Sectigo eIDAS qualified Time Stamping Authority (TSA) Policy & Practice Statement

Sectigo (Europe) S.L.
Version 1.0.7
Effective: December 3, 2020
Rambla Catalunya, 86 3 1,
08008 Barcelona, Spain
ww.sectigo.com

Copyright Notice

Sectigo (Europe) S.L.
Rambla Catalunya, 86 3 1,
08008 Barcelona, Spain

Contents

INTRODUCTION

Sectigo is a Trust Services Provider (TSP) that issues trusted digital Time Stamps tokens to entities including private and public companies and individuals in accordance with this Sectigo Time Stamping policy and practice statement.

Sectigo runs a qualified time-stamping service providing qualified time-stamp tokens according to the EU regulation 910/2014 of 23 july 2014 on electronic identification and trust services for electronic transactions in the European Single Market, repealing the directive 1999/93/EC from 13 december 1999, commonly named eIDAS. Sectigo conforms to the requirements established in Article 42 of Regulation (EU) 910/2014.

This Timestamping Policy and Practice Statement (TSPPS) applies to the eIDAS Qualified Timestamping Services of Sectigo.

This TSPPS is an auxiliary service, and the overall Sectigo Certification Practice Statement (CPS) according to eIDAS determines its terms and conditions.

This document states only additional timestamping specific practices according to eIDAS.

In its role as a TSP, Sectigo performs functions associated with public key operations that include receiving requests, issuing, etc. for users within the Sectigo Public Key Infrastructure (PKI).

1. Scope

This document describes the Time stamping policy and practice statement, specifying the general policies and processes to create and issue time stamps and the additional services associated.

Specific technical details and processes are specified in this document in addition to the general Sectigo´s CPS according to eIDAS.

For issuance of qualified time-stamps tokens Sectigo conforms to the ETSI standard EN 319 421 *"Policy and Security requirements for Trust Service Providers issuing Time-Stamps".* In addition, Sectigo also follows the ETSI standard EN 319 422 *"Time-stamp protocol and time-stamp token profiles"* for the definition of the time-stamp profile.

This document is only one of a set of documents relevant to the provision of Time Stamping Services by Sectigo and that the list of documents contained in this clause are other documents that this document will from time to time mention, although this is not an exhaustive list.

This document, related agreements and policies referenced within this document are available online at *www.sectigo.com/legal*.

2. References

For the purposes of the present document, the standards referenced in the CPS according to eIDAS and the following apply:

ETSI EN 319 421 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time Stamps

ETSI EN 319 422 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

Recommendation ITU-R TF.460-6 - Standard-frequency and time-signal emissions

RFC 1305 - Network Time Protocol

3. Definitions and abbreviations

3.1. Definitions

For the purposes of the present document, the definitions given in the CPS according to eIDAS and the following apply:

Term	Definition
Coordinated Universal Time	time scale based on the second as defined in Recommendation ITU-R TF.460-6
Network Time Protocol	is a networking protocol for clock synchronization between computer systems over packet-switched, variable latency data networks.
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-Stamping Authority (TSA)	TSP providing time stamping services using one or more time-stamping units
Time-stamping service	Trust service for issuing time-stamps
Trust service	Electronic service that enhances trust and confidence in electronic transactions
TSA Policy and Practice Statement	statement of the policy and practices that a TSA employs in issuing timestamps
Time-Stamping Unit (TSU)	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

3.2. Abbreviations

For the purposes of the present document, the acronyms given in the CPS according to eIDAS and the following apply:

Acronym	Full Name
NTP	Network Time Protocol
TSA	Time Stamping Authority
TSU	Time Stamp Unit
TSPPS	Time Stamp Policy & Practice Statement
UTC	Coordinated Universal Time

4. General Concepts

4.1. General policy requirements concepts

This TSPPS considers the ETSI EN 319 401 as a reference for generic policy requirements common to all classes of trust service providers service.

These 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 this TSPPS 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. Time-stamping services

The provision of time-stamping services is broken down in this document into the following component services for the purposes of classifying requirements:

- Time-stamping provision: This service component generates time-stamps.
- Time-stamping management: This service component monitors and controls the operation of the time-stamping 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 time-stamping provision service.

4.3. Time-Stamping Authority (TSA)

A Trust Service Provider (TSP) providing time-stamping services to the public, is called the Time-Stamping Authority (TSA). The TSA has overall responsibility for the provision of the time-stamping services identified in clause 4.2. The TSA has responsibility for the operation of one or more TSUs which creates and signs on behalf of the TSA.

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 this TSPPS are met.

The CAs issue certificates to the Time Stamp Units of the TSA. These certificates allow the relying parties to identify the TSA.

This service is available at *http://timestamp.sectigo.com/qualified*

The TSU clocks are supervised locally by the reference time servers. These servers are autonomous and benefit from a synchronization procedure with the UTC(k) references.

4.4. Subscriber

The Subscriber is the natural person or legal person who owns the time stamp produced by the TSA. The Subscriber is the natural or legal person who accepts the terms and conditions defined in the Subscriber Agreement.

