing Timestamps.

The Gjaldstovan Timestamping Practice Statement is a form of Trust Service Practice Statement as specified in ETSI EN 319 401 [3] applicable to Trust Service Providers issuing Timestamps.

This document specifies the Timestamp policy and the practice statement for the Gjaldstovan Timestamping Authority

5 Timestamp Policies

5.1 General

The policy requirements are defined in this policy in terms of a timestamp policy. The policy specifies one timestamp policy: a baseline timestamp policy (BTSP) for TSAs issuing time-stamps, supported by public key certificates, with an accuracy of 1 second or better against UTC.

5.2 Identification

The identifier of this timestamp policy is:

a) BTSP : itu-t(0) identified-organization(4) etsi(0)time-stamp-policy(2023)policy-identifiers(1) baseline-ts-policy (1)

By including this object identifier in a timestamp, the TSA claims conformance to the identified timestamp policy. A TSA shall include the identifier for the timestamp policy being supported in the TSA disclosure statement made available to subscribers and relying parties to indicate its claim of conformance.

5.3 User Community and Applicability

This policy is aimed at meeting the requirements of time-stamp for long term validity (e.g. as defined in ETSI EN 319 122 [i.1]) but is generally applicable to any use which has a requirement for equivalent quality. This policy may be used for public timestamping services on the Faroe Islands.

6 Policies and Practices

6.1 Risk Assessment

Gjaldstovan shall carry out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues.

Gjaldstovan shall select the appropriate risk treatment measures, taking account of the risk assessment results.

The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.

Gjaldstovan shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and this practice statement.

The risk assessment shall be regularly reviewed and revised.

The Gjaldstovan TSP management Board shall approve the risk assessment and accept the residual risk identified.

6.2 Trust Service Practice Statement

Gjakdstovan shall ensure the quality, performance and operation of the timestamping service through the implementation of various security policies and controls.

The securty policies and controls are reviewed regularly by an independent 3rd party. Trained personnel check the adherence of the security controls to the policies.

6.2.1 Timestamp Format

The service issues timestamps signed using the digest algorithm SHA-256.

6.2.2 Accuracy of the Time

The timestamping service time source is a Stratum 1 time server. The time server is a stable and precise Meinberg hardware appliance with directly connected Meinberg outdoor GPS antenna and onboard TCXO oscillator which is capable of bridging interferences or a temporary loss of reception. For additional backup the appliance is also using ntp.org pools for reference time source.

The timestamping service ensures an accuracy of 1 second with respect to UTC.

It shall be noted that the time of timestamping is not the timestamping request acceptance moment, but the timestamping system processing moment.

6.2.3 Limitations of Service

No stipulation.

6.2.4 Obligations of Subscriber

No stipulations.

6.2.5 Obligations of Relying Parties

Before relying on a timestamp, the Relying Party shall:

1. Verify that the Timestamp has been correctly signed
2. Verify that the certificate used to sign the Timestamp was valid at the time indicated within the Timestamp and that the private key used to sign the Timestamp has not been compromised before the time of the verification. See section 6.2.6 of this practice statement and section 9.6.4 of the Gjaldstovan Root CPS.
3. Consider any limitations on the usage of the Timestamp indicated by this practice statement.
4. Consider any other precautions prescribed in agreements or elsewhere.

6.2.6 Verification of the Timestamp

Timestamp verification includes the following:

6.2.6.1 Verification of Timestamp Issuer

TSU and issuing CA certificates are published to allow Relying Parties to verify that Timestamps are issued by a TSU operated by Gjaldstovan.

The certificates can be found here: https://repository.samleiki.fo/certs.html

6.2.6.2 Verification of the Timestamp Revocation Status

An OCSP responder service is available to check the revocation status of the used certificates in the timestamp.

6.2.7 Applicable Law

Gjaldstovan will, in relation to this CPS, comply with applicable national laws, rules, regulations, ordinances, decrees and orders.

6.2.8 Service Availability

Gjaldstovan implements the following measures to ensure availability of the service:

- Redundant setup of the Timestamping service, including Timestamp issuing, inorder to avoid single points of failure
- Redundant high-speed internet connection in order to avoid loss of service
- Use of uninteruptable power supplies

Gjaldstovan does not guarantee 100% availability but aims to provide 99,5% availability per year.

6.3 Terms and Conditions

This document represents the applied trust service policy.

For Subscribers, please refer to the obligations in section 6.2.4. Service specific agreements may apply.

For Relying Parties, please refer to the obligations in section 6.2.5.

6.4 Information Security Policy

The requirements identified in ETSI EN 319 401 [4], clause 6.3 shall apply.

6.5 TSA Obligations

6.5.1 General

No stipulations.

6.5.2 TSA Obligations Towards Subscribers

The present document places no specific obligations on the subscriber beyond any TSA specific requirements stated in the TSA's terms and conditions, section 6.3 of this document.

6.6 Information for Relying Parties

Refer to the obligations of Relying Parties in section 6.2.5.

7 TSA Management and Operation

7.1 Introduction

These policy requirements are not meant to imply any restrictions on charging for TSA services. The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objective will be met.

