Signicat Time-stamp policy and Practice statement ETSI 319 421

Document ID:	Signicat-TSP002
Policy ID:	2.16.578.1.46.1.14.3.6
Owner:	CISO
Version:	Version 1.6
Date:	2020-04-06
Review & Update Schedule	When needed, but at least annually
Distribution:	Public

Table of contents

1 Introduction

As the volume of viable information being both produced and stored digitally increases, the need for a trustworthy way of proving when it was created and that it hasn't been altered since, increases. It is also essential that such proof is both recognized by EU/EEA law and can ensure non-repudiation in any judicial dispute. A Time-Stamp Authority (hereinafter TSA) is a service for providing such proof by digitally time-stamping a datum, using PKI cryptography to ensure integrity and enable verification of the time-stamp. The TSA ensures correct time by synchronizing its time-stamping unit's clock with a TA (*Time authority*) connected to the authoritative BIPM network (*Bureau international des poids et mesures*), the international network of time authorities responsible for coordinating the universal time (UTC).

Such time-stamps can be used in support of digital signatures or for any application requiring proof that a datum existed at a given time.

To summarize:

- The trusted time-stamp ensures that the datum existed in its given form, at the time when the time-stamp was generated.
- When a time-stamp provided by a TSA is applied to an electronic signature/seal, it will increase the trustworthiness of when that signature/seal actually was created.

1.1 Scope

The present document (the "*Policy & Practice Statement"*) describes the practices adopted for fulfilling the requirements given in the ETSI's best practice time-stamp policy (BTSP) for the Signicat TSA – "*ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*" [ETSI BTSP].

The Policy & Practice Statement both defines the time-stamp policy (P) and describes the practices used to comply with it (PS), and is hereinafter just referenced to as P/PS.

The structure is quite similar to the one used in "*ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*" [ETSI BTSP] to ease navigation during assessments.

1.2 Revision history

Version	Date	Author	Comments
1.6	2020-04-06	TSA auditor	Internal review against EN 319 401 v 2.2.1. Changed distribution to public.
1.5	2019-10-31	CISO	Updated the key algorithm
1.4	2019-06-25	CISO	Added versioning to the OID.
1.3	2019-05-03	CISO	Clarifying active signing key.
1.2	2018-04-11	Signicat	Added explanation of dual control regime.
1.1	2018-01-18	CLP, Signicat	Legal revision, proof reading, and small adjustments.
1.0	2017-10-08	Signicat	Version 1.0

2 References

ID	Reference	URL
ACABC	The Accredited Conformity Assessment Bodies' Council	http://www.acab-c.com/accredited-bodies/
ANSI/TIA	The Telecommunications Industry Association (TIA) ANSI/TIA-942-A Telecommunications Infrastructure Standard for Data Centers	http://www.tia-942.org/
BF	Basefarm is the ISO 27001 certified data center, which hosts most of Signicat's trusted services.	https://www.basefarm.com/en/
EIDAS	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	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
ETSI119312	Cryptographic Suites	https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.03.01_60/ts_119312v010301p.pdf
ETSI319401	ETSI EN 319 401: "General Policy Requirements for Trust Service Providers"	https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.02.01_60/en_319401v020201p.pdf
ETSI319421	ETSI EN 319 421: "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"	https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf
ETSI319422	ETSI EN 319 422: "Time-stamping protocol and time-stamp token profiles"	https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf
EU9546	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012