4.5. Time-stamp policy and TSA practice statement

This clause explains the relative roles of timestamp policy and TSA practice statement. It places no restriction on the form of a timestamp policy or practice statement specification.

A timestamp policy is a form of Trust Service Policy as specified in ETSI EN 319 401 applicable to trust service providers issuing timestamps.

TSA Practice Statement is a form of Trust Service Practice Statement as specified in ETSI EN 319 401 applicable to trust service providers issuing timestamps.

This document specifies the timestamp policy and the practice statement for the Sectigo TSA.

5. Time-stamp policies

5.1. General

This document defines a set of rules adhered to by Sectigo when issuing timestamps, supported by public key certificates, with an accuracy of one (1) second or better against UTC.

5.2. Identification

This document is the Sectigo eIDAS qualified Timestamping Policy and Practice Statement.

It defines the commitments of the TSA in terms of security and organization of the processes for the issuance and management of timestamps issued by these TSAs.

The identifier of the certificate policy in the TSA certificate(s) specified in the present document is: 1.3.6.1.4.1.6449.1.2.1.9

By including this object identifier itu-t(0) identified-organization(4) etsi(0) time stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1) in a time-stamp token, Sectigo claims conformance to this time-stamp policy.

When Sectigo declares a time stamp as qualified following EU regulation No. 910/2014 (eIDAS), the certificate for signature validation is issued under the certificate policy declared in ETSI EN 319 411-2, which also incorporates ETSI requirements EN 319 411-1.

5.3. User community and applicability

This document is aimed at meeting the requirements of timestamps for long term validity but is generally applicable to any use which has a requirement for equivalent quality.

This document may be used for public timestamping services or timestamping services used within a closed community.

6. Policies and practices

6.1. Risk assessment

In common with most organisations operating in an increasingly information and technology dependent environment, Sectigo, and its corporate subsidiaries (collectively referred to as "Sectigo") is often exposed to potential information security threats which, should they result in an incident, have the capability to cause Sectigo direct financial loss, operational disruption, and damage to the company's reputation. Sectigo regards its information as a highly valuable asset and as a result, our information and processing systems are critical to our business and need to be protected appropriately.

Information may exist in a variety of forms whether electronic, paper and other types of media, and carries with it important, and at times, critical details regarding both the day-to-day and strategic activities of Sectigo's businesses and that of our customers and trading partners. The loss, corruption or theft of information or supporting business systems could have a serious impact on the integrity of Sectigo's business activities and reputation.

This Risk Management Framework is defined for all assets and activities relating to Sectigo business processes.

Sectigo's approach to risk management consists of two areas:

- Risk Assessment: An assessment of the threats to, impacts on, and the vulnerabilities of assets and the likelihood of their occurrence.
- Risk Treatment: Process of selecting and implementing security controls in order to reduce the risks identified in the risk assessment to an acceptable level.

Sectigo performs a full Risk Assessment across the organisation on an annual basis.

6.2. Trust Service Practice Statement

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

The security policies and controls are reviewed regularly by an independent body, whilst trained trustworthy personnel check the adherence of the security controls to the policies.

Additionally, for compliance to ETSI EN 319 421 the following measures have been implemented

6.2.1. Timestamp format

The issued timestamp tokens by Sectigo are compliant to RFC 3161 and ETSI EN 319 422. The service issues RSA 4096 timestamps that uses the SHA384 hash algorithm.

See Annex B for additional information.

6.2.2. Accuracy of the time

As a reliable source of time, Sectigo has a small subset of our machines talking to Stratum 1 sources and also Stratum 2 or 3 for reference.

The timestamping service uses this time signal together with an NTP Time Monitor for monitoring time.offset and time.drift from a set of UTC(k) laboratory NTP servers. With that setup the timestamping service reaches an accuracy of the time well under +/-1s with respect to UTC.

Everything runs ntpd, which picks the right server and keeping the time in sync.

Sectigo uses NTP sources from national time providers, universities and specific projects such as the NTP pool project.

6.2.3. Obligations of the subscriber

Please see the subscriber agreement for additional information.

6.2.4. Obligations of relying parties

Relying parties use PKI services in relation with various Sectigo certificates or timestamps for their intended purposes and may reasonably rely on such certificates or timestamps.

Relying parties are subject to the stipulations of the relying party agreement.

6.2.5. Verification of the Timestamp

Timestamp verification includes the following

6.2.5.1. Verification of the timestamp issuer

A TSA that uses appropriate electronic certificates issues the timestamp. The public keys of the used certificates, including the TSU and CA certificates, are published to enable a verification that the timestamp has been signed correctly by the TSA.

6.2.5.2. Verification of the timestamp revocation status

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

6.2.6. Compliance with applicable law

This TSPPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders, including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. Sectigo complies with all applicable laws, rules, regulations, ordinances, decrees, and orders when providing services pursuant to this TSPPS.