The provision of a timestamp in response to a request is at the discretion of the TSA depending on any service level agreements with the subscriber.

7.2 Internal Organization

The requirements identified in ETSI EN 319 401 [4], clause 7.1 shall apply. In addition the following particular requirements apply:

a) The Gjaldstovan TSA shall be a legal entity according to national law.

b) The Gjaldstovan TSA shall have a system or systems for quality and information security management appropriate for the timestamping services it is providing.

c) It shall employ 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 timestamping services.

7.3 Personnel Security

The requirements identified in ETSI EN 319 401 [4], clause 7.2 shall apply.

7.4 Asset Management

The requirements identified in ETSI EN 319 401 [4], clause 7.3 shall apply.

7.5 Access Control

The requirements identified in ETSI EN 319 401 [4], clause 7.4 shall apply.

7.6 Cryptographic Controls

7.6.1 General

The requirements identified in ETSI EN 319 401 [4], clause 7.5 shall apply.

7.6.2 TSU Key Generation

The following particular requirements apply:

a) The generation of the TSU's signing key(s) shall be undertaken in a physically secured environment (as per clause 7.8) by personnel in trusted roles (as per clause 7.3) under, at least, dual control. The personnel authorized to carry out this function shall be limited to those required to do so under the TSA's practices.

b) The generation of the TSU's signing key(s) shall be carried out within a secure cryptographic device which:
i) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [3], or equivalent national or internationally recognized evaluation criteria for IT security. This shall be to a security target or protection profile which meets the requirements of the policy, based on a risk analysis and taking into account physical and other non-technical security measures; or
ii) meets the requirements identified in ISO/IEC 19790 [2] or FIPS PUB 140-2 [6], level 3.

The secure cryptographic device should be as per i).

c) The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamps key should be as specified in ETSI TS 119 312 [i.7]. Each TSU under this policy shall in its practice statement describe the used algorithms in use, only allowing algorithms within the current version of ETSI TS 119 312.

d) A TSU's signing key should not be imported into different cryptographic modules.

e) If there are same keys in different cryptographic modules, they shall be associated with the same public key certificate into all the different cryptographic modules.

f) A TSU shall have a single time-stamp signing key active at a time.

7.6.3 TSU Private Key Protection

The TSU private keys shall remain confidential and their integrity shall be maintained with at least the following particular requirements:

a) The TSU private signing key shall be held and used within a cryptographic module which:
i) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [3], or equivalent national or internationally recognized evaluation criteria for IT security. This shall be to a security target or protection profile which meets the requirements of the policy, based on a risk analysis and taking into account physical and other non-technical security measures; or
ii) meets the requirements identified in ISO/IEC 19790 [2] or FIPS PUB 140-2 [6], level 3.

The secure cryptographic device should be as per i).

b) If TSU private keys are backed up, they shall be copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 7.8). The personnel authorized to carry out this function shall be limited to those required to do so under the TSA's practices.

c) Any backup copies of the TSU private signing keys shall be protected to ensure its integrity and confidentiality by the cryptographic module before being stored outside that device.

7.6.4 TSU Public Key Certificate

The TSA shall guarantee the integrity and authenticity of the TSU signature verification (public) keys with at least the following particular requirements:

a) TSU signature verification (public) keys shall be made available to relying parties in a public key certificate.

b) The TSU signature verification (public) key certificate should be issued by a certification authority operating under ETSI EN 319 411-1 [i.10].

c) The TSU shall not issue timestamp before its signature verification (public key) certificate is loaded into the TSU or its cryptographic device.

When obtaining a signature verification (public key) certificate, the TSA should verify that this certificate has been correctly signed (including verification of the certificate chain to a trusted certification authority).

7.6.5 Rekeying TSU's Key

The validity period of TSU's certificate shall not be longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose (see clause 7.6.2c).

7.6.6 Lifecycle Management of Signing Cryptographic Hardware

The following particular requirements apply:

a) Time-stamp signing cryptographic hardware shall not be tampered with during shipment.

b) Time-stamp signing cryptographic hardware shall not be tampered with when and while stored.

c) Installation, activation and duplication of TSU's signing keys in cryptographic hardware shall be done only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 7.8).

d) TSU private signing keys stored on TSU cryptographic module shall be erased upon device retirement in a way that it is practically impossible to recover them.

7.6.7 End of TSU Key Life Cycle

The TSA shall define an expiration date for TSU's keys. This date shall not be longer than the end of validity of the associated public key certificate. This date should take into account the lifetime defined in 'recommended key sizes versus time' from ETSI TS 119 312 [i.7].

However in order to be able to verify during a sufficient lapse of time the validity of the time-stamps, the validity of the TSU's signing key should be reduced.

The expiration date for TSU's keys may be defined when the TSU cryptographic module is initialized or by setting a private key usage period within the TSU's public key certificate.

The TSU private signing keys shall not be used beyond the end of their validity period. In particular:

a) Operational or technical procedures shall be in place to ensure that a new key is put in place when a TSU's key expires.

b) The TSU private signing keys, or any key part, including any copies shall be destroyed such that the private keys cannot be retrieved.

