Qualified service for long-term preservation and guarantee of electronic signatures (QPS)

Policies, Practices and Procedures Statement

Version 1.4

Date: 15 January, 2026

Important Notice

Address: 29 A Tudor Vladimirescu Avenue,

AFI Tech Park 1, Bucharest, Romania

Phone: 004-021-31.19.901

Web: www.certsign.ro

Document History

Version	Effective Date[1]	Reason	Person who made the change
1.0	September 2024	First version	PKI Policies Manager
1.1	10 October 2024	Minor updates	PKI Policies Manager
1.2	30 October 2024	Corrections after audit	PKI Policies Manager
1.3	15 January 2025	Annual review	PKI Policies Manager
1.4	15 January 2026	Annual review	PKI Policies Manager

This document was created and is the property of:

Owner	Author	Date created
certSIGN	PKI Policies Manager	September 2024

Distribution List

Destination	Date distributed
Public-Internet	October 2024
Public-Internet	January 2025
Public-Internet	January 2026

This document was approved by:

Version	Name	Date
1.1	Policies and Procedures Management Body	October 2024
1.2	Policies and Procedures Management Body	October 2024
1.3	Policies and Procedures Management Body	January 2025
1.4	Policies and Procedures Management Body	January 2026

[1] Effective Date = Last day of the month, if not specified

Content

1 Introduction 7
1.1 Overview 7
1.2 Document name and identification 7
1.3 PKI Participants 7
1.3.1 certSIGN TSP for QPS 7
1.3.2 Registration authorities 8
1.3.3 Subscribers 8
1.3.4 Relying parties 8
1.3.5 Other participants 8
1.4 QPS Service usage 9
1.4.1 Appropriate QPS service uses 9
1.4.2 Prohibited QPS service uses 9
1.5 Policy administration 9
1.5.1 Organization administering the document 9
1.5.2 Contact person 10
1.5.3 Person determining PPPS suitability for the policy 10
1.5.4 PPPS approval procedures 10
1.6 Definitions and acronyms 10
1.6.1 Definitions 10
1.6.2 Acronyms 14
2 Publication and repository responsibilities 15
2.1 Repositories 15
2.2 Publication of QPS service information 15
2.3 Time or frequency of publication 15
2.4 Access control on repositories 15
3 Long-Term Preservation Service - QPS 16
3.1 Preservation goals 16
3.2 Storage Models 16
3.3 Preservation schemes 17
3.4 Long-term preservation policies 18
3.5 Process for generating preservation evidence 18
3.6 Process for validating preservation proofs 19
3.7 The process of re-auditing preservation evidence 19
3.8 Export-import document set process 19
4 QPS life-cycle operational requirements 20
4.1 QPS service registration and contracting process 20
4.2 Uploading and validation of the documents (PreservePo) 22
4.3 Reporting information (RetriveTrace) 22
4.4 Maintaining long-term validity 23
4.5 Document availability (RetrivePO & RetriveTrace) 23
4.6 Document Download (RetrivePO) 23
4.7 Deletion of documents/validation materials (DeletePO) 23
4.8 Termination of the Service Agreement 23
5 Facility, Management and Operational Controls 24
5.1 Physical Controls 24
5.1.1 Site location and construction 24

5.1.2 Physical access 25
5.1.3 Power and air conditioning 25
5.1.4 Water exposure 25
5.1.5 Fire prevention and protection 26
5.1.6 Media storage 26
5.1.7 Waste disposal 26
5.1.8 Offsite backup 26
5.2 Procedural controls 26
5.2.1 Trusted roles 26
5.2.2 Number of persons required per task 27
5.2.3 Identification and authentication for each role 27
5.2.4 Roles requiring separation of duties 27
5.3 Personnel control 28
5.3.1 Qualifications, experience and clearance requirements 28
5.3.2 Background check procedures 28
5.3.3 Training requirements 28
5.3.4 Retraining frequency and requirements 28
5.3.5 Job rotation frequency and sequence 28
5.3.6 Sanctions for unauthorized actions 28
5.3.7 Independent contractor requirements 29
5.3.8 Documentation supplied to personnel 29
5.4 Audit logging procedures 29
5.4.1 Types of events recorded 29
5.4.2 Frequency of processing log 31
5.4.3 Preservation period for audit log 31
5.4.4 Protection of audit log 31
5.4.5 Audit log backup procedures 31
5.4.6 Audit collection system (internal vs. external) 31
5.4.7 Notification to event-causing subject 31
5.4.8 Vulnerability assessments 31
5.5 Records archival 32
5.5.1 Types of data archived 32
5.5.2 Preservation period for archive 32
5.5.3 Protection of archive 32
5.5.4 Archive backup procedures 32
5.5.5 Requirements for time-stamping of records 32
5.5.6 Archive collection system (internal or external) 33
5.5.7 Procedures to obtain and verify archive information 33
5.6 Compromise and Disaster Recovery 33
5.6.1 Incident and compromise handling procedures 33
5.6.2 Recovery Procedures 34
5.6.3 Business continuity capabilities after a disaster 35
5.7 QPS termination 35
5.8 Supply chain 36
6 Technical security controls 36
6.1 Activation data 36
6.1.1 Activation data generation and installation 36

6.1.2 Activation data protection 37
6.1.3 Other aspects of activation data 37
6.2 Computer security controls 37
6.2.1 Specific computer security technical requirements 38
6.2.2 Computer security rating 38
6.3 Life cycle security controls 38
6.3.1 System development controls 38
6.3.2 Security management controls 39
6.3.3 Life cycle security controls 39
6.4 Network security controls 39
6.5 Time-stamping 41
7 Profiles, Formats, and Preservation Schemas 42
7.1 Preservation scheme with signature completion and storage 42
7.2 Preservation scheme with signature completion and temporary storage 43
7.3 Preservation scheme with signature completion and without storage 44
7.4 General data preservation and storage scheme 45
7.5 General data preservation scheme and temporary storage 46
7.6 General data preservation scheme and no storage 48
8 Compliance audit and other assessments 50
8.1 Frequency or circumstances of assessment 50
8.2 Identity/qualifications of assessor 50
8.3 Assessor's relationship to assessed entity 50
8.4 Topics covered by assessment 50
8.5 Actions taken as a result of deficiency 50
8.6 Communication of results 50
9 Other business and legal matters 51
9.1 Fees 51
9.2 Financial Responsibility 51
9.2.1 Insurance coverage 51
9.3 Confidentiality of business information 51
9.3.1 Scope of confidential information 51
9.3.2 Information not within the scope of confidential information 52
9.3.3 Responsibility to protect confidential information 52
9.4 Privacy of personal information 52
9.4.1 Privacy Plan 52
9.4.2 Information Treated as Private 52
9.4.3 Information not Deemed Private 53
9.4.4 Responsibility to Protect Private Information 53
9.4.5 Notice to use Private Information 53
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 53
9.4.7 Other Information Disclosure Circumstances 53
9.5 Intellectual Property Rights 53
9.6 Representations and warranties 54
9.6.1 certSIGN representations and warranties 54
9.6.2 Subscriber representations and warranties 54
9.6.3 Relying Party representations and warranties 54
9.6.4 Representations and warranties of other participants 54

