Certigna

TIME-STAMP POLICY

CERTIGNA TSA

Edited:	2024-06-25
Version :	1.6
OID :	1.2.250.1.177.2.9.1
Authors :	J. Allemandou
Classification :	Public

SUMMARY

1 INTRODUCTION

1.1 Overview

CERTIGNA has a Time-stamping Authority (TSA) named "Certigna TSA" to provide qualified time-stamps.

This Time-stamp Policy (TP) also identifies obligations and requirements on certificate users. Time-stamp Policy describes the practices that the TSA applies and agrees to respect as part of the provision of the time-stamp service.

The reader's attention is drawn to the fact that the understanding of this Time-stamp Policy guess he is familiar with the concepts related to the technology of Public Key Infrastructure (PKI) and to time-stamping.

This Time-stamp Policy meets the requirements of:

- eIDAS Regulation (EU) N°910/2014 for qualified time-stamping service ;
- the « Time-stamp policy » of the « Référentiel Général de Sécurité » (RGS) developed by the National Agency for the information systems security (ANSSI);
- Best Practices Policy for Time-Stamp (BTSP) described by ETSI EN 319 421 specifications and identified by the following 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)).*

1.2 Document Name and Identification

This Time-stamp Policy can be identified by the name of the « Certigna TSA » and by its OID: 1.2.250.1.177.2.9.1.

Several time-stamping Units (TSU) are implemented to sign the time-stamps issued by the TSA. These TSU are using time-stamping seal certificates issued by two authorities:

- Current "Certigna Entity CA" Certification Authority (CA) and targeting the compliance with ETSI EN 319 411-2 specifications. These certificates are identifiable by the following OID:
    - 1.2.250.1.177.2.6.1.9.1: ETSI EN 319411-2 certified at QCP-l level
    - 1.2.250.1.177.2.6.1.9.2: ETSI EN 319411-2 certified at QCP-l level
- New "Certigna Time Stamping CA" Certification Authority (CA) and targeting the compliance with ETSI EN 319 411-2 specifications. These certificates are identifiable by the following OID with a certification in progress:
    - 1.2.250.1.177.11.1.1.4.1 : ETSI EN 319411-2 QCP-l-qscd level (In progress)
    - 1.2.250.1.177.11.1.1.4.2: ETSI EN 319411-2 QCP-l level (In progress)

1.2.1 Revisions

Version	Date	Document change
1.0	2017-08-06	Creation
1.1	2019-02-12	Revision of the graphic chart and commitments.
1.2	2020-06-09	New TESSI graphic chart and precisions about: - Compliance RGS Time-stamp Policy (see 1.1), - Addition of OID of certificates by TSU (see 1.2), - Privacy of Personal Information (see 3.6), - Limitations of liability (see 3.8), - Dispute Resolution Provisions (see 3.9).
1.3	2020-11-02	Revision of the document and precisions about: - Standards targeted by TSU certificates (see 1.2), - Revocation of TSU certificates at the end of TSA life (see 4.8).
1.4	2022-09-01	New TESSI graphic chart and precisions about the qualifications of the HSM.
	2023-09-08	Revision of the document without modification
1.5	2024-04-04	New graphic chart and precisions about: - Contacts - The future use of new TSU certificates for which the certification is in progress.
1.6	2024-06-25	Revision of the document and precisions about: - OID of certificates used by the timestamping service (see 1.2); - Commitment to availability of the timestamping service (see 5.6.1).

1.3 What is time-stamping ?

Time-stamping allows to attest that a data exists at a given moment. For this purpose, an unequivocal representation of the data to time-stamp is associated with an instant in time. For example, the representation of a data can be its hash value associated with a hash algorithm identifier.

The guarantee of this association is provided by means of a signed structure called « time-stamp ». This time-stamp contains in particular:

The time-stamp Policy identifier under which the time-stamp was generated;

- The hash value and the hash algorithm of the data that has been time-stamped;
- The date and UTC time;
- The certificate identifier of the Time-stamping Unit (TSU) which has generated the time-stamp (which also contains the name of the Time-stamping Authority).

End-users have access to the validity information of time-stamping certificates (certification chains, Certificates Revocation Lists (CRL), ...) to check the time-stamps.

The private key or the keys used to generate time-stamps are managed by the TSA, which retains full responsibility to satisfy the requirements defined in this Time-stamp Policy. The TSA can operate several Time-stamp Units (TSU). Each TSU has its own key-pair

1.4 Trust in time-stamping

The guarantee provided by the TSA is based on technical elements and management rules which are presented in this Time-stamp Policy. This Time-stamp Policy presents to users the commitments that the TSA takes, in terms of security, and describes in a macroscopic manner the means implemented to fulfil these commitments.

This Time-stamp Policy presents the level of trust achieved by the time-stamp service. It reflects the formal recognition of the importance given by the TSA to the security of the service.

The requirements for time-stamping services described in this Time-stamp Policy include requirements relating both to time-stamp management and to the operation of TSU that publish the time-stamps.

The TSA has the responsibility to ensure that these requirements are met and may subcontract to others parties a subset of time-stamping service.

1.5 PKI Participants

1.5.1 Time-stamping Authority

A Trust Services Provider (TSP) providing time-stamp services to the public is called an "Electronic Time-stamping Service Provider". It comprises one or more TSA which is responsible for providing time-stamping services and is responsible for the operations of one or more TSUs which generate and sign time-stamps on behalf of the TSA.

The TSA performs all or part of these functions directly or by subcontracting them. In any case, the TSA retains the responsibility. The TSA undertakes to comply with the obligations described in this Time-stamp Policy and ensures that these requirements are met. It also undertakes that the components of the TSA, internal or external to the TSA, to which they are applicable also respect them.

The TSA ensures the compliance with the requirements and procedures prescribed in this policy, even when the time-stamp features are implemented by subcontractors.

The TSA adheres to any additional obligations indicated in the time-stamp either directly or incorporated by reference.

The TSA provides time-stamping services in accordance with this TP and the associated TPS.

The TSA fulfills all its commitments as stipulated in the Terms and Conditions.

1.5.2 Certification authority

The CA is responsible for the provision of the TSU's certificates management services throughout their life cycle (generation, distribution, renewal, revocation, ...) and relies on a technical infrastructure: a PKI. The CA is responsible for the implementation of the CP to the PKI set in place.