Specifically, Sectigo TSA complies with:

- eIDAS regulation
- ETSI EN 319 401, 319 421 and 319 422
- RFC 3161

6.2.7. Service availability

Sectigo has implemented the following measures to ensure availability of the service:

- Redundant setup of IT Systems, including HSM infrastructure, in order to avoid single points of failure
- Redundant high-speed internet connections in order to avoid loss of service
- Use of uninterruptable power supplies

Sectigo aims to provide 99,9% service availability per year.

6.3. Terms and conditions

Sectigo publishes this TSPPS, terms and conditions, the Relying Party Agreement and Subscriber Agreements in the Repository.

Information regarding limitations of the service, terms and conditions can be checked under the terms of use document.

6.4. Information security policy

Sectigo has implemented an information security policy which all employees must adhere to. The information security policy is reviewed on a regular basis and when significant changes occur.

6.5. TSA obligations

6.5.1. General

The TSA is responsible for:

- The compliance with this TSPPS and its internal or published policies and procedures.
- The compliance with applicable laws and regulations.
- Providing infrastructure and certification services, including but not limited to the establishment and operation of the Sectigo Repository and web site for the operation of PKI services.
- Providing trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.

- Providing prompt notice in case of compromise of its Private Key(s).
- The compliance of the timestamps with the TSP
- The compliance of all different components of the TSA and the related controls with the principles of security
- Providing support to Subscribers and relying parties as described in this TSPPS.
- Making available a copy of this TSPPS and applicable policies to requesting parties.

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.

6.6. Information for relying parties

The obligations of relying parties are covered in the relying party agreement. In addition, the relying party shall do the following:

- 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;
- take into account any limitations on the usage of the time-stamp indicated by the time-stamp policy
- take into account any other precautions prescribed in agreements or elsewhere.

7. TSA management and operation

7.1. Introduction

Sectigo has implemented information security policies and operational procedures to maintain the security of the service.

Sectigo may charge subscriber fees for some of the services it offers.

Sectigo retains its right to affect changes to such fees.

7.2. Internal organization

For the proper operations of the timestamping service, Sectigo maintains non-disclosed documentation that specifies all operational controls concerning personnel security, access controls, risk assessment etc. These internal documents are used by independent bodies to confirm compliance of the service against ETSI EN 319 421/eIDAS.

- Legal entity: The TSA is provided by Sectigo.
- Information security management and quality management of the service is carried out within the security concept of the service.
- Sectigo operates its TSU from a data center, which provides the basic infrastructure (Internet access, electricity, physical security, etc.) of the trust service.

7.2.1. Contact person

The Sectigo policy authority may be contacted at the following address:

Sectigo Policy Authority
3rd Floor, Building 26 Exchange Quay, Trafford Road
Salford, Greater Manchester, M5 3EQ, United Kingdom
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767
URL: *https://www.sectigo.com*
Email: *legalnotices@sectigo.com*

7.3. Personnel security

Access to the secure parts of Sectigo's facilities is limited using physical and logical access controls and is only accessible to appropriately authorized individuals filling trusted roles for which they are properly qualified and to which they have been appointed by management.

Sectigo requires that all personnel filling trusted roles are properly trained and have suitable experience before being permitted to adopt those roles.

7.3.1. Qualifications, experience, and clearance requirements

Consistent with this TSPPS, Sectigo follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties.

7.3.2. Background check procedures

All trusted personnel have background checks before access is granted to Sectigo's systems. These checks may include, but are not limited to, verification of the individual's identity using a government issued photo ID, credit history, employment history, education, character references, social security number, criminal background, and a Companies House cross-reference to disqualified directors.

7.3.3. Training requirements

Sectigo provides suitable training to all staff before they take on a trusted role should they not already have the complete skill-set required for that role. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached.

7.3.4. Retraining frequency and requirements

Personnel in Trusted Roles have additional training when changes in industry standards or changes in Sectigo's operations require it. Sectigo provides refresher training and informational updates sufficient to ensure that trusted personnel retain the requisite degree of expertise.

7.3.5. Job rotation frequency and sequence

Sectigo ensures that any change in the staff will not affect the operational effectiveness of the service or the security of the system.

7.3.6. Sanctions for unauthorized actions

Any personnel, who, knowingly or negligently, violate Sectigo's security policies, exceed the use of their authority, use their authority outside the scope of their employment, or allow personnel under their supervision to do so may be liable to disciplinary action up to and including termination of employment. Should the unauthorized actions of any person reveal a failure or deficiency of training, sufficient training or retraining will be employed to rectify the shortcoming.

7.3.7. Independent contractor requirements

Once the independent contractor completes the work for which it was hired, or the independent contractor's employment is terminated, all access rights assigned to that contractor are removed as soon as possible and within 24 hours from the time of termination.

7.3.8. Documentation supplied to personnel

The selection of documentation supplied to Sectigo personnel is based on the role(s) they are to fill. Such documentation may include a copy of this TSPPS, the eIDAS regulation and other technical and operational documentation necessary to maintain Sectigo's TSA operations.