9.7 Disclaimers of warranties 54
9.8 Limitations of liability 54
9.9 Indemnities 55
9.10 Term and termination 55
9.10.1 Term 55
9.10.2 Termination 55
9.10.3 Effect of termination and survival 55
9.11 Individual notices and communications with participants 55
9.12 Amendments 55
9.12.1 Procedure for amendment 55
9.12.2 Notification mechanism and period 56
9.13 Dispute resolution procedures 56
9.14 Governing law 56
9.15 Compliance with applicable law 56
9.16 Miscellaneous provisions 56

1 Introduction

The Policies, Practices and Procedures Statement on the **Qualified service for the long-term preservation and guarantee of electronic signatures (QPS)** – (hereinafter referred to as **PPPS-QPS** or **PPPS**) details the policies, practices and procedures that certSIGN applies on the long-term qualified preservation service for qualified signatures.

The content of the **PPPS-QPS** is compliant with the latest versions of the requirements ETSI TS 119 511 and ETSI TS 119 512.

certSIGN complies with Romanian Law no.214/2024 on the use of electronic signatures, time-stamping and the provision of trust services based on them.

1.1 Overview

certSIGN Trust Services Provider (TSP), Subscribers and affiliated Relying Parties must adhere to the current **PPPS-QPS** for the usage of the long-term qualified preservation service on qualified electronic signatures and qualified seals. This document describes the general rules for providing validation and preservation services.

1.2 Document name and identification

The title of this document is **Qualified service for the long-term preservation and guarantee of electronic signatures (QPS) - Policies, Practices and Procedures Statements** hereinafter referred to as **PPPS-QPS** or **PPPS**.

The electronic form of this document is available in the Repository at address https://www.certsign.ro/repository.

1.3 PKI Participants

certSIGN TSP regulates the most important relations between entities belonging to: certSIGN, advisory teams (including auditors) and customers (users of the services provided):

- certSIGN Trust Services Provider for QPS,
- Registration Authority,
- Repository,
- Subscribers,
- Relying Parties,
- Suppliers of certSIGN regarding digital signatures preservation and management.
- Policies and Procedures Management Body
- Auditors

certSIGN provides services for every natural or legal entity accepting the regulations of the present PPPS. The purpose of this PPPS (that includes certificates and signitures validation procedures, signature preservation procedures and information system security) is to ensure the users of the certSIGN services that the declared levels of credibility related to managed signatures comply with the certSIGN TSP's practices.

1.3.1 certSIGN TSP for QPS

certSIGN Trust Services Provider is the authority providing the long-term preservation services that deals with validity check and preservation of the electronic signatures, electronic seals, time stamps and their certificates, optionally including the signed and sealed electronic document preservation.

The Preservation service of certSIGN is identified by the following OID: 1.3.6.1.4.1.25017.5

The Qualified Preservation Service of certSIGN is identified by OID: 1.3.6.1.4.1.25017.5.2

1.3.2 Registration authorities

The Registration Authority receives, verifies and approves or rejects the registration of Subscribers requests for the use of preservation services. Verification of applications intends to authenticate (based on the documents enclosed in the applications) both the subscriber and the data specified in the request. The Registration Authority may also submit applications to the certSIGN TSP in order to cancel a subscription.

The Registration Authority is operated by certSIGN or a delegated third party.

External RAs must comply with the same security requirements that the TSP respects in terms of human resources, operational security, network and personal data as specified in this document.

1.3.3 Subscribers

Subscriber

Subscribers are legal or natural persons that request to Certsign a subscription for the preservation services usage and with whom they sign a Subscriber Agreement.

Subscribers may request the validation and/or preservation of qualified digital signatures with or without the corresponding documents. A Subscriber is also responsible for immediately notifying certSIGN upon (suspicion of) private key compromise on any certificate used for the signatures in preservation.

1.3.4 Relying parties

A Relying Party, can be any entity that uses certSIGN services and makes decisions based on the validity of the applied digital signatures / timestamps on the preservation documents.

A Relying Party is responsible for how it verifies the current status of a signature/ timestamp. Such a decision shall be taken every time a Relying Party is willing to rely on an electronic signature/ timestamp. A Relying Party shall use the information in a digitally signed document only after applying to a trusted validation service to decide whether a signature was used according to the stated purpose.

1.3.5 Other participants

Policies and Procedures Management Body (PPMB) is a committee created in certSIGN by the Board in order to supervise the entire activity of all certSIGN Authorities. The roles and responsibilities of PPMB are described in certSIGN internal documentation.

certSIGN services providers: external providers supporting certSIGN activities under a signed contractual agreement.

Public Notaries or Lawyers: may perform identification and guarantee for the real identity of the Subjects, according to Romanian law.

Qualified Electronic Signature Creation Device Providers: the external providers supporting certSIGN activities under a signed contractual agreement ensure the provision of physical cryptographic devices utilized by Subscribers.

1.4 QPS Service usage

The service applicability area sets the purpose in which this may be used. This scope is defined by two elements:

- One that defines the service applicability (for example signature or seal validity, signature/seal and/or document preservation, integrity),
- And another that entails a list or a description of the allowed and prohibited applications.

The Relying Party is responsible for setting the credibility level necessary for a signature/ timestamp to be used for a certain purpose. The Relying Party shall decide, by taking into consideration the significant risk factors, what type of signature meets the formulated requests.

The QPS service offers:

1) providing evidence of the existence over long periods of time of general data, regardless of whether this data is signed or not;

2) to preserve over long periods of time the ability to validate a digital signature, to maintain its validity, status and to obtain proof of the existence of associated signed data; and/or

3) augmenting/maintaining the preservation evidence submitted to the QPS service

1.4.1 Appropriate QPS service uses

The QPS services may be used in applications that properly manage digital signatures/ timestamps and public/private keys.