For Time-stamping certificates signed in its name, the CA has the following functions:

- Registration and renewal functions;
- Certificate generation function;
- Secret generation function;
- Publication function of the general conditions of the Certification Policy, CA certificates and certificate application forms;
- Revocation management function;
- Information function on the status of certificates via the Certificate Revocation List (CRL) updated at regular intervals and in a query mode / real-time response (OCSP).

The CA provides these functions directly or outsourcing them, some or all. In all cases, the CA retains responsibility. CA is committed to respecting the obligations described in its Certification Policy. It is also committed that the components of the PKI, internal or external to the CA, which they incumbent also respect them.

1.5.3 Subscriber

The subscriber is a legal or a natural person to whom a time-stamp is issued and who is bound to any subscriber obligations.

When the subscriber is an organization, it comprises several end-users or an individual end-user and some of the obligations that apply to that organization will have to apply as well to the end-users. In any case the organization will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such an organization is expected to suitably inform its end users.

When the subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

It is recommended that the subscriber, at the time of obtaining a time-stamp, verify that the certificate of the timestamp unit is not revoked.

1.5.4 User

The user is an entity (natural person or system) that trusts a time-stamp issued under le Time-stamp Policy. To trust a time-stamp, the user must:

- Verify that the time-stamp has been successfully signed, and that the certificate of the TSU is valid at the time of verification.
- Consider the limitations on the use of the time-stamp indicated in this TP and the Terms and Conditions.

1.6 Définitions et acronymes

1.6.1 Definitions

Useful terms to the understanding of the CP are the followings:

Subsciber - Legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations.

Administrative authorities - This term refers to government departments, local authorities, public administrative institutions, the bodies administering social protection systems and other bodies responsible for the management of an administrative public service.

Certification Authority - In a Trust Service Provider (TSP), a Certification Authority is responsible, on behalf and under the responsibility of this TSP, applying at least one certification policy and is identified as such, as an issuer («issuer" field of the certificate).

Timestamping Authority (TSA) - Authority responsible for the management of a timestamp service in compliance with Time-stamp Policy and relying on one or several TSU.

Electronic Seal - Digital Seal done by an application server with data to be used either as part of an authentication service data origin, either as part of a service non-repudiation.

Electronic Certificate - Electronic file certifying the link between a public key and the identity of its owner (natural or legal person or system). This certificate takes the form of an electronic signature made by a TSP. It is issued by a CA. The certificate is valid for a given period specified therein.

Component - Platform operated by an entity and comprised of at least one computer station, an application and, where applicable, cryptographic means. Component play a specific role in the operational implementation of at least one function of PKI. The entity may be the CSP itself or an external entity related to CSP contractual, regulatory or hierarchical.

Time-stamp – Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

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

TSA Practice Statement (TPS) - A TPS identifiers the practices (organization, operational procedures, human and technical means) that the TSA applies for time-stamping service delivery and in compliance with the time-stamp policy that it has undertaken to respect.

Public Key Infrastructure - Components, functions and procedures dedicated to the management of cryptographic keys and certificates used for trusted services. PKI can be composed of a CA, a certification operator, a centralized registration authority and / or local certification agents, an archiving entity, a publishing entity, ...

Authorities Revocation List - List including the serial numbers of the certificates of intermediate authorities which have been revoked, and signed by the root CA.

Certificate revocation list - List including serial numbers of certificates that have been revoked, and signed by the issuing CA.

Time-stamping module - Security product including a cryptographic resource and which is dedicated to implement the time-stamp functions of the TSU, in particular the generation, the conservation and the implementation of the TSU private key and also the time-stamps generation.

Certification Policy - A set of rules, identified by a name (OID), defining the requirements that a CA comply in the implementation and delivery of its services and indicating the applicability of a certificate to a specific community and / or a class of applications with common security requirements. A CP can also, if necessary, identify the obligations and requirements on other stakeholders including ESCM and certificate users.

Time-stamp Policy (TP)– Set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements.

Security product - A software or hardware that implements security features necessary for securing information or system.

Certificate Manager – Person in charge and responsible of the electronic certificate used by an application service.

RSA - Public key algorithm (Rivest, Shamir and Adleman).

Time-stamping service - Trust service for issuing time-stamps.

TSA system - Composition of IT products and components organized to support the provision of time-stamping services.

Information System - Any set of means to develop, process, store or transmit information subject to electronic exchange between users and administrative authorities and between administrative authorities.

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.

Time-stamp user – Entity (person or application) which relies on a time-stamp issued under the time-stamp Policy.

End user – Subscriber or user of time-stamps.

Note - An agent of an administrative authority which conducts electronic exchange with another administrative authority is, for the latter, a user.

Note - In the remainder of the document, the term "entity" is used to designate a company or an administration. The name "enterprise" covers enterprises in the broadest sense, namely all legal persons governed by private law: companies, associations as well as craftsmen and self-employed workers.

1.6.2 Acronyms

Useful abbreviations for the understanding of this CP are the followings:

AA	Administrative Authority
CA	Certification Authority
RA	Registration Authority
DRA	Delegate Registration Authority
TSA	Time-stamping Authority
ANSSI	National Agency for information systems security
CGU	Terms and Conditions
CNIL	National Commission for Computing and Liberties
CSR	Certificate Signature Request
DN	Distinguished Name
CPS	Certification Practice Statement
ETSI	European Telecommunications Standards Institute
PKI	Public Key Infrastructure
ARL	Authority Revocation List
CRL	Certificate revocation list
OC	Certification Operator
OCSP	Online Certificate Status Protocol
OID	Object Identifier
CP	Certification Policy
BCP	Business Continuity Plan

PP	Protection Profile
PKCS	Public Key Cryptographic Standards
TSP	Trust Service Provider
RSA	Rivest Shamir Adleman
ISS	Information systems security
TSU	Time-stamping Unit
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

2 RISK ASSESSMENT

A risk assessment is carrying out by TSA to identify and evaluate trust service risks taking into account of business and technical issues.

TSA is taking account of the risk assessment results to determine the treatment measures which ensure that the level of security is commensurate to the degree of risk.

TSA determines all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the trust service practice statement.

The risk assessment of time-stamping service is reviewed and revised at minimum once a year, after what, the risk assessment is approved, and the residual risks identified is accepted.

3 POLICIES AND PRACTICES

3.1 Time-stamp policy

For this policy, the date and time of each time-stamp are synchronized with UTC time with an accuracy of one second.

This Time-stamp Policy requires the use of the time-stamp format described at chapter 5.5.2 and a time-stamping protocol in accordance with RFC 3161.