7.4. Asset management

Management of Sectigo's assets will be based on their classification in terms of their value, legal requirements, sensitivity and criticality to Sectigo. Classifications and associated protective controls for assets should take account of business needs for sharing and restricting information and the business impacts associated with such needs.

Assets are broken down into the following categories:

- Information Assets – Information relating to the assets, held on paper, databases or data files. This includes, but is not limited to, system documentation, user manuals, training material, operational or support procedures, continuity plans, backup files, archived information.
- Software Assets – Application software, system software, development tools and system utilities.
- Physical Assets – Computer equipment, removable media, communications equipment (routers, switches etc.) and other technical equipment.
- Services – Communication/Internet services.
- Personnel – All Sectigo employees, contractors and third-party personnel.

7.5. Access control

Different security layers with respect to physical access and logical access ensure a secure operation of the timestamping service.

Access to Sectigo's information, information processing facilities and business processes must be controlled based on business and security requirements. This policy will consider:

- User Access Management & Responsibilities.
- Network Access Management.
- Operating System, Application & Database Access Management.

7.6. Cryptographic controls

Sectigo uses several private keys to fulfil its service. One private key pair is used to issue the public key timestamp certificates that are used within the TSUs. One or more private key pair is or are used within the TSU to issue the timestamp.

All private keys are stored in a FIPS 140-2 Level 3 or QSCD listed hardware security module (HSM).

7.6.1. TSU Key pair generation

For TSU key pairs created under this TSPPS, Sectigo prepares and follows a key generation script.

Sectigo's keys are generated & held in Hardware Security Modules (HSM)s that are compliant, as a minimum, to FIPS 140-2 level 3, or are listed as QSCD.

All key operations are performed within the security of the HSM. All keys that are exported from the HSM are encrypted with a suitable encryption algorithm with the encryption key generated by the HSM.

Access to these keys is restricted to authorized, trusted personnel of Sectigo. Key data must be stored securely at all times unless attended by authorised personnel of Sectigo.

Access to the cryptographic operation software on the HSM is controlled, at a minimum, through the use of multi person Smart Cards & PINs, which must be entered/presented before any key operations may be performed. Access to the Smart Cards & PINs is restricted to authorized Sectigo officers under multi person control (Sectigo settings require N from M cards to be present). Authorized Sectigo personnel with access to Smart Cards & PINs is logged.

Sectigo uses SHA384 in the responses of the time-stamps.

These key operations, for example, key generation, backup & recovery that involve an HSM are performed in a key ceremony. All key ceremonies are performed in a secure, controlled area. During the ceremony, at least two authorised Sectigo personnel are present at all times.

No other persons are allowed in the secure area during the key ceremonies to protect against information loss through tampering or overseeing. All visible 'Sensitive' information is kept to a minimum at all times during the key ceremonies.

All key ceremonies are performed on a computer with a verified clean installation of the operating system that is isolated from all computer networks. The cryptographic operation control software shall be a fresh install and verified to be operating correctly before use.

All media created from a key ceremony must be classified and stored in accordance with this classification.

All obsolete media from a key ceremony must be disposed of in a secure manner i.e. destruction, at the end of the key ceremony, or within a maximum period of 1 working day. All media that is not fully disposed of immediately must be partially destroyed and securely stored until full disposal takes place.

7.6.2. TSU private key protection

The Sectigo infrastructure uses trustworthy systems. A trustworthy system is computer hardware, software and procedures that provide an acceptable resilience against security risks, provide a reasonable level of availability, reliability and correct operation, and enforce a security policy.

7.6.2.1. Cryptographic module standards and controls

Sectigo securely generates and protects its own private key(s), using a trustworthy system certified to FIPS 140-2 Level 3 or higher or listed as QSCD, and takes necessary precautions to prevent the compromise or unauthorized usage of it.

The TSA ensures the security of these modules throughout their life cycle. In particular, the TSA implements the procedures required for:

- ensuring their integrity during their transport from the supplier
- ensuring their integrity during their storage before the key ceremony
- ensuring that the operations of activation of the signature keys are conducted under the control of two staff members having trusted roles
- ensuring that they are in a proper functional state
- ensuring that the keys that they contain are destroyed after being decommissioned.

7.6.2.2. Private key backup

TSUs private keys are backed up accordingly.

7.6.2.3. Private key storage on cryptographic module

Private Keys are generated and stored inside Sectigo's Hardware Security Modules (HSMs), which have been certified to at least FIPS 140-2 Level 3 or listed as QSCD.

7.6.3. Public key certificate

Sectigo guarantees the integrity and authenticity of the TSU signature verification (public) keys as follows:

- TSU signature verification (public) keys are available to relying parties in publicly available certificates. The certificates can be found on the Setigo´s website at *https://sectigo.com/legal*

- The TSU does not issue a 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, Sectigo verifies that this certificate has been correctly signed (including verification of the certificate chain to its trusted certification authority).

7.6.4. Rekeying TSU keys

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

Once a year or when significant changes occur, Sectigo's Policy Authority verifies any cryptographic algorithms used within the TSU against the algorithms recognized as suitable

7.6.5. Life cycle management of signing cryptographic hardware

All cryptographic hardware will be inspected during the commissioning process to ensure conformity to supply and no evidence of tampering found nor while stored.