The applications for which the Signature is deemed to be trustworthy shall be decided by the Relying Parties themselves based on the nature and purpose of the Signature, including any applicable limitation as written in the Signature/Certificate.

It is the responsibility of the Subscriber to use the QPS service according to this PPPS.

It is the Subscriber's responsibility to use software applications that correctly interprets, displays and uses the information and restrictions encoded in the signatures/certificates, such as but not limited to: key usage, limited liability per transaction, etc.

It is the responsibility of the Subscriber and the Relying Party to decide for which purpose the signatures/ timestamps are considered trustworthy. A Relying Party must always take into account the level of assurance and other information in the PPPS before deciding on the applicability of the signature.

1.4.2 Prohibited QPS service uses

Any usage of a service other than the usage explicitly allowed in the PPPS, is prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

The present document is administered by the certSIGN Trust Service Provider (TSP) through the Policies and Procedures Management Body (PPMB). The PPMB includes senior members

of the management as well as staff responsible for the operational management of the certSIGN TSP PKI environment.

Name	S.C. certSIGN S.A. Office: 29 A Tudor Vladimirescu Avenue, AFI Tech Park 1, Bucharest, Romania Trade Register Number: J40/484/2006 Tax registration code: RO 18288250 Registered office: 107A Oltenitei Street. building C1, fl.1, room 16, District 4, Bucharest, Romania, PC 041303
Phone	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Table: 1.5.1 Organization administering the document

1.5.2 Contact person

Name	Policies and Procedures Management Body (PPMB)
Phone	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Table: 1.5.2 Contact person

1.5.3 Person determining PPPS suitability for the policy

Name	Policies and Procedures Management Body
Phone	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Table: 1.5.3 Person determining PPPS suitability for the policy

1.5.4 PPPS approval procedures

Policies and Procedures Management Body is responsible for the approval of the PPPS.
Subscribers shall adhere to the PPPS implemented and published at: http://certsign.ro/repository.
Subscribers who do not accept the new, modified terms and regulations of PPPS shall make a suitable statement within 15 days of the date of the new version of PPPS publication. This will lead to termination of the contract related to the QPS services provided.

1.6 Definitions and acronyms

1.6.1 Definitions

Auditor - person who assesses the compliance with the requirements as specified in given requirements documents
Authentication – electronic process that enables the electronic identification of a natural or legal entity, or the origin and integrity of electronic data to be confirmed
Certificate – a Subject's public key, together with some additional information, rendered un-forgeable by encryption with the private key issued by a certification authority
Certificate Revocation List (CRL) –a signed list indicating a set of certificates that are no longer considered valid by the TSP.
Certification Authority - authority trusted by one or more users to create and assign certificates

Certification Authority Revocation List - a revocation list with CA-certificates issued to certification authorities that are no longer considered valid by the TSP
Certification Practice Statement (CPS) – a statement of practices which a Certification Authority employs in issuing, managing, revoking, and renewing or re-keying certificates
Policies, Practices and Procedures Statement (PPPS) – a statement of the policies, practices and procedures which a TSP employs in providing a trust service
Cross- certification – a certificate that is used in order to establish a reliable relationship between two certification authorities
Data Object - actual binary/octet data being operated on (e.g. transformed, digested, or signed) by an application and which may be associated with additional information like an identifier, the encoding, size or type.
Electronic signature – data in electronic form that are attached to or logically associated with other data in electronic form and which are used by the signatory to sign
EU qualified preservation service - preservation service that meets the requirements for qualified preservation service for qualified electronic signatures and/or for qualified electronic seals as laid down in Regulation (EU) 910/2014
Export-import package - information extracted from the preservation service including the submission data object (SubDO), the preservation evidence and preservation-related metadata, allowing another preservation service to import it in order to continue to achieve the preservation goal based on this information.
Long-term - time period during which technological changes may be a concern
EXAMPLE: Possible technological changes are obsolescence of cryptographic technology such as crypto algorithms, key sizes or hash functions, key compromises.
Long-term preservation - Extension of the validity status of a digital signature over long periods of time and/or extension of provision of proofs of existence of data over long periods of time, in spite of obsolescence of cryptographic technology such as crypto algorithms, key sizes or hash functions, key compromises or of the loss of the ability to check the validity status of public key certificates.
Metadata - data about other data. NOTE: See ISO 14721:2012.
Object identifier (OID) – alphanumeric / numeric identifier registered in accordance with the ISO/IEC 9834 standard and uniquely describing a specified object or its class.
Preservation evidence - evidence produced by the preservation service which can be used to demonstrate that one or more preservation goals are met for a given preservation object.
Preservation evidence augmentation - addition of data to an existing preservation evidence to extend the validity period of that evidence.
EXAMPLE: Adding a new time-stamp protecting additional validation data which can be used to validate a previous signature and/or time-stamp, and/or the hash of the protected data using a stronger hash algorithm.
Preservation evidence policy - set of rules that specify the requirements and the internal process to generate or how to validate a preservation evidence.
Preservation goal - one of the following objectives achieved during the preservation time frame: extending over long periods of time the validity status of digital signatures, providing proofs of existence of data over long periods of time, or augmenting externally provided preservation evidences.
NOTE: A preservation service can achieve one or more preservation goals.
Preservation interface - component implementing the preservation protocol on the side of the preservation service.

Preservation object - typed data object which is submitted to, processed by or retrieved from a preservation service.
Preservation object identifier - unique identifier of a (set of) preservation object(s) submitted to a preservation service.
Preservation period - for a preservation service with storage, duration during which the preservation service preserves the submitted preservation objects and the associated evidences.
NOTE: The submitted preservation objects can be updated during the preservation period.
Preservation profile - uniquely identified set of implementation details pertinent to a preservation storage model and one or more preservation goals which specifies how preservation evidences are generated and validated.
Preservation protocol - protocol to communicate between the preservation service and a preservation client.
Preservation scheme - generic set of procedures and rules pertinent to a preservation storage model and one or more preservation goals which outlines how preservation evidences are created and validated.
Preservation service - service capable of extending the validity status of a digital signature over long periods of time and/or of providing proofs of existence of data over long periods of time.
Preservation service provider - trust service provider providing a preservation service.
Preservation service policy - trust service policy for a preservation service.
Preservation service practice statement - trust service practice statement for a preservation service.
Preservation storage model - one of the following ways of implementing a preservation service - with storage, with temporary storage, without storage.
Preservation subscriber - legal or natural person bound by agreement with a preservation trust service provider to any subscriber obligations
Proof of existence - evidence that proves that an object existed at a specific date/time
Proof of integrity - evidence that data has not been altered since it was protected
NOTE: A proof of existence requires and implies a proof of integrity.
Private key – one of the asymmetric keys belonging to a Subject and used only by that Subject. In the case of asymmetric key system, a private key describes the transformation of a signature. In the case of asymmetric encryption system, a private key describes decrypting transformation. The private key is (1) the key whose purpose is decryption or signature creation, for the sole usage of the owner; (2) that key from a key pair which is known only to the owner.
Public key – one of the keys from a Subject's asymmetric key pair which may be available to the public. In the case of asymmetric cryptography system, the public key defines the signature verification transformation. In the case of asymmetric encryption, a public key defines messages' encryption transformation.
Public Key Infrastructure (PKI) – architecture, techniques, practices and procedures that collectively support the implementation and operation of certificate-based public key cryptography systems; PKI consists of hardware, software, databases, network resources, security procedures and legal obligation joined together, which collaborate to provide and implement certificate services, as well as other services, associated with the infrastructure (e.g. time stamp).