3.2 Time-stamp practice statement

The Time-stamp Practice Statement (TPS) sets out the mechanisms and procedures implemented to achieve the security objectives o the Time-stamp Policy, in particular the processes used by the TSA for the creation of time-stamps and the maintaining the accuracy of its clocks.

The TPS is a detailed description of the operational practices of the TSA implemented for the issuance of time-stamps and the management of time-stamping service.

The TPS defines how the TSA complies with the physical, environmental, procedural, organizational, and technical requirements identified in this Timestamping Policy.

This Time-stamping Policy (TP) is thus a less specific document than the corresponding TPS. The Timestamping Policy is defined independently of the details of the specific operating environment of the TSA, while the TPS is tailored to the organizational structure, operating procedures, equipment and working environment of the TSA.

3.3 Terms and Conditions

Given the complexity of reading a TP and a TPS for non-specialist users of the domain, the TSA also provides Terms and Conditions corresponding to “TSA Disclosure Statement”.

The Terms and Conditions are not intended to replace this Time-stamping Policy or TPS but are intended for subscribers and non-technical users of time-stamps so they can easily understand the essential information they need to know.

The Terms and Conditions incorporate at least the following information:

- The trust service policy being applied.
- Any limitations on the use of the service;
- The subscriber's obligations, if any;

- Information for parties relying on the trust service;
- The period of time during which TSP event logs are retained;
- Limitations of liability;
- The applicable legal system;
- Procedures for complaints and dispute settlement;
- The conformity assessment scheme of this time-stamp policy;
- The TSA contact information;
- The minimum period of time, excluding revocation, during which time-stamps will be verifiable;
- Accuracy of time in time-stamps versus UTC time;
- Provisions for validating the chain of certificates linked to TSU's certificates;
- The name of the country in which the timestamping authority is established and the identifier of the TSA (as included in the TSU's certificates).

The Terms and Conditions are available to subscribers as an appendix to their contract and to users via the CERTIGNA site at the following address: https://www.certigna.com/politique-horodatage

3.4 Information security policy

The TSA has an information security policy which is documented, implemented, maintained, reviewed every year and approved by management.

This information security policy sets out the organization's approach to managing its information security and the security objectives that have been determined. This policy is communicated to all employees and to the impacted contributors.

3.5 Policy Administration

3.5.1 Organization Administering the Document

The CA has a Security Committee responsible for the development, monitoring, modification, and validation of this TP. It shall act on any necessary changes to be made to the CP at regular intervals.

3.5.2 Contact Person

3.5.2.1 FAQs et customer support

Answers to frequently asked questions can be found in our FAQ section at https://www.certigna.com/faq/.

If you have any other questions, you can contact our Customer Service department as follows:
- Contact e-mail: contact@certigna.fr ;
- Telephone: 0 806 115 115 (Free service) available Monday to Friday from 09:00 to 18:00;
- Chat on the https://www.certigna.com website, available Monday to Friday from 09:00 to 18:00.

3.5.2.2 Reporting au malicious or dangerous certificate

For reporting a malicious or dangerous certificate (suspected Private Key compromise, certificate misuse, or other types of fraud, compromise, inappropriate conduct, etc.) or any other matter related to certificates, use the contact form available at https://www.certigna.com/contactez-nous/ by selecting “Certificate considered malicious or dangerous”.

3.5.2.3 Making a complaint

To bring a complaint to CERTIGNA's attention, please use the contact form available at the following address https://www.certigna.com/contactez-nous/ and select the "Réclamation" reason.

You can also make a complaint to our customer service department using the following contact details:
- Contact e-mail: contact@certigna.fr ;
- Telephone: 0 806 115 115 (Free service) available Monday to Friday from 09:00 to 18:00;
- Chat on the https://www.certigna.com website, available Monday to Friday from 9am to 18:00;
- Mail addressed to

CERTIGNA
20 allée de la Râperie
Zone de la plaine
59650 Villeneuve d'Ascq, France

Information on the processing of your personal data is available in the Policy on the use of personal data, which can be accessed at the following address: https://www.certigna.com/politique-dutilisation-des-donnees-personnelles/.

3.5.3 Person Determining TPS Suitability for the Policy

The Security Committee ensures the compliance of the TPS with the TP. IT can optionally be assisted by external experts to ensure compliance.

3.5.4 TPS approval procedures

The TPS translates into technical, organizational and procedural terms the requirements of the TP based on the company's "Information security policy". The Security Committee shall ensure that the means used and described in this TP meet these requirements as the approval process in place. A compliance check of the TPS against the TP is made through the internal and external audits for the CA qualification.

Any update request of the TPS also follows this process.
Any new approved version of the TPS is published without delay.

3.6 Repositories

3.6.1 Entity in charge of providing information

CERTIGNA provides to users and applications using time-stamps signed by TSU's certificates, information about the revocation status of TSU's certificates used by the TSA. These informations are published through several servers:

- Web Servers currently used:
  - http://crl.certigna.fr/entityca.crl
  - http://crl.dhimyotis.com/entityca.crl
- Web Servers used in future:
  - http://crl.certigna.com/CertignaTimeStampingCA.crl
- OCSP Servers currently used:
  - http://entityca.ocsp.certigna.fr
  - http://entityca.ocsp.dhimyotis.com
- OCSP Servers used in the future:
  - http://ocsp.certigna.com

3.6.2 Information to be Published

The TSA and CA issues to the users and subscribers:

- This Time-stamp Policy ;
- The Time-stamp Practice Statement on demand to CERTIGNA contact;
- The Certification Policy of the CA issuing TSU's certificates and the associated Certification Practice Statement;;
- The Terms and Conditions of Time-stamping service;
- The Terms and Conditions of CA certification service;
- The certificates used by TSU and the associated CA certificates (root and subordinate CA).
- The Certificate Revocation List (ARL / CRL).

Note: Due to the complexity of reading a TP for subscribers or certificate users not experts in this field, the TSA publishes Terms and conditions that the future subscriber is obliged to read and to accept previous the issuance of time-stamps.

3.7 Publication of Information

3.7.1 Publication of TP, Terms and conditions, and forms

The TP, the TPS, the Terms and Conditions of the TSA and the various forms required for certificate management are published in electronic format at https://www.certigna.com.

3.7.2 Publication of CPS

The CA issues, to the CM, Subjects and certificate users, the CPS to make possible the assessment of compliance with this CP. Details on its practices are however not made public.