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.

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.

7.6.6. End of TSU key life cycle

The validity of all used private keys never exceeds the validity of certificates issued using those private keys.

After expiration of the private keys, the private keys within the cryptographic hardware are destroyed in a manner such that the private keys cannot be retrieved or used anymore.

7.7. Time-stamping

The Sectigo Qualified Timestamping Service issues qualified timestamps which conform to the timestamp profile defined in ETSI EN 319 422.

7.7.1. Clock synchronization

Sectigo´s TSA is connected to some UTC(k) laboratories as their primary time source and all are stratum 1. These include laboratories around the world, such as the NIST (US), the NICT (JP), the BEV (AT) and the AOS (PL). Sectigo is including more NTP endpoints from these UTC(k) laboratories from time to time to get a better and synchronized accuracy of the time.

The TSA guarantees that its clock is synchronized with UTC time throughout NTP with a declared accuracy of one second.

More particularly:

1. the calibration of every TSU clock is maintained in such a way that the clocks cannot drift beyond the declared accuracy;

2. the clocks of the TSUs are protected from threats related to their environment, which could lead to a desynchronization with the UTC time greater than the declared accuracy;

3. the TSA guarantees that the internal clock drift of a TSU beyond the declared accuracy will be detected.

4. if the clock of a TSU is detected as not being within the declared accuracy, timestamps are no longer generated;

5. the TSA guarantees that the clock synchronization is maintained when a leap second is scheduled, as notified by the appropriate body. The change to take into account the leap second is carried out during the last minute of the day on which the leap second is scheduled. A record is made of the exact time (as per the declared accuracy) when this change is made.

7.8. Physical and environmental security

All sites operate under a security policy designed to provide reasonable assurance of the detection, deterrence and prevention of unauthorized logical or physical access to TSA related facilities.

7.8.1. Site location and construction

Sectigo operates worldwide, with separate operations, research & development and server operation sites. Physical barriers are used to segregate secure areas within buildings and are constructed to extend from real floor to real ceiling to prevent unauthorized entry. External walls of the site are of solid construction.

7.8.2. Physical access

Card access systems are in place to control and monitor access to all areas of the facility. Access to the Sectigo physical machinery within the secure facility is protected with locked cabinets and logical access controls. Security perimeters are clearly defined for all Sectigo locations. All of Sectigo's entrances and exits are secured or monitored by security personnel, reception staff, or monitoring/control systems.

7.8.3. Power and air conditioning

Sectigo secure facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating/air ventilation systems are used to prevent overheating and to maintain a suitable humidity level.

7.8.4. Water exposures

Sectigo has made reasonable efforts to ensure its secure facilities are protected from flood and water damage. Sectigo has personnel located on-site to reduce the extent of damage from a flood and any subsequent water exposure.

7.8.5. Fire prevention and protection

Sectigo has made reasonable efforts to ensure its secure facilities are protected from fire and smoke damage (fire protection is made in compliance with local fire regulations). IT equipment is located to reduce the risk of damage or loss by fire. The level of protection from fire reflects the importance of the equipment.

7.8.6. Media storage

Amongst other ways, Sectigo protects media by storing it away from known or obvious fire/water hazards. Media is also backed up on-site and off-site.

7.8.7. Waste disposal

Sectigo disposes of waste in accordance with industry best practice. Sectigo has procedures in place to dispose of all media types, including, but not limited to, paper documents, hardware, damaged devices, and read only optical devices. These procedures apply to all information classification levels, with the method of disposal dependent on the classification.

7.8.8. Off-Site backup

Sectigo backs up much of its information to a secure, off-site location that is sufficiently distant to escape damage from a disaster at the primary location. The infrastructure team, taking into account the criticality and security requirements of the information, determines the frequency, retention, and extent of the backup.

Backup of:

- critical TSA software is performed weekly and is stored offsite.
- critical business information is performed daily and is stored offsite. Access to backup servers/media is restricted to authorized personnel only.
- media is regularly tested through restoration to ensure it can be relied on in the event of a disaster.

Backup servers/media is appropriately labeled according to the confidentiality of the information.

7.9. Operation security

Sectigo employs approved policies and procedures to ensure that all information and information processing facilities are operated consistently, without compromising the security of operations or services.

This TSPPS will consider the following aspects:

- Operational procedures and responsibilities.
- Segregation of duties.
- Capacity management.
- Separation of development, testing and operational environments
- Control of operational software
- Security of system documentation.
- Physical media in transit.
- Publicly available information.
- Information systems audit consideration.

7.9.1. Operational Procedures and Responsibilities

- Documented operating procedures shall be planned, developed, authorised, documented and made available to all users who need them.

- Documented procedures shall be prepared for system activities associated with information processing and communication facilities, for example, backup, equipment maintenance, media handling, media classification, access control, physical security etc.

- Operating procedures shall be treated as formal documents with all changes authorised by management.