Qualified Certificate for Electronic Signature - a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of the Regulation (EU) 910/2014;
Qualified Certificate for Electronic Seal - a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III of the Regulation (EU) 910/2014;
Qualified Electronic Signature Creation Device refers to an electronic signature creation device that meets the requirements laid down in Annex II of the Regulation (EU) 910/2014
Regulation (EU) no. 910/2014 - REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and the repealing Directive 1999/93/EC
Registration Authority - entity that is responsible for identification and authentication of subjects of certificates mainly
Root CA - certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s)
Subject: entity identified in a certificate as the holder of the private key associated with the public key provided in the certificate
Subordinate CA - certification authority whose Certificate is signed by the Root CA, or by another Subordinate CA
Subscriber – legal or natural entity bound by agreement with a trust service provider to any subscriber obligations
Time-stamp - data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time
Time-stamping authority - trust service provider which issues time-stamps using one or more time-stamping units
Time-stamping service - trust service for issuing time-stamps
Time-stamping unit - set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time
Trust service provider - a natural or a legal entity who provides one or more trust services either as a qualified or as a non-qualified trust service provider;
Trusted list - list that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation.
NOTE: In the context of European Union Member States, as specified in Regulation (EU) No 910/2014, it refers to an EU Member State list including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.
Validation data - data that is used to validate a digital signature

1.6.2 Acronyms

AUG	Augmentation goal
CA	Certification Authority
CARL	Certification Authority Revocation List
CRL	Certificate Revocation List
DN	Distinguished Name
EUMS	European Union Member State
NIMB	National Institute of Metrology Bucharest
OCSP	On-line Certificate Status Protocol
OVR	Overall
PDS	Preservation of Digital Signatures
PGD	Preservation of General Data
PKI	Public Key Infrastructure
PO	Preservation Object
POC	Preservation Object Container
PPMB	Policies and Procedures Management Body
PPPS	Policies, Practices and Procedures Statement
PSP	Preservation Service Provider
QES	Qualified Electronic Signature or Qualified Electronic Seal
QPS	Qualified Preservation Service
QSCD	Qualified Electronic Signature Creation Device
RA	Registration Authority
RSA	Rivest, Shamir, Adleman asymmetric cryptographic algorithm
SCVP	Server-based Certificate Validation Protocol
SigS	Digital Signature Creation Service
SubDO	Submission Data Object
TS	Trust Service
TSA	Time-Stamping Authority
TSP	Trust Service Provider
UTC	Coordinated Universal Time
ValS	Validation Service
WOS	Without Storage
WST	With Storage
WTS	With Temporary Storage

2 Publication and repository responsibilities

certSIGN publishes the PPPS at least annually, even if there are no changes.
All the procedures are annually scheduled for review and updates.

2.1 Repositories

The Repository is available on-line: https://www.certsign.ro/repository. It contains:

- The QPS Policies, Practices and Procedures Statement for the certSIGN TSP
- Terms and conditions for the use of QPS services

The Repository is managed and controlled by certSIGN; certSIGN undertakes to:

- Ensure the publishing and archiving of the PPPS, the recommended applications' lists and recommended devices,
- Provide constant access to information in the Repository for certSIGN Authorities, Subjscribers and Relying Parties,
- Ensure secure and controlled access to information in the Repository.

2.2 Publication of QPS service information

Availability
Availability of the document repository is designed to exceed 99.8% of business hours - defined as 24 hours a day, seven days a week, excluding planned maintenance periods.
Planned maintenance periods will be announced on https://www.certsign.ro at least 24 hours in advance.

In case of unavailability due to a catastrophe, failure of infrastructure outside the control of certSIGN or any other reason, certSIGN shall make best endeavours to reinstate availability of the service within 24 hours.

2.3 Time or frequency of publication

The information published by certSIGN is updated annually, or on the following events:

- PPPS updates,
- Audit reports performed by authorized institutions – when certSIGN receives them;
- Additional information – after every update.

2.4 Access control on repositories

All information published by certSIGN in the Repository at the address https://www.certsign.ro/repository is available for the public.

certSIGN implemented logical and physical protection mechanisms against unauthorized additions, deletions or modifications of the information published in the Repository.

Subscribers and Relying Parties have read-only access via the internet to all the repositories mentioned in section 2.1.

certSIGN may take reasonable measures to protect against and prevent from abusive usage of repository, the OCSP, and CRL download services.

On discovering a breach of information integrity in the Repository, certSIGN will take appropriate actions to re-establish the information integrity, will impose legal actions for those who are guilty and will immediately notify the affected entities.

3 Long-Term Preservation Service - QPS

The primary task of the long-term preservation service is the preservation of the validity of the digitally signed documents or seals placed on an electronic document.
The present PPPS defines the requirements for the long-term validity assurance of electronic signatures and seals.
certSIGN may specify and restrict the format of the accepted electronic signatures or seals, the accepted Certification Authorities and any other parameter.

3.1 Preservation goals

The Long Term Electronic Signature Preservation Service pursues different preservation objectives, which have an influence on the operational tasks supported, and which can be used separately or in combination:
- **General Data Preservation (PGD)** provides evidence of the long-term existence of the data object presented to the preservation service.
- **Digital Signature Preservation (PDS)** extends over long periods of time the ability to validate a digital signature, to maintain its validity status and to obtain a proof of existence of the associated signed data.
- **Augmentation (AUG)** indicates that the preservation service supports the enhancement of the preservation evidence presented. Augmentation is done only in combinationation with the other two goals (PGD or PDS).
All of these objectives require:
The long-term preservation services cover the following goals:

- Proof of integrity of an electronic document;
- Proof of existence of an electronic document (at a time/in the past);
- Maintenance of the validity status of electronic signatures/seals over long periods;
- Data availability.