3.7.3 Publication of CA Certificate

The Subscribers and users can access the CA certificates that that are signing the certificates of TSU at the following address: https://www.certigna.com.

3.7.4 Access Controls on Repositories

Access to information published to users is free.

Access to change the publishing systems (add, delete, change the information published) is strictly limited to authorized internal functions of the PKI, through a strong access control, based on a two-factor authentication.

3.8 Compliance

3.8.1 Privacy of Personal Information

3.8.1.1 Privacy Plan

CERTIGNA retains the personal data for a period of three years from the end of the commercial relationship with the customer and 3 years from the last contact with the prospect. The delay starts from the last connection to the customer account or the last sending of an email to customer service, or from a click on a hypertext link of an email sent by CERTIGNA, a positive response to an email requesting if the client wishes to continue to receive commercial prospecting at the end of the three-year period.

In order to monitor the quality of our services, calls made to our customer service are likely to be registered and kept for a period of 30 days.

In accordance with the law n ° 78-17 of January 6, 1978 relating to data, files and freedoms, modified and the European regulation "2016/679 / EU of April 27, 2016" relating to the protection of natural persons to the processing of personal data and the free movement of such data, you have the right to access, oppose, rectify, delete and portability of your personal data. You can exercise your right by sending an email to: privacy@certigna.com, or by mail to the following address:

CERTIGNA, Service du DPO,
20 Allée de Râperie, 59 650 Villeneuve d'Ascq, France

Your request must indicate your surname and first name, e-mail or postal address, be signed and accompanied by a valid proof of identity.

3.8.1.2 Information Treated as Private

The information considered as personal are the subscriber's application files for time-stamps delivery.

3.8.1.3 Notice and Consent to Use Private Information

Accordance with the laws and regulations on French territory, personal information submitted by Subject to CA must not be disclosed or transferred to third parties except in

the following circumstances: prior consent of the Subject, court order or other legal authorization.

3.8.1.4 Disclosure pursuant to Judicial or Administrative Process

The disclosure of confidential information is only made to the authorities empowered officially and exclusively on their specific request in accordance with French law.

3.8.2 Intellectual Property Rights

The brand "CERTIGNA" is protected by the Code of Industrial Property. The use of this trademark by the entity is allowed only in the framework of the subscription contract.

3.8.3 Limitations of Liability

The TSA is subject to a general obligation of means. The TSA cannot be held liable for the Subscriber for direct damage that may be attributed to it for the services entrusted to it under these TCSU.

The TSA's responsibility cannot be sought for any indirect loss, such as, in particular, loss of turnover, loss of profit, loss of orders, loss of data, loss of opportunity, disturbance to the image or any other special damage or events beyond its control or any fact not attributable to it.

The TSA is only responsible for the tasks specifically assigned to it under this Policy. The TSA cannot be held responsible in any way for the use made by the Subscribers or the Users of the time-stamps, nor the contents of the documents and the data which are given to it by the Subscribers or the Users. In any case, the responsibility of the TSA cannot be sought in case of:

- Fault, negligence, omission or default of the CA, which would constitute the exclusive cause of the occurrence of the damage,
- Malfunction or unavailability of tangible or intangible property in the case where it has been provided by the Subject,
- Delay in providing the data to be processed due to the Subscriber;
- Loss of the qualification of a third-party provider that is beyond the control of CERTIGNA (ex: the supplier of cryptographic support used for TSU's keys).

By express agreement between the TSA and the Subscriber, the liability of the TSA is limited, by certificate request, all damages, to the sum of two (2) times the amount paid under the timestamps request through a pack or a month subscription.

The TSA may not be held liable for any unauthorized or improper use of time-stamps issued by its time-stamping service.

The TSA shall under no circumstances be held liable for any damage caused using the time-stamps issued by the TSA.

The TSA cannot be implicated by delays or losses that the transmitted data on which a time-stamp is requested by the application service.

The TSA cannot be held liable for problems related to force majeure, within the meaning of the Civil Code. If a case of force majeure has a duration exceeding fifteen days, the subscriber will be authorized to terminate the contract and there will be no prejudice.

The data transmitted in a time-stamp request and the verification of their value in the associated response remain the responsibility of the subscribers.

3.9 Dispute Resolution Provisions

The validity of this TP and any other question or dispute relating to its interpretation, execution or termination will be governed by French law.

The TSA and the Subscriber commit themselves to devote their best efforts to the amicable resolution of all the questions or the litigation which could divide them, before the seizure of the jurisdiction hereinafter designated.

The TSA and the Subscriber agree, in the event that an amicable agreement is impossible to stop, that the courts of Lille will have exclusive jurisdiction to hear any dispute resulting from the validity, interpretation, execution or termination hereof, and more generally from any dispute arising herein that could divide them, notwithstanding pluralities of defendants or warranty claim.

4 NON-TECHNICAL SECURITY MEASURES

REMINDER – TSA conducted a risk analysis to determine the specific security objectives, to cover the business risks of the entire TSA, and technical and non-technical security measures to implement. Its TP was developed based on this analysis. This TP is established based on this risk analysis.

4.1 Physical Security Controls

4.1.1 Site Location and Construction

The information systems used for TSA functions are hosted in several production centers with the same security features. The location of the sites does not present major risks.

4.1.2 Physical Access

A strict control of physical access to the components of TSA is performed, with access logging and video surveillance: the defined security perimeter around the systems for the time-stamping is limited to people within a trusted role.

Outside working hours, the implementation of physical and logical intrusion detection means strengthening the security of the PKI. In addition, any person (external service provider, etc.) entering in this physically secure area cannot be left without the supervision of an authorized person.

4.1.3 Power and Air Conditioning

Measures concerning the supply of electricity and air conditioning are taken to meet the commitments of the TSA described in this TP on ensuring the level of availability of its functions, including revocations management features and information functions on the status of certificates.

4.1.4 Water Exposures

Measures for protection against water damage are taken to address the TSA commitments described in this TP on ensuring the level of availability of its functions, including revocations management functions and information functions on the status of certificates.

4.1.5 Fire Prevention and Protection

Measures for prevention and protection against fire are taken to address the TSA commitments described in this TP on ensuring the level of availability of its functions, including revocations management functions and information functions on the status of certificates.

4.1.6 Media Storage

The information and their supporting assets involved in the activities of the TSA are identified, inventoried and their security needs defined in terms of availability, integrity and confidentiality.