- Operating procedures shall be documented in an operations manual. The operations manual should contain the following topics:
    - Detailed architecture overview of all systems and applications
    - Overview of all interfaces;
    - Responsibilities and deputy regulations for administrative tasks;
    - Change management process;
    - Configuration management;
    - Vulnerability/patch management;
    - Capacity management;
    - Backup and recovery;

  - Logging scheme;
  - Escalation process;
  - User management.

- Critical tasks where the four-eyes principle may be necessary shall be identified, documented, and applied when deemed necessary. Typical examples include:
  - Remote maintenance by external parties;
  - Highly privileged Active Directory, Root administration;
  - Renewal of root/intermediate certificates.

- All systems and applications shall be configured securely. Sectigo's Information Security Policies, along with any other internal regulations, takes precedence over best practices or industry standards.

7.9.2. Segregation of Duties

- Duties and responsibilities of personnel within Sectigo shall be organised so that it is not possible for one person to both authorise and undertake a change to production systems, infrastructure or data.

- Physical access to the certificate manufacturing facilities and equipment shall be limited to authorised personnel and operated under at least dual custody.

- Administration, logging and audit duties of any single system within Sectigo shall be organised so that no one person is responsible for both the administering and audit tasks.

- Personnel in systems development may not authorise code changes to the production environment or sign off testing of their own code.

7.9.3. Capacity Management

- A capacity management process to ensure adequate capacity of IT systems and infrastructure shall be documented and implemented. This capacity management process shall be used to:
  - Set boundaries for acceptable service performance and availability;
  - Monitor the usage of resources and send warning messages to the operations team when set thresholds are reached;
  - Make projection for future resources requirements;
  - Ensure the integrity and availability of information systems.

- The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure adequate system performance.

- Capacity requirements such as electrical power, network bandwidth, storage shall be

identified when adding/modifying information processing assets.

- System tuning and monitoring shall be applied to ensure and, where necessary, improve the availability and efficiency of the systems.

- Detective controls, such as trend analysis, shall be in place to indicate problems in due course.

- Special attention shall be paid to resources that involve high lead time or cost.

7.9.4. Separation of Development, Testing & Operational Environments

- IT systems and applications in non-production environments shall be logically and/or physically separated from the production environment(s). This rule should also apply to cloud environments. Examples of separation measures are as follows:
    - IT systems from non-production and production environments should be placed on different networks
    - Applications from non-production and production environments should be installed on different IT systems
    - Data from non-production and production environments should be managed by different application instances
    - Privileged access rights to non-production and production environments should be different
    - Supporting IT systems, such as backup or file shares, should be separated between non-production and production environments
    - Where possible, physical separation shall be preferred over logical separation to offer better security

- IT systems and applications in non-production environments shall fulfil the same information security requirements as IT systems and applications in production environments if they host or process production data.

- IT systems and applications in non-production environments shall fulfil the same information security requirements as IT systems and applications in production environments if they host or process personal data.

7.9.5. Control of Operational Software

- Only required functionalities, services, and applications to meet operational and business requirements shall be installed and running on IT systems and applications in production environments.

- A formal process for installing applications and enabling services on IT systems and applications in production environments shall be developed, documented, and

implemented. The process should include the following topics:

- Define when it is preferable to perform the installation
- Define when it is necessary a formal approval and by whom
- Differentiate between temporary and permanent applications
- Uninstall temporary applications when they are no longer required
- Rules to follow when resolving urgent problems
- Documentation of the services and applications that should be installed/enabled on IT systems in production environments to easily identify unauthorized applications and services.

7.9.6. Security of System Documentation

- Where appropriate, system documentation shall be protected against unauthorised access.

- System documentation shall be stored securely and be readily available in the event of an incident/disaster.

7.9.7. Physical Media Transfer

- Media Containing information shall be protected against unauthorised access, misuse or corruption during transportation.

- Reliable transport or couriers shall be used when transporting media containing Sectigo information.

- Media shall be handed over to the courier/third party representative only after proper identification.

- Media packaging shall be sufficient to protect the contents from any physical damage likely to arise during transit.

- Additional controls shall be adopted while transporting sensitive information. For example, locked container, delivery by Sectigo personnel, temper-evident packaging, splitting information across a number of different deliveries/dispatch routes.

7.9.8. Publicly Available Information

- Software, data and other information requiring a high level of integrity on a publicly available system shall be protected by an appropriate mechanism

- Sectigo shall carry out periodic checks to check the integrity of the publicly available information owned/controlled.

- Formal approval processes shall be in place before information owned by Sectigo is made

publicly available.

7.9.9. Information Systems Audit Considerations

IT Security Audits on Information systems shall be properly planned and agreed. The following topics, as a minimum, shall be carefully planned:

- Access rights required to perform the audit (least-privilege principle);
- Scope and tests to be performed;
- Time of day when the audit is going to be done;
- Expected duration of the audit.