Data integrity is verified during the preservation time frame by means of a proof of integrity (hash, signature/seal).
The proof of existence indicates that the digital object(s) existed at a specific time and it is implemented by combining a proof of integrity and a trusted time indication (qualified time-stamp).
To maintain the validity status of the electronic signature/seal, all elements needed to verify the validity and which cannot be guaranteed to be available in the future, need to be preserved as well. This can include certificates, revocation information (CRLs, OCSP responses), trusted lists, etc.
Data availability is ensured by using dedicated storage devices in two different locations in a highly available configuration using a clustered backend that provides mirrored copies of all documents and associated meta-data.

3.2 Storage Models

Preservation With Storage (WST)
In this storage model, the QPS Service stores the data objects as well as the preservation records that are produced for them by the preservation service. In this model, the QPS supports the export and import of storage objects and evidence produced by itself and other storage services, provided that the storage objects and evidence are compatible with the formats supported by the QPS.
This storage model is specified by the value ***WithStorage (WST)*** in *PreservationStorageModelType.*

Preservation With Temporary Storage (WTS)

In this storage model, the QPS Service does not store data objects permanently, but only stores them for as long as necessary to create the appropriate evidence. Preservation evidence is produced asynchronously and is stored for a maximum of 5 days to allow the client to retrieve it.
For this storage model, the customer sends the complete data object to the QPS Service.
This storage model is specified by the value ***WithTemporaryStorage (WTS)*** in the *PreservationStorageModelType*.

Preservation WithOut Storage (WOS)
In this preservation storage model, the QPS Service does not store the data objects and preservation records are produced synchronously.
This storage model is specified by the value ***WithoutStorage (WOS)*** in *PreservationStorageModelType*.

3.3 Preservation schemes

A preservation scheme supports at least one preservation target and works only with one storage model.
A preservation scheme is a fairly abstract description and can be implemented by one or more preservation profiles, which are described by profile elements that can be read automatically. The Profile element describes the technical aspects of a Preservation Profile that allow a client to use the Preservation Interface to communicate with the QPS Service.
The set of Preservation Profiles supported by the QPS Service can be retrieved using the RetrieveInfo function exposed by the Preservation Service.
A Preservation Profile contains (refers to) policy-related information that addresses aspects of evidence creation and validation and signature validation if the preservation target is PDS. If the preservation target is PGD, the data received from the client will be signed by the QPS Service (via the client connected to a qualified electronic signature service) and then the elements defined in the equivalent preservation profiles defined for the PDS preservation target will be applied.

Preservation schema	Preservation Goal	Storage Model	Records/Preservation records
pds+wst+aug	PDS & AUG	WST	PAdES Document Time-Stamp[2]
pgd+wst+aug	PGD & AUG	WST	PAdES Document Time-Stamp[2]
pds+wts+aug	PDS & AUG	WTS	PAdES Document Time-Stamp[2]
pgd+wts+aug	PGD & AUG	WTS	PAdES Document Time-Stamp[2]
pds+wos+aug	PDS & AUG	WOS	PAdES Document Time-Stamp[2]
pgd+wos+aug	PGD & AUG	WOS	PAdES Document Time-Stamp[2]

[2] Conform ETSI EN 319 142-1

3.4 Long-term preservation policies

The certSIGN Preservation service is identified by the following OID: 1.3.6.1.4.1.25017.5.
certSIGN Preservation supports the following basic preservation service policies:
- OID 0.4.0.19511.1.2 - Qualified is the policy applied when the explicit requirement is for keeping qualified signatures/seals as defined in EU Regulation No 910/2014 - *itu-t(0) identified-organization(4) etsi(0) pres-service-policies(19511) policy-identifiers(1) qualified (2).*

Each policy is applied within a preservation profile, with specified preservation objectives, within a storage model, which applies a specific set of operations on specified formats (detailed in Chapter 7):

- 1.3.6.1.4.1.25017.5.2.1 With signature completion and storage
- 1.3.6.1.4.1.25017.5.2.2 With signature completion & temporary storage
- 1.3.6.1.4.1.25017.5.2.3 With signature completion and without storage
- 1.3.6.1.4.1.25017.5.2.4 General data preservation and storage scheme
- 1.3.6.1.4.1.25017.5.2.5 General data preservation scheme and temporary storage
- 1.3.6.1.4.1.25017.5.2.6 General data preservation scheme and no storage

The applied preservation evidence creation policy and a recommended preservation evidence validation policy are announced in the applicable profile/policy element, with type equal to the following URI:
- http://uri.etsi.org/19512/policy/preservation-evidence - generally applicable
- http://uri.etsi.org/19512/policy/signature-validation - applicable only to digital signature/seal (PDS) preservation when validation data is not provided by the Subscriber.

Input data formats supported by the QPS service are: pdf, PAdES.
Output data formats supported by the QPS service are: PAdES-LTA (with PAdES Document Timestamp according to ETSI EN 319 142-1).
The signature validation policies used are described in "certSIGN Paperless Validation Policies and Practices Statement for Qualified Signature/Seal Validation Service": https://www.certsign.ro/en/document/policies-and-practices-for-qualified-validation-service/

3.5 Process for generating preservation evidence

The Preservation Authority enables archiving of electronic signatures and implements technologies capable of extending the long-term resilience of electronic signatures beyond their technological validity period. The Preservation Authority integrates with the Validation Authority in order to obtain the necessary validation elements for the long-term guarantee of electronic signatures and to ensure their validation process.
The Preservation Authority allows the management of signatures in PAdES PDF/A formats. In order to guarantee the security and durability of the RSA cryptographic algorithms used, according to ETSI TS 119 312, the Preservation Authority performs processing on the signatures to generate PAdES-B-LT formats that include validation information (Signatures with Long-Term Validation Material), and then maintains the signatures using stronger formats such as PAdES-B-LTA (Signatures providing Long-Term Availability and Integrity of Validation Material).
These processes involve applying qualified timestamps or qualified seals over the whole of the preservation evidence.
The details of TimeStamp creation and operations process, procedures and algorithms are detailed in "certSIGN Time Stamping Authority 2 Disclosure Statement": https://www.certsign.ro/en/document/certsign-tsa-2-disclosure-statement/

3.6 Process for validating preservation proofs

The Electronic Signature Validation Authority is a centralised server-based component with advanced validation capabilities for incoming digital signatures. In addition to signature validation, the component also collects the information required for validation, verifies it and adds it to the signature in order to provide the information required for long-term signature preservation and validation. The obtained formats are sent back to the user or can be further processed at the preservation service level for archiving and long-term assurance purposes. For the validation of a signature several aspects are considered such as the integrity of the signed data, the availability and validity of the information needed for validation, the harmonisation with the policies of the certification authorities operated at the certificate providers' level, the generation of signature formats that provide the necessary material for long-term validation.