Specific measures are implemented to avoid compromise or theft of information. The assets corresponding to this information are managed according to procedures conforming to these security needs. They are handled in a secure manner to protect the assets from damage, theft and unauthorized access. Management procedures protect media against obsolescence and deterioration during the period during which the TSA agrees to keep the information contained therein.

4.1.7 Waste Disposal

The measures taken for the disposal of media are compliant with the level of confidentiality of the corresponding information.

4.1.8 Off-site Backup

Outsourced backups are implemented and organized in such a way as to ensure that the IGC functions are available as soon as possible after an incident, and in accordance with the commitments of this TP, in particular regarding the availability and protection of the confidentiality and integrity of saved information.

4.2 Procedural Controls

4.2.1 Trusted Roles

Each timestamping service component distinguishes at least the seven following functional trust roles:

- **Security officer**: The security officer is responsible of implementing the component's security policy. He manages the controls on the physical access to the component's

system hardware. He is authorised to review the archives and is responsible of analysing the event logs to detect any incident, anomaly, attempted compromise, etc.

- **Application manager**: Within the component to which he is attached, the application manager is responsible of implementing the certification policy and the declaration of the PKI's certification practices on the level of the application for which he is responsible. His responsibility includes all the functions provided by this application and the corresponding performances.
- **System administrator**: He is responsible of the start-up, configuration and technical maintenance of the component's IT hardware. He provides the technical administration of the component's systems and networks.
- **Operator**: Within a PKI component, based on his duties, an operator runs applications for the functions implemented by the component.
- **Controller**: Designated by a competent authority, this person's role is to regularly perform verifications on the compliance of the implementation of the functions provided by the component relative to the certification policies, to the PKI's declarations of certification practices, and to the component's security policies.
- **Registration Officer**: Responsible for approving end entity Certificate generation and revocation.
- **Secret share holder**: It has the responsibility to ensure the confidentiality, integrity and availability of the secrets assigned to him.

The different roles are defined in the description of functions specific to any entity operating the TSA services on the principles of separation of duties and least privilege. These roles determine the sensitivity of the functions, depending on responsibilities and access levels, background checks and employee training and awareness.

Measures are in place to prevent equipment, information, media and software relating to TSA services are removed from the site without permission.

4.2.2 Number of Individuals Required per Task

For reasons of availability, each task must be performed by at least two people. For some sensitive tasks like operations on HSM (e.g. key ceremony), many people are required for security reasons and "dual control."

4.2.3 Identification and Authentication for Trusted Roles

Each role assignment to a member of the TSA staff is attributed and accepted formally. This role is clearly mentioned and described in his/her job description. TSA checks the identity and permissions of any member of its staff before assigning privileges to its functions. Assigning a role to a member of staff following the TSA particularly strict procedure with

signing of the minutes for the allocation of all elements necessary for the performance of this role in the PKI (keys, access codes, cryptographic keys, etc.).

4.2.4 Role Requiring Separation of Duties

About trusted roles, the following rollups are prohibited within the PKI:

- Security officer and system administrator / operator;
- Controller and any other role;
- System operator and administrator.

4.3 Personnel Security Controls

4.3.1 Qualifications, Experiences, and Clearance Requirements

All staff must work within the TSA components must sign the internal security charter. This charter contains a confidentiality clause which applies both in respect of third parties and users. It lists the roles of each employee within the TSA. She is co-signed by the employee and the security officer. Matching skills of personnel involved in the TSA is checked in compliance with its duties on the components.

The management personnel, the security officer, system administrators, have the expertise necessary for the performance of their respective roles and are familiar with the security procedures applied to the operation of the TSA. AC informs any employee involved in the TSA trusted roles of its responsibilities for TSA services and procedures related to system security and monitoring staff.

4.3.2 Background Check Procedures

The TSA ensures that all employees involved on the TSA suffered no contradiction in justice conviction with their functions. The employees provide a copy of the bulletin Number 3 before their Assignment of his/her criminal record. This check is renewed periodically (at least every 3 years).

In addition, the TSA ensures that the employees do not suffer from conflict of interests detrimental to the impartiality of their tasks.

4.3.3 Training Requirements and Procedures

Initial training to software, hardware and internal operating and safety procedures is provided to employees, in line with the role that the TSA assigns. An awareness on the implications of the operations whose they are responsible is also achieved.

The management staff employed have:

- Knowledge of the time-stamping technology;
- Knowledge of the digital signature technology;
- Knowledge of the mechanisms for calibrating or synchronizing the clocks of TSU with UTC time;

For staff with safety responsibilities, a good knowledge of security procedures, and experience with information security and risk assessment is required.

4.3.4 Retraining Frequency and Sequence

The staff concerned receives adequate information and training prior to any changes in systems, procedures in the organization.

4.3.5 Sanctions for Unauthorized Actions

Any member of the TSA staff acting in contradiction with established policies and procedures of this TP and internal processes and procedures of the TSA, or negligently or maliciously, will see his/her privileges revoked and will be subject to administrative sanctions or judicial proceedings.

4.3.6 Independent Contractor Controls

The staff of external providers involved in local and / or components of the TSA must also meet the requirements of this Section 5.3. This is translated into appropriate clauses in contracts with those providers. If so, whether the level of intervention requires, it may be asked to the provider to sign the IT charter and / or provide background check elements.

4.3.7 Documentation Supplied to Personnel

Each employee has the adequate documentation of operational procedures and specific tools that implements and general policies and practices of the component within which he/she works. The CA gives him/her the impacting security policies. Operators have the operator manuals corresponding to the components on which they are involved.

4.4 Internal organization

The TSA is a legal entity according to national law.

The TSA has a system for quality and information security management appropriate for the time-stamping services it is providing. It employees enough personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide time-stamping services.

The TSA organization is reliable. Trust service practices under which the TSA operates are non-discriminatory.

The TSA makes its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the TSP terms and conditions.

The TSP maintains sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law, to cover liabilities arising from its operations and/or activities.

The TSA has the financial stability and resources required to operate in conformity with this policy.

The TSA shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.

The TSA has a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third-party arrangements.

4.5 Audit Logging Procedures

Relevant events involved in the management and operation of the PKI are recorded in manuscript or electronically form (by seizure or by automatic generation) and, for purposes of audit.

4.5.1 Types of Events Recorded

The operating systems of the PKI servers will log the following events automatically on start-up and in electronic form (non-exhaustive list):

- Create / modify / delete user accounts (access rights) and corresponding authentication data;
- Start and stop IT systems and applications;
- Events related to logging: actions taken following a failure of the logging function;
- Connecting / disconnecting users with trusted roles, and corresponding unsuccessful attempts.