7.10. Network security

Sectigo develops, implements, and maintains a comprehensive security program designed to protect its networks. In this security program, general protections for the network include:

- Segmenting all PKI systems into networks or zones based on their functional, logical, and physical relationship;
- Applying the same security controls to all systems co-located in the same zone with a system;
- Maintaining Root CA Systems in a high security zone and in an offline state or air-gapped from other networks;
- Implementing and configuring Security Support Systems that protect systems and communications between systems inside secure zones and communications with non-PKI systems outside those zones;
- Configuring network boundary controls (firewalls, switches, routers, and gateways) with rules that support only the services, protocols, ports, and communications that Sectigo has identified as necessary to its operations;
- For all PKI Systems, implementing detection and prevention controls to guard against viruses and malicious software; and
- Changing authentication keys and passwords for any privileged account or service account on any TSU system whenever a person's authorization to administratively access that account on the TSU system is changed or revoked.

7.11. Incident management

Sectigo ensures that effective incident management processes are employed across Sectigo Ltd., and its corporate subsidiaries (collectively referred to as "Sectigo") to have:

- A consistent response to incidents happening to Sectigo's systems and applications.
- Incidents detected, reported and logged.
- Clear roles and responsibilities defined in the incident prevention and response processes.

- Incidents analysed and lessons learned.

An incident is any breach of information security; that is, any event that compromises the integrity, confidentiality and/or availability of Sectigo's systems, applications, or the information held within these. An incident is also defined as any non-compliance of Sectigo's policies or legal requirements.

A formal incident management reporting process, together with an incident response and escalation procedure will enable the incident to be managed and normal operations restored in a timely manner.

The process shall enable the incident to be analysed to identify possible causes and enable any weaknesses in Sectigo's processes to be improved in order to prevent re-occurrence.

7.12. Collection of evidence

All types of recorded events indicated in the CPS according to eIDAS are covered including the following:

- Generation of time stamps
- All events related to the life cycle of the TSUs (key management, certificate management, …)
- TSU shutdown/restart
- Desynchronization of the TSU clocks

7.13. Business continuity management

Sectigo operates a fully redundant TSA system. In the event of a short- or long-term loss of an office location, operations at other offices will be increased.

The backup TSA is readily available in the event that the primary TSA should cease operation. All of Sectigo's critical computer equipment is housed in a co-location facility run by a commercial data-center, and all of the critical computer equipment is duplicated within the facility. Incoming power and connectivity feeds are duplicated. The duplicate equipment is ready to take over the role of providing the implementation of the TSA, and allows Sectigo to specify a maximum system outage time (in case of critical systems failure) of 1 hour.

Sectigo operations are distributed across several sites worldwide. All sites offer facilities to manage the lifecycle of a timestamp token.

As well as a fully redundant TSA system, Sectigo maintains provisions for the activation of a backup TSA and a secondary site should the primary site suffer a total loss of systems. This disaster recovery plan states that Sectigo will endeavor to minimize interruptions to its TSA operations.

7.14. TSA termination and termination plans

In case of termination of TSA operations for any reason whatsoever, Sectigo will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Sectigo will take the following steps, where possible:

- Notifying the supervisory body prior to termination
- Providing Subscribers, Relying Parties, and other affected parties with ninety (90) days' notice of its intention to cease acting as a TSA.
- Revoking all TSU certificates.
- Making reasonable arrangements to preserve its records according to this TSPPS.
- Reserving its right to provide succession arrangements for the re-issuance of timestamps a successor TSA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as Sectigo's.
- The destruction of the private keys of the TSUs, including any backup copies.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

This plan is verified, reviewed and updated annually.

7.15. Compliance

The practices specified in this TSPPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the ETSI EN 319 401 and ETSI EN 319 421 and other industry standards related to the operation of a TSA such as the IETF RFC 3161.

Sectigo is also compliant with the eIDAS regulation

An independent external auditor assesses Sectigo's compliancy with the ETSI standards and the eIDAS regulation.

7.15.1. Frequency or circumstances of assessment

The audit mandates that the period be divided into an unbroken sequence of audit periods. An audit period must not exceed two years in duration.

7.15.2. Identity/qualifications of assessor

An accredited CAB performs Sectigo's audit. A CAB means a natural person, legal entity, or group of natural persons or legal entities that collectively possess the following qualifications and skills:

- Independence from the subject of the audit;

- The ability to conduct an audit that addresses the criteria specified in an eligible audit scheme;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- Bound by law, government regulation, or professional code of ethics

7.15.3. Assessor's relationship to assessed entity

The auditor or CAB is independent of Sectigo, and does not have a financial interest, business relationship, or course of dealing that would create a conflict of interest or create a significant bias (for or against) Sectigo.

7.15.4. Topics covered by assessment

The CAB assess the compliance of the audited component, on all or part of the implementation of:

- the documentation (TSPPS, policies, procedures, …);
- the technical components of the TSA

Before every audit, the CAB suggests a list of components and procedures that they wish to verify. They use this to develop the detailed audit plan.

7.15.5. Communication of results

Sectigo will make the audit report available to the Supervisory Body in charge of qualifying and certifying the service. Sectigo is not required to make publicly available any general audit finding that does not impact the overall audit opinion.