The details of the validation process used are described in "certSIGN Paperless Validation Policies and Practices Statement for Qualified Signature/Seal Validation Service": https://www.certsign.ro/en/document/policies-and-practices-for-qualified-validation-service/

3.7 The process of re-auditing preservation evidence

In accordance with the service contract signed with the Subscriber, certSIGN may provide for periodic re-auditing of the preservation evidence by applying qualified time stamps or qualified seals over all the preservation evidence.
The Preservation Service uses certSIGN Time Stamping Authority (TSA), which issues time stamps (according to ETSI EN 319 422) and certSIGN Signature or Seal Creation Service (SigS), which issues qualified digital signatures. It will also use a Validation Service (ValS) (according to ETSI TS 119 441 and ETSI TS 119 442) to collect certification path information and revocation information.
The Long-Term Electronic Signature Preservation Service may use both internal storage and external storage under its control for the long-term preservation of electronic signatures.
In addition, the preservation service can call the customer via the notification interface to inform him of relevant events. An important type of event is that a previously applied cryptographic algorithm is expected to become weak (according to ETSI TS 119 312) and therefore the client and/or the preservation service must take additional measures.

3.8 Export-import document set process

The QPS allows the Subscriber to request the export-import package, which contains the retained data, evidence and all the information needed to validate the evidence;
Export-import package requests will be accepted as follows:
- by e-mail: the application must be submitted from a known and previously approved e-mail address;
- by physical presence: any person who has a formal power of attorney to represent the Subscriber may submit an application at the certSIGN office.
For each request received a ticket will be opened, with all the details, for tracking.
Importing large quantities of documents from different platforms requires a different approach. The format is according to Annex G of ETSI TS 119 512.
Documents must be present in their original form together with proofs of retention. The import service has to revalidate the data and check the proofs of preservation for accuracy, after which they mark the proofs again with the certSIGN time stamp.
QPS can export all documents to a Subscriber and provide both the original documents and the associated proofs of retention.

4 QPS life-cycle operational requirements

This chapter describes the basic procedures that apply to all operational activities needed to operate and maintain the preservation services provided by certSIGN.
A detailed description of the procedures related to PKI component services (CAs, RAs, CRLs signers, OCSP responder, etc.) and the persons/roles involved in the operational process of these components is included in the internal confidential documentation.

certSIGN QPS includes the following operational activities:

a) QPS Subscriber Registration - service contracting;
b) Upload signatures/seals or documents for long-term preservation;
c) Checking the current status of signatures/seals or documents preserved.
d) Maintaining the long-term validity of signatures/seals or documents;
e) Updating of signatures/seals or documents kept (augmentation)
f) Downloading/uploading signatures/seals or documents preserved
g) Deletion of signatures/seals or documents preserved
h) Termination of the preservation contract

certSIGN Long-Term Preservation Service (QPS) provides the following:

1. The Subscriber can upload electronic documents to the archive operated by certSIGN.
2. certSIGN QPS securely preserves the accepted digital signatures and/or the associated electronic documents and long-term validation material – and ensures during the whole preservation period that:
   - only authorized persons have access to the preserved data;
   - the entitled Subscriber has continuous access to the preserved data;
   - the preserved data cannot be modified or deleted without authorization.
3. certSIGN QPS ensures the long-term validity provision of the electronic signatures and seals, standalone or placed on the documents preserved.
4. QPS ensures the long-term readability of the signatures in the documents, during the preservation period. The preservation period is 30 years usually, except if the validity of the service agreement ceases before the end of this period.
5. The Subscriber has access continuously to the documents, signatures and seals placed by them in the archive of the QPS and to the corresponding long-term validation material, and they can download them.
6. After the reception of the input from the Subscriber, based on individual agreement, QPS could check the digital signatures or seals provided separately or on provided documents, validates and/or completes the long-term validation material, places electronic time stamps on the long-term validation material, and saves all.
7. At the request of the Subscriber QPS deletes the the signatures/seals and/or documents from its storage.

certSIGN implementation of the preservation service follows the "Operational and notification protocols" as described in chapter 8 of ETSI TS 119 511 and detailed in ETSI TS 119 512. certSIGN is in accord with the requirements of the "Preservation process" from chapter 9 of ETSI TS 119 511.
As a QTSP, certSIGN follows the requirements in Annex A of ETSI TS 119 511 for an EU Qualified Preservation Service.

4.1 QPS service registration and contracting process

The whole process is managed by a specific entity called Registration Authority or RA, which is operated by certSIGN directly or relying on a third party in accordance with national legislation.
certSIGN may delegate Subscriber identification and registration tasks to third parties who can provide methods/procedures that offer an equivalent level of assurance to the Registration Authority. In any case, certSIGN, as a trusted service provider, assumes liability for the acts or omissions of all third-party agents.

Subscriber Identification
The RA is responsible for verifying the following:
- The identity of the Subscriber, based on an identity document
- Attributes of the Subscriber, as a natural or legal person,
- Subscriber's request for the requested service.

The identification and registration process is carried out in accordance with the rules and methods described in the PPPS, RA procedures and applicable legislation.

The Subscriber is provided with the following information and documents:
- Contractual agreement (or their online address)
- Terms and Conditions (or their online address)
- PPPS online address, notifications or other documents required to be provided by/to the Subscriber (defined in the Contract Agreement with the Subscriber).

Signing the Contract Agreement
After verifying the identity of the Subscriber, the RA informs the Subscriber of its rights and obligations as well as the options and details of the agreement for the provision of long-term storage services.
The RA's responsibility is to collect the information necessary to validate the Subscriber's needs and to guide the Subscriber in choosing the desired QPS service configurations. At the same time the RA shall show the Subscriber how to use the QPS service.
The RA operator checks the documents and verifies that the information entered is complete and correct.
By signing the Contract Agreement and accepting the Terms and Conditions, the Subscriber understands and accepts the following:
- his/her/its responsibility that the information provided to the RA is accurate, complete, valid and up-to-date,
- that certSIGN retains for the duration of the contract and for 3 years from the date of conclusion of the contract, all information related to registration and enrolment, preservation request and all activities related to the updating and maintenance of the retained data,
- that in the event that certSIGN (as TSP for the preservation services) ceases its activity, this data may be transferred to a third party with the agreement of the parties,
- acknowledges the rights, obligations and responsibilities of certSIGN and other PKI participants as defined in the Subscriber Agreement and national laws,
- that the Subscriber has the obligation to inform certSIGN of any change or event that may affect the validity of the retained data.