Other events are also collected. It is those concerning safety and not automatically generated by computer systems:

- Physical access (recorded electronically);
- The logical access to systems;
- The actions of maintenance and configuration changes in manually registered systems;
- Changes in personnel;
- Operation of disposal and reset of media containing confidential information (keys, activation data, personal information on Subscribers).

Specific events to different functions of the TSA are also logged:

- Events related to life-cycle of TSU keys and associated CA certificates or activation data (generation, backup and recovery, revocation, destruction, disposal of media, ...);
- Events related to good functioning of time-stamping services;
- Events related to synchronization of clocks to UTC time, including information concerning normal re-calibration or synchronization of clocks used in time-stamping and the detections of loss of synchronization.

The logging process allows real-time recording of transactions. In case of manual input, writing is made exceptions the same business day as the event. The events and specific data to be logged are documented by the TSA.

4.5.2 Retention Period for Audit Logs

The retention period for event logs on site is 1 month. Archiving of event logs is made no later than 1 month after their generation.

4.5.3 Protection of Audit Log

Only members dedicated TSA can process these files. The systems generate event logs (except for physical access control systems) are synchronized to a reliable source of UTC time (cf. 6.8. Timestamp / dating system).

4.5.4 Audit Log Backup Procedures

Security measures are implemented by any entity operating a PKI component to ensure the integrity and availability of event logs for the component considered, in accordance with the requirements of this CP. A backup is performed at high frequency to ensure the availability of such information.

4.5.5 Vulnerability Assessment

The event logs are monitored once per workday to identify abnormalities related to failed attempts (access or instruction).

Event logs are analysed in their entirety to the frequency of at least once every workday and upon detection of an abnormality. A summary analysis is produced for the occasion.

A reconciliation between the various logs of functions that interact with each other is made at the rate of at least 1 time per week to verify the correlation between dependent events and to reveal any abnormality. The auditor is assisted by a person with skills related to the different environments used.

4.6 Records Archival

4.6.1 Types of Records Archived

TSA is archiving:

- Event Logs of various components of the TSA;
- The TP;
- The TPS;
- The certificates issued for the TSU and associated CA;
- The requests for revocation ;
- The CRL issued for the TSU and associated CA;

4.6.2 Retention Period for Archive

4.6.2.1 Certificates, CRL / ARL and OCSP responses issued by the CA

Certificates of Subjects and of CA, and the CRL / ARL, are archived for at least seven years after their expiration. OCSP responses produced are archived for at least two years after their expiration.

4.6.2.2 Event logs

Event logs specified in Chapter 4.5.1 are archived for seven years after their generation.

4.6.3 Protection of Archive

During the time of their conservation, the archives are protected in integrity. They can be played back and used by the dedicated members of the TSA. Write access to these files is protected (rights management). Access to read the logs (stored on NetApp servers) is only possible from a machine identified and authorized in the internal networks.

4.6.4 Archive Backup Procedures

The mirroring process (automatic or manual in case of recovery) guarantees the existence of a backup of the entire archive.

4.6.5 Archive Collection System

Archiving is achieved with archiving servers which ensure the availability, integrity and confidentiality of archives.

4.6.6 Procedures to Obtain and Verify Archive Information

Archives can be recovered only by the dedicated members of the TSA authorized to process these files within a maximum of two workdays. Data about contractors can be retrieved on their request.

4.7 TSA Compromise and disaster recovery

4.7.1 Procedure for reporting and processing incidents

Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

The TSA address any critical vulnerability not previously addressed, within a period of hours after its discovery. If this is cost effective given the impact, the TSA shall create and implement a plan to mitigate the vulnerability, or the TSP shall document the reason why the vulnerability will not be treated.

In the event of a major incident, such as loss, suspicion of compromise, compromise, theft of the private key of the CA, the triggering event is the finding of this incident in the component concerned, which must inform the TSA immediately.

The TSA will notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSA shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

4.7.2 TSA compromise

In the event of a major incident which affects the security of time-stamping services, including the compromise (real or suspected) of the signing private key of a TSU or the detected loss of calibration of time-stamps that affects the issued time-stamp, TSA has defined and maintain a Business Continuity Plan.

The Business Continuity Plan provides that appropriate information is made available to subscribers and users of time-stamps with a description of the compromise that's happened. The TSA will take all necessary measures to ensure that the time-stamps of the TSU are not generated until actions are taken to restore the situation.

Whenever possible, the TSA will make available to all its subscribers and users of time-stamps any information that may be used to identify time-stamps that may have been affected, unless this contravenes Subscriber privacy or security of time-stamping services.

The contact identified on the website of the ANSSI (https://www.ssi.gouv.fr) will be immediately informed.

4.7.3 Business Continuity Capabilities after a Disaster

The various components of the PKI have the necessary means to ensure the continuity of their activities in accordance with the requirements of the Time-stamp Policy.

The TSA uses the redundancy of its information systems into several sites and its Business continuity plans to ensure the services continuity.

4.8 TSA Termination

One or more components of the TSA may have to stop working or to transfer it to another entity. The transfer of activity is defined as:

- The End of the activity of a TSA component having no effect on the validity of TSU's certificates issued prior to the transfer;
- The resumption of this activity organized by the TSA in collaboration with the new entity.

The cessation of activity is defined as the end of the activity of a TSA component influencing the validity of TSU's certificates issued prior to the relevant termination.

To ensure a constant level of confidence during and after such events, the CA takes the following actions:

- The TSA will make available to all its subscribers and users of time-stamps the information concerning its transfer or its cessation of activity;
- The TSA shall revoke the authorizations given to the subcontractors to act on its behalf in the execution of any functions relating to the process of generating time-stamps.
- The TSA will transfer to a reliable body its obligations to maintain the records and archives necessary to demonstrate its proper functioning for a reasonable period of time.
- The TSA will maintain or transfer to a reliable organization its obligations to make available to users of time-stamps for a reasonable period its public keys and its certificates;
- The TSA will revoke TSU certificates.
- The TSA will destroy the private keys of the TSU and their copies in such a way that they cannot be recovered.
- The TSA will indicate in its TP the arrangements made for the end of the service including:
  - A notice to subscribers and users of time-stamps.
  - A transfer of the obligations of the TSA to other bodies.
- It carries information to the administrative authorities. In particular, contact of the ANSSI is warned (https://www.ssi.gouv.fr). The CA will inform him including any obstacles or additional delay encountered during the process of transfer or retirement.
- The TSA will take the necessary measures to cover the expenses to fulfil these minimum requirements in case the TSA goes bankrupt or for other reasons would be unable to cover the expenses by itself.