ID	Reference	URL
EUGDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April - *General Data Protection Regulation*	http://eur-lex.europa.eu/eli/reg/2016/679/oj
FIPS140	NIST's FIPS 140-2, level 3 certification for Utimaco CryptoServer Se-Series Gen2 HSM.	https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2814
ISO15408	ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security"	Not allowed to publish. Printed version available.
ISO19790	ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules"	Not allowed to publish. Printed version available.
ISO27001	ISO/IEC 27001:2013: "Information technology -- Security techniques -- Information security management systems -- Requirements"	https://www.iso.org/standard/54534.html
ISO27002	ISO/IEC 27002:2013: "Information technology - Security techniques - Code of practice for information security management".	https://www.iso.org/standard/54533.html
ITU460	Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions"	https://www.itu.int/rec/R-REC-TF.460/recommendation.asp?lang=en&parent=R-REC-TF.460-6-200202-I
PKI2010	Kravspesifikasjon for PKI i offentlig sektor (Norwegian)	https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/2010_kravspek_pki_norsk.pdf?id=2156639
RFC3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol	https://www.ietf.org/rfc/rfc3161.txt
TIER3	Uptime Institute, Data center certifications, Tier 3	https://en.wikipedia.org/wiki/Uptime_Institute
TSP001	Disclosure Statement & Terms and Conditions	https://www.signicat.com/certifications

3 Definitions and abbreviations

3.1 Definitions

Definition	Explanation
[DUAL] - Dual control	Regime for key management and possibly other vital operations, where the protection requirements are substantial. For Signicat TSA dual control means 2/6 – i.e. two out of six persons are needed to perform those operations.
Disclosure statement	set of statements about the policies and practices of a service that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements
Relying party	recipient of a time-stamp who relies on that time-stamp
Subscriber	legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations
Time-stamp	data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time
Time-stamp policy/ Practice statement (Signicat-P/PS, present document)	named set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements, and also description of the practices that the time-stamping service employs in issuing time-stamps
Time-stamping service	trust service for issuing time-stamps
Trust service	electronic service that enhances trust and confidence in electronic transactions

Definition	Explanation
TSA system	composition of IT products and components organized to support the provision of time-stamping services

3.2 Abbreviations

Abbreviation	Full form	Explanation
BIPM	Bureau International des Poids et Mesures	
BTSP	Best practices Time-Stamp Policy	Name used on the policy requirements and practice statement described in ETSI EN 319 421
CA	Certification Authority	
GMT	Greenwich Mean Time	
GNSS	Global Navigation Satellite System	Multiple global satellite navigation systems, e.g. GPS, GLONASS, Galilleo, BeiDou.
IERS	International Earth Rotation and Reference System Service	
ISMS	Information Security Management System	Set of policies and procedures implemented to systematically managing an organization's sensitive data in a way that minimizes risks and maximizes trustworthiness and reliability.
IT	Information Technology	
JV	Justervesenet	The Norwegian Time laboratory, part-of the BIPM network.
TAI	International Atomic Time	
TSA	Time-Stamping Authority	TSP providing time-stamping services using one or more time-stamping units

Abbreviation	Full form	Explanation
TSP	Trust Service Provider	Entity which provides one or more trust services
TST	Time-Stamp Token	Structure containing signed time-stamp over a datum. Based on RFC-3161
TSU	Time-Stamping Unit	Set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.
UTC	Coordinated Universal Time	Time scale based on the second as defined in Recommendation ITU-RTF.460-6 [ITU460]
UTC(k)	Coordinated Universal Time laboratory *k*	Time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns.

4 Time-stamp policy identification and accuracy

4.1 Accuracy

The policy defined by the present document has an **accuracy of 1 second, or better**.

4.2 Identification

The identifier of the time-stamp policy specified in the present document available in the documents information: ***OID: 2.16.578.1.46.1.14.3.#***

```
joint-iso-itu-t(2) country(16) norway(578) organisasjon(1) signicat(46)
policies(1) timestamp-policies(14) signicat-timestamp-policy-ETSI-319-421-
qualified(3) version (#)
```

Signicat will include this OID in each time-stamp object issued in accordance with this policy. The # indicates the version of this policy.

The underlying ETSI policy for time-stamp is:

BTSP: a best practices policy for time-stamp

OID: 0.4.0.2023.1.1

```
itu-t(0) identified-organization(4) etsi(0)
time-stamp-policy(2023)
```

```
policy-identifiers(1) best-practices-ts-policy (1)
```

5 Time-Stamp Policy and Practice

This section defines the policy requirements and their corresponding practices applicable for the Signicat TSA. The practices, which the Signicat TSA operates under are non-discriminatory.