Registration process
The registration process takes place within the RA.
The RA verifies the signed contract and fills in the registration data in the certSIGN Preservation system. The RA is responsible for the correct registration of the Subscribers' options for the correct configuration of the QPS service.
Once the registration process is completed the Subscriber is notified (by phone or email) that he/she can start using the QPS services and receives both the QPS access link and his/her account credentials (multi-factor access).

4.2 Uploading and validation of the documents (PreservePo)

QPS accepts the signatures/seals and documents to be preserved only after the identification of the Subscriber within the framework of a secure procedure. The procedure ensures the integrity, confidentiality of the signatures/seals and documents.
The signed Service agreement clearly specify which signature/seal and file format is accepted by QPS, how it verifies the electronic signatures and seals and under what conditions it accepts the electronic documents.
For documents without signature/seal certSIGN secure them by sealing with certSIGN seal.
The validity of the electronic signatures or seals on the received documents are verified using the certSIGN Validation Service (QVSA). The verification may be based on the partial or full (long-term) validation material attached to the electronic signatures or seals. Any still necessary information for the validation is collected by certSIGN QPS and preserved.
After processing the validation materials QPS places a qualified Time Stamp on each validation material. The link to any external service is through TLS mutual connections.
QPS verifies the received signatures/seals and documents as soon as possible, but no later than 24 hours from admission and send a confirmation to the Subscriber that the validation material has been compiled successfully, and it accepted documents.
If the process is interrupted somewhere, QPS notifies the Subscriber in an error message. Based on the error message it must be clearly identifiable which signture/seal or document is involved, and what was the reason for rejection.
If the verification on the acceptance of the signature/seal or document does not arrive to the Subscriber within the stated deadline, it shall be considered that QPS did not accepted the signature/seal or document.
certSIGN is solely responsible for the preservation of the signature/seal or document and for ensuring the long-term credibility of the included electronic signatures and seals in case of sending positive confirmation.

4.3 Reporting information (RetriveTrace)

At the request of the Subscriber, QPS issues a report on information about uploaded signatures/seals or documents. Depending on the request the report may include:

1. Confirmation that the given signatures/seals or documents have unchanged hash, so they are identical to the signatures/seals or documents with the same hash submitted by the Subscriber.
2. Time of acceptance of the signatures/seals or documents in the QPS.
3. File size
4. Number of document versions

QPS issues the report on-demand.
No knowledge of signatures/seals or stored documents is required to issue the report, as it is issued based on preservation object identifier (POID).

4.4 Maintaining long-term validity

For signatures/seals and documents submitted for long-term preservation in the QPS archive, certSIGN ensures their continued validity, as contracted, by periodically augmenting the validation materials - with a qualified timestamp applied to latest version of the preservation object, using updated algorithms.
Following each augmentation operation performed as planned certSIGN shall inform the Subscriber by a status report.

4.5 Document availability (RetrivePO & RetriveTrace)

certSIGN ensure that the Subscriber can download his signatures/seals or documents preserved in the archive and the corresponding long-term validation material during the validity period of the service agreement.
The Subscriber may also request a history of the operations that have been performed on its documents.
The Subscriber only has access to the signatures/seals or documents and the long-term validation material preserved in the archive of the QPS through a secure channel.
certSIGN ensures that every Subscriber only have access to his signatures/seals or documents and the long-term validation material to which he is really entitled to access.

4.6 Document Download (RetrivePO)

certSIGN QPS makes available to the Subscriber, depending on the agreements, that by using the software and hardware devices of the QPS, they may download their preserved documents stored by QPS.

4.7 Deletion of documents/validation materials (DeletePO)

certSIGN QPS makes available the selective deletion of the signatures/seals or documents and all the corresponding validation materials preserved in the archive at the request of the Subscriber. The deletion means the physical deletion of the preserved signatures/seals or documents and its overwriting in such a way that it cannot be restored (or only with unrealistically high financial expenditure) from the data medium later. The deletion is performed on the whole system of the certSIGN QPS, and during the deletion will destroy every preserved copy of the signatures/seals or documents.
certSIGN specify in the Subscriber Agreement the manner and conditions of the admission and processing of the deletion request.

4.8 Termination of the Service Agreement

In case of the termination of the contract certSIGN makes available the signatures/seals or documents and the long-term validation material commissioned by the Subscriber to be preserved for download to the Subscriber or to another entitled person.
After the termination of the contract certSIGN deletes the signatures/seals or documents and the long-term validation material corresponding to the Subscriber.

5 Facility, Management and Operational Controls

As a Trust Service Provider, certSIGN places security at the core of its activities. In order to ensure that all of its assets, activities and services are secure, certSIGN has implemented, maintains and continuously improves an ISO 27001:2022 certified information security management system. In accordance with the requirements of this security framework, all security activities start with a risk assessment to identify and classify all the information assets, to evaluate the risks they are exposed to and to determine the required technical, managerial, organizational and procedural controls. certSIGN maintains an inventory of all information assets and assigns them a classification consistent with the risk assessment.

All those controls related to the TSP assets and activities are compliant with the applicable requirements from the following standards:

- ETSI EN 319 401, General Policy Requirements for Trust Service Providers
- ETSI TS 119 511, Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
- ETSI TS 119 512, Protocols for trust service providers providing long-term data preservation servicesPhysical Controls

5.1 Physical Controls

Network computer system, operator's terminals and information resources of certSIGN are located in dedicated areas, physically protected against unauthorized access, destruction or disruption of their operation. These locations are monitored. Every entry and exit, as well as power fluctuations, are recorded in the event journal (system logs). The temperature and humidity are monitored and controlled.