If the TSA is bankrupt, it is the commercial court which decides on the follow-up to the company's operations. Nevertheless, if any, CA is committed to supporting the commercial court under the following conditions: before bankruptcy, there is a prior period, generated most of time by several alert procedures or by a legal redress; during this period, TSA is committed to preparing for the commercial court, if appropriate, a proposal to transfer TSU certificates to another authority with the same level of certification.

5 TECHNICAL SECURITY CONTROLS

5.1 TSU keys management

5.1.1 Generation of TSU key pairs

The TSA ensures that all cryptographic keys of TSU are produced in circumstances controlled and described by the TSA.

The generation of the TSU's signing keys:

- is undertaken in a physically secured environment by personnel in trusted roles under, at least, dual control;
- is carried out within a secure cryptographic device compliant with the requirements of chapter 5.3 below.

The TSU's keys cans be stored in different cryptographic modules for availability needs. In this case, their public keys certificates are the same.

A TSU has a single time-stamp signing key active at a time.

5.1.2 Required algorithms

The TSA, within the limits of the algorithms it recognizes:

- supports hash values generated by subscribers and uses hash algorithms compliant with requirements of the ANSSI and of ETSI specifications. The TSA supports at least the following algorithms: SHA256, SHA384, SHA512.
- Generates time-stamps signed according to the algorithms and key lengths conforming to the requirements of the ANSSI and of the ETSI specifications. The TSU key pairs have the following characteristics: Key pairs RSA 2048 bits / Hash algorithm SHA-256 (256 bits).

5.1.3 TSU private key protection

The TSA ensures that TSU's private keys are remained confidential and their integrity is maintained. TSU's private keys are kept and used inside a cryptographic module compliant with the requirements of chapter 5.3 below.

5.1.4 TSU certificate

The TSA guarantees the integrity and authenticity of the TSU signature verification (public) keys:

- The TSU signature verification (public) keys is made available to relying parties in a public key certificate.
- The TSU not issues time-stamps 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 verify that this certificate has been correctly signed (including verification of the certificate chain to a trusted certification authority).

The validity period of TSU's certificate is fixed to 3 years. This period is no longer than:

- the cryptographic lifetime of the associated private key;
- the end of validity of CA certificate that issued it.

5.1.5 TSU private key use duration

The duration of use of a TSU private key is limited to 1 year. The duration of use of a key is reduced so that the validity of the time-stamps generated with this key can be carried out for at least 2 years.

The TSA guarantees that TSU private keys are not used beyond the end of their life cycle via procedures in place to ensure that a new key pair is set up when the end of The period of use of a UH private key has been reached.

5.1.6 TSU private key destruction

The TSA ensures the destruction of the private key and its copies when the end of the period of use of this private key has been reached.

5.1.7 TSU private key archiving

The TSU private keys are archived in no case.

5.1.8 TSU private key copies

For each TSU private key, a backup copy is positioned in another system compliant with the requirements of the chapter 5.3 below. Their export outside the cryptographic module If necessary is under an enciphered form and with an integrity control mechanism.

The corresponding encryption provides a level of security equivalent to or greater than the storage within the cryptographic module, and is based on an algorithm, a key length and

an operating mode capable of withstanding cryptanalytic attacks for at least the lifetime of the key.

The Backup copy is not used for timestamp token issuance so that only the initial private key is active.

TSU private keys are handle only by personnel in trusted roles using, at least, dual control in a physically secured environment. Personnel authorized to implement backup copies of the keys is limited to do so in accordance with the practices of the TSA.

The Certigna Entity CA's Certification Practice Statement describes in details the measures implemented.

5.2 TSU Certificates and CRL profiles

See section 7 of the following CA's Certification Policies available at the address https://www.certigna.com/autorites-de-certification/ :

- Certigna Entity CA *[CA currently used]*
- Certigna Time Stamping CA *[CA used in the future]*

5.3 TSU cryptographic module management

5.3.1 Life cycle management of TSU cryptographic module

The TSA ensures that:

- Time-stamp signing cryptographic hardware is not tampered with during shipment and is not tampered with when and while stored.
- Installation, activation and duplication of TSU's signing keys in cryptographic hardware are 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 are erased upon device retirement in a way that it is practically impossible to recover them.

5.3.2 Security objectives for TSU cryptographic module

The device used by the TSA to store and implement its TSU private keys and to generate time-stamps meets the security requirements formulated in the corresponding Certification Policy, including the following requirements:

- Ensure that TSU key generation is performed exclusively by authorized users and guarantee the cryptographic robustness of the generated key pairs;
- Ensure the confidentiality and integrity of the TSU private keys of signature throughout their life cycle, and allow their safe destruction at the end of their life;

- Guarantee the authenticity and integrity of the public keys when they are exported from the module;
- When importing into the module, check the correspondence between the imported certificate and the TSU public key contained in the module;
- Be able to identify and authenticate users;
- Limit access to its services according to the user and the role assigned to him;
- Be able to conduct a series of tests, during initialization, customization and operation, to verify that it is working correctly and enter in a safe state if it detects an error;
- be able to detect attempts at physical alterations and enter in a safe state when an alteration attempt is detected;
- Allow to create a digital signature, to sign the countermarks of time generated by the TSU, which does not reveal the private keys of the UH and which can not be falsified without the knowledge of these private keys;
- Create audit records for each security change;
- Guarantee the synchronization of its clock with UTC time according to the precision defined in the TPS;
- Provide time-stamps in accordance with requests received.

5.3.3 Qualification of TSU cryptographic module

The cryptographic module used for TSU complies to following requirements:

- The module is qualified/certified in compliance with the Certification Policy of TSU certificates,
- The module is FIPS 140-2 Level 3 certified, or Common Criteria EAL4 or superior.

5.4 Time management

5.4.1 Declared accuracy

The declared accuracy is of 1 second.

5.4.2 Clock synchronization with UTC

The TSU ensures that its clock is synchronized with UTC within the declared accuracy:

- The calibration of the TSU clocks is maintained such that the clocks do not drift outside the declared accuracy.
- The TSU clocks are protected against threats which could result in an undetected change to the clock that takes it outside its calibration.
- The TSA detects if the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC.
- 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.
- The clock synchronization is 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.