5.1 Risk assessment

A policy that defines the methodology for risk assessment has been developed as part of Signicat's information security management system [ISMS]. Based on this, Signicat performs an annual risk assessment, which also covers the Signicat TSA.

During these risk assessments, each recognized risk is analyzed and evaluated taking into account business and technical issues. Appropriate treatment measures are then applied to ensure that the level of security is commensurate to the degree of risk.

The Signicat TSA is submissive to an external audit as required by the eIDAS regulation. Such audits are performed by an accredited external body [ACABC] every second year with an interim audit in the intermediate year.

5.2 Practice statement

The present document describes the applied practices for Signicat TSA.

5.3 Terms and conditions

The terms and conditions for using the Signicat TSA can be found in "*Signicat-TSP001*", the Disclosure Statement & Terms and Conditions.

5.4 Information security policy

Signicat has established an Information Security Management System, which covers processes, organizational units, locations, network and IT infrastructure for providing Signicat SaaS products, and forms the basis for Signicat's ISO-27001 certification.

The Signicat TSA operates in accordance with the ISMS.

5.5 TSA obligations

5.5.1 General

Signicat TSA will adhere to any additional obligations indicated in the issued time-stamp either directly or incorporated by reference.

Additionally, the following external parties have obligations towards Signicat TSA:

5.5.1.1 Basefarm

Ensure a reliable hosting environment for the Signicat TSA by providing:

- a secure physical environment by using separate, locked racks for the TSA with mounted alarms and controlled access;
- a duplicated setup at two different geographical locations;
- maintaining and adhering to ISO27001 compliant policies concerning how the TSA hosting is conducted;

5.5.1.2 PrimeKey

Provide a RFC3161 / RFC 5816 compliant software (SignServer), with all latest security patches applied.

Also provide continuous support for the aforementioned software (service agreement).

5.5.1.3 Utimaco

Provide FIPS-140-2, Level 3 certified HSMs.

Also provide updates of software running on the HSM (firmware), and

Assist in maintenance operations on the HSMs, such as battery changes (service agreement)

5.5.2 Obligations towards subscribers

Signicat TSA is obliged to operate according to the requirements stated in the Disclosure Statement & Terms and Conditions.

5.6 Information for relying parties

See the Disclosure Statement & Terms and Conditions.

5.7 Disclosure statement

See the Disclosure Statement & Terms and Conditions.

6 TSA management and operation

6.1 Introduction

The TSA management and operation are submissive to Signicat's ISMS policies and procedures to ensure that required security objectives are accomplished.

The provision of a time-stamp token in response to a request is at the discretion of Signicat depending on agreements with the subscriber and/or a reliant party.

6.2 Internal organization

Signicat TSA is fully owned and operated by Signicat AS – organization no. 989 584 022 and is a legal entity according to Norwegian law.

An internal TSA organization has been established within the Signicat's company organization. The TSA personnel have the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide time-stamping services.

6.3 Personnel security

Personnel involved with Signicat TSA, have been properly vetted and have received adequate training prior to taking on any task or responsibility within the TSA operation.

6.4 Asset management

Signicat manages its assets according to the ISMS. This implies that a complete inventory of all important assets is maintained. Each asset is appropriately classified and protected consistent with the conducted risk assessment.

6.5 Access control

Access control is strictly controlled and in accordance with the ISMS. The principle of least privilege is applied, which means that users and systems only get access to parts/areas/systems they need to fulfill their tasks.

Users are uniquely identified and there is a formal process of registration and de-registration. Users are also accountable for their actions.

To ensure that only authenticated users with sufficient permissions can access the TSA system, two factor authentication and dual control [DUAL] have been deployed.

The TSA is also set up on a separate network segment and shielded against alien communication attempts.