7.7 Timestamping

7.7.1 Timestamp issuance

Timestamps shall conform to the timestamp profile as defined in ETSI EN 319 422 [5]. The timestamps shall be issued securely and shall include the correct time. In particular:

a) The time values the TSU uses in the timestamp shall be traceable to at least one of the real time values distributed by a UTC(k) laboratory.

b) The time included in the time-stamp shall be synchronized with UTC [1] within the accuracy defined in the policy and, if present, within the accuracy defined in the timestamp itself.

c) If the timestamp provider's clock is detected (see clause 7.7.2 c)) as being out of the stated accuracy (see clause 7.7.1 b)) then timestamps shall not be issued.

d) The timestamp shall be signed using a key generated exclusively for this purpose.

e) The timestamp generation system shall reject any attempt to issue timestamps when the end of the validity of the TSU private key has been reached.

7.7.2 Clock synchronization with UTC

The TSU clock shall be synchronized with UTC [1] within the declared accuracy with at least the following particular requirements:

a) The calibration of the TSU clocks shall be maintained such that the clocks do not drift outside the declared accuracy.

b) The declared accuracy shall be of 1 second or better.

c) The TSU clocks shall be protected against threats which could result in an undetected change to the clock that takes it outside its calibration.

d) The TSA shall detect if the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC.

e) If it is detected that the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC, the TSU shall stop time-stamp issuance.

f) The clock synchronization shall be maintained when a leap second occurs as notified by the appropriate body. The change to take account of the leap second shall occur during the last minute of the day when the leap second is scheduled to occur. A record shall be maintained of the exact time (within the declared accuracy)when this change occurred.

7.8 Physical and Environmental Security

The requirements identified in ETSI EN 319 401 [4], clause 7.6 shall apply. In addition the following particular requirements apply:

a) Access controls shall be applied to the cryptographic module to meet the requirements of security of cryptographic modules as identified in clause 7.6.

b) The following additional controls apply to timestamping management:

- The timestamping management facilities shall be operated in an environment which physically and logically protects the services from compromise through unauthorized access to systems or data.
- Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area. Every entry and exit shall be logged.
- Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the timestamping management. Any parts of the premises shared with other organizations shall be outside this perimeter.
- Physical and environmental security controls shall protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation. The TSA's physical and environmental security policy for systems concerned with timestamping management shall address as a minimum the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.
- Controls shall protect against equipment, information, media and software relating to the timestamping services being taken off-site without authorization.

Other functions may be supported within the same secured area provided that the access is limited to authorized personnel.

7.9 Operation Security

The requirements identified in ETSI EN 319 401 [4], clause 7.7 shall apply. In addition the following particular requirements apply:
System Planning

a) Capacity demands shall be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

7.10 Network Security

The requirements identified in ETSI EN 319 401 [4], clause 7.8 shall apply. In addition, the following particular requirements apply:

a) The TSA shall maintain and protect all TSU systems in a secure zone.

b) The TSA shall configure all TSU systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the TSA's operations.

c) Only trusted roles shall access secure zones and high security zones.

7.11 Incident Management

The requirements identified in ETSI EN 319 401 [4], clause 7.9 shall apply.

7.12 Collection of Evidence

The requirements identified in ETSI EN 319 401 [4], clause 7.10 shall apply. In addition the following particular requirements apply:

TSU Key Management

a) Records concerning all events relating to the life-cycle of TSU keys shall be logged.

b) Records concerning all events relating to the life-cycle of TSU certificates (if appropriate) shall be logged.

Clock Synchronization

c) Records concerning all events relating to synchronization of a TSU's clock to UTC shall be logged. This shall include information concerning normal re-calibration or synchronization of clocks used in timestamping.

d) Records concerning all events relating to detection of loss of synchronization shall be logged.

7.13 Business Continuity Management

The requirements identified in ETSI EN 319 401 [4], clause 7.11 shall apply. In addition the following particular requirements apply:

a) The TSA's disaster recovery plan shall address the compromise or suspected compromise of TSU's private signing keys or loss of calibration of a TSU clock, which may have affected time-stamps which have been issued.

b) In the case of a compromise, or suspected compromise or loss of calibration when issuing time-stamp the TSA shall make available to all subscribers and relying parties a description of compromise that occurred.

c) In the case of compromise to a TSU's operation (e.g. TSU key compromise), suspected compromise or loss of calibration the TSU shall not issue time-stamps until steps are taken to recover from the compromise.

d) In case of major compromise of the TSA's operation or loss of calibration, the TSA shall make available to all subscribers and relying parties information which can be used to identify the time-stamps which may have been affected, unless this breaches the privacy of the TSAs users or the security of the TSA services.

7.14 TSA Termination and Termination Plans

The requirements identified in ETSI EN 319 401 [4], clause 7.12 shall apply. In addition the following particular requirements apply:

a) When the TSA terminates its services, the TSA shall revoke the TSU's certificates.

7.15 Compliance

The requirements identified in ETSI EN 319 401 [4], clause 7.13 shall apply.