Note: A leap second is an adjustment to UTC by skipping or adding an extra second on the last second of a UTC month. First preference is given to the end of December and June, and second preference is given to the end of March and September.

5.5 Time-stamps management

5.5.1 Time-stamp requests management

The time-stamps are issued securely and include the correct time with the declared accuracy. The time values the TSU uses in the time-stamp are traceable to at least one of the real time values distributed by a UTC(k) laboratory.

Note: The Bureau International des Poids et Mesures (BIPM) computes UTC on the basis of its local representations UTC(k) from a large ensemble of atomic clocks in national metrology institutes and national astronomical observatories round the world. The BIPM disseminates UTC through its monthly Circular T [i.6] (list 1). This is available on the BIPM website (www.bipm.org) and it officially identifies all those institutes having recognized UTC(k) time scales.

The time-stamps are signed using a key generated exclusively for this purpose. The time-stamps generation system rejects any attempt to issue time-stamps when the end of the TSU private key use duration has been reached.

5.5.2 Timestamp profile

Time-stamps issued by the TSA have a TimeStampToken structure conforming to RFC 3161.

A time-stamp includes:

- The identifier of the UH certificate,
- The identifier of this time-stamping policy,
- A unique identifier linked to the time countermark.
- A representation of the data to be timed (ie the hash value and the hash algorithm identifier) as supplied by the subscriber.

Champ	Description
version	1
policy	1.2.250.1.177.2.9.1.1
messageImprint	SHA256
serialNumber	Positive serial number
genTime	YYYYMMDDhhmmssZ
accuracy	1 second
ordering	Absent
nonce	Similar to the value present in the query where applicable.
tsa	Subject DN of TSU certificate
extensions	id-etsi-tsts-EuQCompliance [Not critical]

5.5.3 Time-stamp verification

The time-stamps users can access to usable information for checking the signing of time-stamps through the following means:

- The TSU certificates joined to the time-stamps,
- The chain of trust associated to TSU certificates available at the following address: https://www.certigna.com/autorites-de-certification/

The UH certificate includes:

- An identifier of the country in which the TSA is established,
- An identifier of the TSA,
- An identification of the TSU which generates time-stamps.

5.6 Operation security

5.6.1 Security for IT systems

A minimum level of safety assurance on the computer systems of persons in trusted role is ensured by:

- Strong identification and authentication of user for system access (physical access control to enter in the room + logic control by id / password or certificate to access the system);
- Management of user sessions (logoff after idle time, file access controlled by role and user name);
- User rights management (to implement the access control policy defined by the TSA, to implement the principles of least privilege, multiple controls and separation of roles);
- Protection against computer viruses and other forms of compromise or unauthorized software and software updates;
- Manage user accounts, including changes and the rapid removal of access rights;
- Network protection against intrusion of an unauthorized person using the firewall;
- Secure inter-site communication (tunnel IPSec VPN) ;
- Audit Functions (non-repudiation and nature of the actions performed).

Monitoring devices and audit procedures of the system settings, including routing elements, are in place.

Certigna is committed to an availability rate of 99.9%, it being specified that an unavailability will be the result of a critical incident defined as the complete interruption of the timestamping service.

5.6.2 Deployment and maintenance

The TSA employs trusted products and systems.

An analysis of security requirements is carried out at the time of the design and specification stage of requirements for any system development projects undertaken by the TSA or on behalf of the TSA to ensure that security is part of the information system.

Change control procedures are applied for new versions, modifications and fault corrections of any operational software.

5.6.3 System planning

Capacity demands are monitored and projections of future capacity requirements to ensure that adequate processing power and storage are available.

5.6.4 Access control

The TSP's system access is limited to authorized individuals.

Controls protect the TSP's internal network domains from unauthorized access including access by subscribers and third parties. Firewalls are configured to prevent all protocols and accesses not required for the operation of the TSA.

The TSA administers user access of operators, administrators and system auditors. The administration includes user account management and timely modification or removal of access.

Access to information and application system functions is restricted in accordance with the access control policy. The TSA system provides sufficient computer security controls for the separation of trusted roles identified in TSA's practices, including the separation of security administration and operation functions. Particularly, use of system utility programs is restricted and controlled.

TSA personnel is identified and authenticated before using critical applications related to the service.

TSA personnel is accountable for their activities.

Sensitive data are protected against being revealed through re-used storage objects being accessible to unauthorized users.

5.7 Security measures for the systems during their lifecycle

5.7.1 Security measures linked to the development of the systems

According to the risk analysis conducted, during the design of any new development project, an analysis of security is achieved and approved by the TSA Security Committee.

The configuration of TSA systems and any changes and upgrades are documented. The development is done in a controlled and secured environment requiring a high level of authorization.

To enable its prospects or future customers to test some of their dematerialized trading applications, CA has set up a test CA issuing TSU certificates identical in all respects to the production certificates (only the certificate issuer is different). This test CA has its own private key. The public key certificate is self-signed. These certificates are used for testing purposes only.

The CERTIGNA solutions are tested in a development/test environment before being used in the production environment. Production and development environments are separated.

5.7.2 Measures related to security management

Any significant change to a system of a component of the PKI is documented and reported to the CA for validation.

5.8 Network security measures

Interconnection to public networks is protected by security gateways configured to accept only the necessary protocols to the desired operation by the TSA.

The TSA guarantees that the components of the local network are kept in a physically secure environment and their configurations are periodically audited for compliance with the requirements specified by the CA.

Controls are implemented to protect the TSA's internal network from unauthorized access including access by subscribers and third parties.

The TSA segments its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services. The TSA applies the same security controls to all systems located in the same zone.

The TSA restricts access and communications between zones to those necessary for the operation of the TSA. Not needed connections and services are explicitly forbidden or deactivated. The established rule set are reviewed on a regular basis.

The TSA maintains any elements of its critical systems in a secured zone.

A dedicated network for administration of IT systems that is separated from the operational network shall be established. Systems used for administration are not used for non-administrative purposes.

Test platform and production platform are separated from other environments not concerned with live operations.

Communication between distinct trustworthy systems are only established through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

The external network connection to the internet is redundant to ensure availability of the services in case of a single failure.

The TSA undergoes or performs a regular vulnerability scan and records evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

The TSA undergoes a penetration test on the TSA's systems at set up and after infrastructure or application upgrades or modifications that the TSA determines are significant. The TSA records evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

The TSA maintains and protects its systems in a secure zone.

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

Only trusted roles can access secure zones and high security zones.

[END OF DOCUMENT]

www.certigna.com