6.6 Cryptographic controls

6.6.1 General

To ensure consistent and secure management of cryptographic controls, these are always selected and used in accordance with Signicat ISMS.

6.6.2 TSU key generation

The following apply to the key generation process.

a) The generation of the TSU's signing key(s) is undertaken in a physically secured environment (as per clause 6.8) by personnel in trusted roles (as per clause 6.3) under dual control. The personnel authorized to carry out this function is limited to those required to do so.

b) The generation of the TSU's signing key(s) is carried out within a hardware security module - HSM, which is a trustworthy system subject to the FIPS 140-2 level 3 security standard [FIPS140].

c) The TSU key generation algorithm is **NIST P-256 EC-DSA**, the resulting signing key length is **256 bits**, and the signature algorithm is **sha256-with-ecdsa**. This is in accordance with both the ETSI TS 119 312 [ETSI119312] and the Norwegian national requirements for cryptography within the public sector [PKI2010].

d) The TSU's signing key will only be duplicated into other secure cryptographic devices to support transparent failover and/ or load balancing – typically when high-

availability (HA) is a demand. The duplication has the nature of a backup-restore sequence and is carried out under at least dual control by trusted roles authorized to do this.

e) If the private key is duplicated as defined in d), then it will be the same public key that is associated with every duplicate. I.e. this public key will also be loaded into any other HSM holding a copy of the private key. This procedure is carried out as a part of the operation referenced in d).

f) The TSU will only have one signing-key active at a time.

6.6.3 TSU private key protection

The Signicat TSA ensures that TSU private keys remain confidential and keep their integrity by submitting to the following:

a) The TSA signing private key is held and used within a secure cryptographic device, which meets the requirements identified in FIPS PUB 140-2, level 3 [FIPS140].

b) The backup, copying, storing, and restoring of TSU private keys are carried out under at least dual control by trusted roles authorized to do this.

c) Any backup of the private key material is encrypted and protected by splitting the decryption key over multiple cards to enforce dual control upon restoring. The backup parts are held by multiple people in trusted roles authorized to do this. The encrypted backups' confidentiality and integrity are protected.

6.6.4 TSU public key certificate

Signicat TSA guarantees the integrity and authenticity of the TSU public key certificate as follows:

1) TSU signature verification (public) keys are published through internal channels to relying parties and distributed to the trusted national supervision body – NKOM – for inclusion on the EU trust list.

2) No time-stamps will be issued before its public key has been loaded into the TSU and has been verified as valid.

6.6.5 Rekeying TSU's key

The validity period of TSU's certificate is no longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose (see clause 6.6.2c).

6.6.6 Life cycle management of signing cryptographic hardware

The following requirements are fulfilled:

a) Time-stamp signing cryptographic hardware has not been tampered with during shipment.

b) Time-stamp signing cryptographic hardware has not been tampered with while stored.

c) Installation, activation and duplication of TSU's signing keys within cryptographic hardware have only been carried out under at least dual control by people in trusted roles authorized for this.

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

6.6.7 End of TSU key life cycle

Signicat TSA specifies expiry dates for the TSU's private keys, based on recommendations defined in *"ETSI TS 119 312 - Cryptographic Suites"* [ETSI119312].

The private signing keys are not used beyond the end of their life cycle through the provision of technical and procedural controls. In particular:

a) Signicat has operational procedures in place, which ensure that a new key is put in place and activated when a TSU's key expires.

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

6.7 Time-stamping

6.7.1 Time-stamp issuance

An issued time-stamp conforms to the time-stamp profile as defined in *"ETSI EN 319 422 - Time-stamping protocol and electronic time-stamp profiles"* [ETSI319422], is issued securely, and contains the correct time within the declared accuracy.