8. Additional requirements as per eIDAS regulation

8.1. TSU public key certificate

If a time-stamp is claimed to be a qualified electronic time-stamp as per Regulation (EU) No 910/2014, the TSU signature verification (public) key certificate should be issued by a certification authority operating under ETSI EN 319 411-2 certificate policy.

This is the ASN.1 object identifier to claim that the time-stamp token is qualified

```
-- object identifiers
id-etsi-tsts OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0)
id-tst-profile(19422) 1 }
id-etsi-tsts-EuQCompliance OBJECT IDENTIFIER ::= { id-etsi-tsts 1 }
-- statements
esi4-qtstStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-tsts-EuQCompliance }
-- By inclusion of this statement the issuer claims that this
-- time-stamp token is issued as a qualified electronic time-stamp according to
-- the REGULATION (EU) No 910/2014.
```

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

Sectigo operates three Time-Stamping Authorities (TSA). The Sectigo TSAs are intended for use when need to provide accurate time to document signed or sealed and to give the integrity needed for this.

The non-qualified TSAs providing time-stamping services are provided from different URLs and use different TSUs identified by different subject names in their public key certificate

The Sectigo Authenticode time-stamping service is available at the URL
http://timestamp.sectigo.com/authenticode

Sectigo also offers a RFC3161 TSA, whose URL is:

http://timestamp.sectigo.com/rfc3161

While the Sectigo qualified TSA is provided from:

http://timestamp.sectigo.com/qualified

Annex A: Change Log

Version	Change Description	Date
1.0	First draft version	February 14, 2020
1.0.1	Updated office address and contact person	September 17, 2020
1.0.2	Include the OID for timestamps	October 14, 2020
1.0.3	Updated sections 4.3, 5.2, 7.6.2.2 and 8.2	October 20, 2020
1.0.4	Updated section 5.2 and Annex B. Adding a new annex C with the TSA hierarchy	October 22, 2020
1.0.5	Updated section 5.2 regarding OIDs	October 23, 2020
1.0.6	Updates in annexes B and C	October 23, 2020
1.0.7	Update on the TST including accuracy and qcStatement and adding some stratum 1 UTC(k) laboratories in section 7.1.1	November 20, 2020

Annex B: Requests & responses format

Request format

The format for sending the applications follows the following scheme:

Content type: application/timestamp-query

Method: POST

Content-length: required

Contains the time stamp request in ASN.1, encoded in DER

Optional fields according to the RFC3161 specification are treated as follows:

Field	Treatment
Nonce	Optional. If present, the response contains the same value
reqPolicy	No use
certReq	No use
Extensions	No use

Response format

If the request cannot be processed, an http response is returned indicating an error code when it cannot respond with a timestamp. Possible errors are:

Reason	Error	Description
Missing content-length field	411	CONTENT_LENGHT REQUIRED
Content-length too large	413	REQUEST ENTITY TOO LARGE
Incorrect content-type	415	UNSUPPORTED MEDIA TYPE
Data are not a timestamp request	400	BAD REQUEST
Server not responding	500	SERVER INTERNAL ERROR

The responses use the following scheme:

Content type: application/timestamp-reply

Method: POST

Content-length: required

Contains the time stamp reply in ASN.1, encoded in DER

Optional fields according to the RFC3161 specification are treated as follows:

Field	Treatment
Time-stamp policy	OIDs.
Ordering	False
Nonce	If comes with the request, return the same value.
Certificates	TSA certificate. subCA certificate.
Accuracy	0x01 seconds, unspecified millis, unspecified micros
Tsa	No present
extensions	esi4-qtstStatement-1 QC-STATEMENT

Annex C: TSA hierarchy

Root certificate

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	RSA: 7b24e01933c796dfc404ce01161f5373
Signature Algorithm:	sha384WithRSAEncryption	
Issuer:	commonName	Sectigo Qualified Time Stamping Root R45
	organizationName	Sectigo (Europe) S.L.
	countryName	ES
Validity (25y):	Not Before:	Monday, October 5, 2020
	Not After:	Wednesday, October 4, 2045
Subject:	commonName	Sectigo Qualified Time Stamping Root R45
	organizationName	Sectigo (Europe) S.L.
	countryName	ES
Thumbprint		RSA: cb73944c042e53bfc4579d2f712f3eea99fe4307

Sectigo Qualified Time Stamping CA R35

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	RSA: 0cda8301d3f3280e71cdb028a352c65b
Signature Algorithm:	sha384WithRSAEncryption	
Issuer:	commonName	Sectigo Qualified Time Stamping Root R45
	organizationName	Sectigo (Europe) S.L.
	countryName	ES
Validity (15y):	Not Before:	Monday, October 5, 2020
	Not After:	Thursday, October 4, 2035
Subject:	commonName	Sectigo Qualified Time Stamping CA R35
	organizationName	Sectigo (Europe) S.L.
	countryName	ES
Thumbprint		RSA: 1d6318b5b7d9ba360d757ac955881bf17c750766