The following apply:

a) The time values the TSU uses in the time-stamp is traceable to the UTC(JV) laboratory through the NTP server ntp.justervesenet.no.

b) The time included in the time-stamp is synchronized with UTC(JV) within the declared accuracy.

c) If the time-stamp provider's clock is detected as being outside the declared accuracy, then no time-stamps will be issued.

d) The time-stamp and the datum are signed using a key generated exclusively for this purpose.

e) The time-stamp generation system will not issue any time-stamps when the end of the validity of the TSU private key has been reached.

6.7.2 Clock synchronization with UTC

To ensure that the synchronization with UTC is valid, an independently running application (TimeMonitor) is monitoring the synchronization between the TSU clock and the setup TAs,

and its main purpose is to prevent the TSA from issuing time-stamps outside the declared accuracy.

The following apply:

a) The calibration of the TSU clocks is carried out by synchronizing with a local NTP server, which acts as a proxy for the external time authorities (TA). The TAs in use are the NTP service from Justervesenet [JV] and Basefarm's Stratum 1-time source, which is a GNSS synchronized clock [BF].

b) The declared accuracy of the time-stamps issued is 1 second.

c) Undetected changes are prevented by monitoring the TSU clock synchronization with the local NTP server's time.

d) No time-stamps will be issued if time has drifted outside declared accuracy.

e) The clock synchronization is maintained when a leap second occurs.

f) The change to take account of the leap second will occur during the last minute of the day when the leap second is scheduled to occur. A record is maintained of the exact time (within the declared accuracy) when this change occurred.

6.8 Physical and environmental security

The physical and environmental maintenance of the operational infrastructure has been outsourced to the infrastructure service provider, Basefarm [BF].

Basefarm is an ISO 27001 certified organization and employs security controls in accordance with that standard. This means that proper entry controls, protection against external and environmental threats, cabling security, and maintenance of equipment are in place.

The Signicat TSA is isolated within a separate, locked cabinet. This includes both the physical server running the TSA software and the utilized HSM(s) for cryptographic artefacts.

This means that only authorized personnel in designated roles are able to perform remote management of Signicat TSA.

The physical and environmental security is in accordance with the Signicat ISMS.

6.9 Operation security

Signicat has as part of its ISMS, followed the guidance of ISO27002 to uphold the operation security. This ensures that:

- Operating procedures are thoroughly documented and kept up-to-date.
- Change management is strictly controlled.
- Capacity management is in place.
- Development, test, and operational environments have been separated.
- The TSA is protected against malware and other unauthorized access.

- Backup and logging are conducted in accordance with requirements imposed by relevant laws and regulations.
- Operational environment is located in a rating 3 certified ANSI/TIA data center [ANSI] to secure availability and redundancy.

The TSA has undergone a risk assessment with mitigations, prior to becoming operational.

6.10 Network security

6.10.1 Security zones

Signicat's systems are segmented into security zones (high, medium, low, and none) based on risk assessments considering the functional, logical, and physical (including location) relationship between the systems and services. The same security controls are applied to all systems co-located in the same zone.

Communications across different zones and/or distinct trustworthy systems is only possible for authorized users in designated roles, using two-factor authentication, over encrypted channels.

6.10.2 Penetration tests

Signicat regularly, and at least annually, undergoes penetration tests on its network, application layers, and web service layer to detect any security threats. Identified threats are registered and remedies decided during the retrospective of the test. Such penetration tests are carried out by an external entity with the required competence to do so.

6.10.3 Vulnerability scans

Signicat regularly, and at least annually, performs vulnerability scans on public and private IP addresses. Such tests are always performed by personnel with the necessary skills, tools, proficiency, code of ethics, and independence to produce reliable results. Detailed procedures have been developed for these tests to ensure that proper coverage is achieved and that correct methodology is applied.

6.11 Incident management

Signicat's incident management follows the guidelines from the ISO 27001/2 specifications.

This means that procedures are in place to manage the full life cycle of all incidents.

Incident Management includes any event which disrupts, or which could disrupt a service. This includes events that are communicated directly to users, either through the Service Desk or through an interface from Event Management to Incident Management tools.

Incidents can also be reported and/or logged by technical staff; if they notice something untoward with a hardware, network or software component they may report or log an incident and refer it to the Service Desk. This does not mean that all events are Incidents. Many classes of events are not related to disruptions at all, but are indicators of normal operation or are simply informal.

Although both incidents and service requests are reported to the Service Desk, this does not mean that they are the same. Service requests does not represent a disruption to the agreed upon level of service, but are a way of meeting the customer's need and may be addressing an agreed target in an SLA. Service requests are dealt with in the Request fulfilment process.

The main purpose of incident management is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the agreed upon levels of service quality are maintained.

Any critical security breach will be notified to the national supervisory body (NKOM) as soon as possible, and at least within 24 hours. Relevant information will also be submitted to relying parties.

Any critical vulnerability not previously addressed, will be processed within a period of 48 hours after its identification. This means that if it is cost effective given the impact, a plan will be created and implemented to mitigate the vulnerability, or the factual basis for not doing so will be documented.

6.12 Collection of evidence

Signicat has established procedures to ensure proper handling of collection of evidence, analysis, identification, etc. in case of security incidents.

To make such evidence available in the first place, core processes are carefully audited, and logs of relevant events are maintained.

Specifically, for the TSA service:

Time-stamp issuance

a) Records concerning all time-stamp issuances are logged and kept for 5 years.

b) Records concerning all operations performed on the SignServer are logged in an audit log, and entries are signed.

TSU key management

c) Records concerning all events relating to the life-cycle of TSU keys are logged.

d) Records concerning all events relating to the life-cycle of TSU certificates are logged.

Clock Synchronization

e) Records concerning all events relating to synchronization of a TSU's clock to UTC are logged. This include information concerning normal re-calibration or synchronization of clocks used in time-stamping.

f) Records concerning all events relating to detection of loss of synchronization are logged.

6.13 Business continuity management

Disasters may come in many forms, but common to all of them is disrupting the normal level of service. In such situations, it is crucial to restore the normal level of service as quickly as possible, without compromising integrity or reliability.

Signicat has developed a business continuity plan – hereinafter BCP - to make disaster recovery possible. Multiple scenarios have been identified, some of which were simulated during training sessions. Mitigations for each scenario are in place.

A part of the BCP also covers TSA specific situations such as 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. Such situations will lead to a cease in time-stamp issuance and that reliant parties are informed about the situations, while a recovery path is being worked out.

6.14 TSA termination or change of provisioning

Signicat has developed a termination plan to be executed if a decision is made to terminate the TSA service.

One intention with this termination plan is to assist subscribers/reliant parties in carrying over the time-stamping service to an alternative TSA with as little disturbance as possible. Also, retention of logs as specified in the Disclosure Statement & Terms and Conditions, beyond the time of termination, will also be conducted.

In case of changes in provisioning, which will make deviations from the time-stamp policy, a similar procedure will be executed to inform affected parties and supervision bodies.

6.15 Compliance

Signicat TSA adheres to applicable law at all times, and also ensures compliance with the following:

a) EU Regulation 910/2014 - EIDAS

b) EN 319 421 - Policy and Security Requirements for Trust Service Providers issuing Time-Stamps [ETSI319421]

c) ETSI EN 319 422 - Time-stamping protocol and electronic time-stamp profiles for cryptographic controls [ETSI319422]

d) RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol [RFC3161]

This compliance is assessed annually by an eIDAS accredited body.

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

7.1 TSU public key certificate

Signicat TSA uses a self-signed public key certificate, which is issued under the same strict regime as other key operations within the Signicat TSA realm.

The following apply:

a) The Public key certificate equals clause 6.6.4 Public key certificate

b) Rekeying equals clause 6.6.5 Rekeying TSU's key

c) End of key life cycle equals clause 6.6.7 End of TSU key life cycle

d) The validity of the private keys is no longer than the end of the validity of the related certificate.