5.1.1 Site location and construction

All certSIGN TSP operations are conducted within a physically protected environment with controls based on the risk assessment that are meant to deter, prevent, detect and counteract the materialization of risks on its assets. We also maintain disaster recovery facilities for our TSP operations, facilities that are protected by physical security controls similar to those implemented at our primary facility. All physical security controls implemented by certSIGN are in accordance with ISO 27001 and 27002 standards and are described in detail in the security policies and procedures. Some of the most important security controls are:

- A clearly defined and protected perimeter through which all entries and exits are monitored;
- Critical components are protected with several perimeters
- An access control system configured to allow access only to those individuals appropriately cleared and specifically authorized to enter the area;
- Manned and electronic monitoring for unauthorized intrusion at all times;
- Personnel not on the access list are properly escorted and supervised;
- A site access log is maintained and inspected periodically;
- Every piece of equipment is correctly maintained to ensure its continuous availability and integrity.

5.1.2 Physical access

Physical access is controlled and monitored by an integrated alarm system. Fire prevention system, intrusion detection system and emergency power system are in place.

certSIGN work schedule is from Monday to Friday between 9.00 and 18.00. Outside this time interval, including public holidays, access to certSIGN premises is allowed only to persons authorized by the Management of certSIGN.

Visitors are permanently escorted by the authorized personnel.

certSIGN premises are divided into:

- Office areas,
- IT areas,
- Operators' area
- Administrators' area,
- Developing and testing area.

IT areas are equipped with monitored security system built on the basis of motion, intrusion and fire. Access to this area is granted only to authorized personnel. Monitoring of access rights is carried out based on electronic cards and appropriate readers, mounted next to the entry area. Every entry to and exit from the area is automatically recorded in the event log.

Access to the *operators' area* is allowed only based on an electronic card and its appropriate reader. Since all sensitive information is protected by the use of locked cabinets, while access to operator's or administrator's terminal requires prior authorization, the implemented physical security is considered adequate. Keys to the area are accessible only to authorized personnel. The area may be occupied solely by certSIGN personnel and authorized individuals, the latter being granted access only if accompanied.

Unattended individuals are not allowed in this area. Programmers and developers do not have access to sensible information. If such access is necessary, the presence of the security administrator is required. Projects being implemented and their software are tested on the development environment of certSIGN.

5.1.3 Power and air conditioning

Ventilation system is available in all areas. In the server areas, the air conditioning units are redundant, and temperature is monitored. When power failures occur, emergency power sources (UPS) allow activities to continue until the automatic intervention of the backup generator within the building. The electrical power infrastructure is designed as such that if the main power of the building is lost, all activities can continue for at least 24 hours using the backup power generator. Each server, network equipment and all the computers of the employees performing activities important for the TSP operations are also connected to UPSs. The main components of the physical security protection system are also connected to UPSs and to the backup power generator.

5.1.4 Water exposure

The risk of flood in the servers' area is mitigated by placing all the pieces of equipment in racks at minimum 15 cm from the floor level. Additionally, all data rooms are monitored by humidity sensors.

5.1.5 Fire prevention and protection

certSIGN location benefits from a fire prevention and extinction system in compliance with the corresponding standards and regulations in this field. The doors of the data rooms are fire-proof certified and all the passages in the walls are sealed with fire-proof substances.

5.1.6 Media storage

In accordance with the requirements of the information classification policy, media containing data or backup information are handled and stored securely within the primary facility. Backup media are also securely stored in a separate location from the original media location with the same security as the primary location. Media containing sensitive data is securely decommissioned of when no longer required.

5.1.7 Waste disposal

After the preservation period expires, paper and electronic media containing information significant for certSIGN security are destroyed.

Secure deletion is made in accordance with certSIGN's Information Security policy.

5.1.8 Offsite backup

Offsite storage comprises also archives, current copies of information processed by the system and installation kits of certSIGN applications. It enables emergency recovery of every certSIGN function within 24 hours in certSIGN's disaster recovery location.

5.2 Procedural controls

5.2.1 Trusted roles

All the roles involved in the provisioning of certSIGN's services are assigned to employees of certSIGN.

All certSIGN's employees are committed under signature to not have conflicting interests with certSIGN, to maintain confidentiality of information and to protect personal data.

certSIGN ensures a separation of duties for critical functions in order to prevent one person from maliciously using the TSP systems without detection.

The security of information processed by certSIGN and of its services is enforced trough procedural controls related to access control. Thus, access to information and application system functions is restricted in accordance to the Access Control Policy. certSIGN manages access rights of operators, administrators, and system auditors. The administration includes user account management and timely modification or removal of access. Sufficient computer security controls for the separation of the identified trusted roles, including the separation of security administration and operation functions, are provided. Particularly, the use of system utility programs is restricted and controlled.

certSIGN may assign at least the following trusted roles to one or more individuals:

- **Security officer** – Overall responsibility for the implementation of the security practices and policies.
- **System administrator (System/Network Administrator)** – Authorized to install, configure and maintain the TSP's trustworthy systems. Installs hardware and operating systems; installs and configures the network equipment.

- **System operator (Application Operator/DB Administrator)**– Responsible for operating the TSP's trustworthy systems on a day to day basis. Authorized to perform system backup and recovery. Provides continuity of backup copies and archives of database and system logs creation; manages databases; has access to confidential information about Subscribers but is not allowed to physically access any other system resources; transfers archive copies and current backup copies to the designated premises.
- **Registration Officers** (**Processing Operator**) Responsible for verifying information that is necessary for enrollment to the use of TSP services;
- **System Auditor** – Authorized to access archives and audit logs of the TSP's trustworthy systems. Responsible for performance of internal audit, compliance of the TSP with this PPPS.

The role of the **auditor** cannot be combined with any other role in certSIGN. No entity having assigned any other role different than an auditor may take auditor's responsibilities.

Employees are formally appointed to trusted roles by the Policies and Procedures Management Body (PPMB). The "least privilege" principle is applied when assigning access rights to trusted roles.

5.2.2 Number of persons required per task

Where dual or multiple control is required, at least two distinct persons, with relevant trusted roles are present in order to be able to perform the operation.

Circumstances requiring dual or multiple control are described in the internal confidential documentation.

5.2.3 Identification and authentication for each role

Each certSIGN employee acting in a trusted role is identified and authenticated to access the infrastructure to conduct his role by means of at least 2 factors authentication credentials.

Every assigned account:

- Is unique and directly assigned to a specific person,
- Is not shared with any other person,
- Is restricted according to function (arising from the role performed by a specific person) based on the certSIGN software system, operating system and application controls.

All actions of employees in trusted roles are traceable and full accountability is ensured.

5.2.4 Roles requiring separation of duties

certSIGN implements and enforces a separation of roles and duties for the roles of Administrator, Operator, and Auditor to ensure that the same person cannot hold multiple roles. All those roles have job descriptions, with specific skills and experience requirements, defined from the viewpoint of roles fulfilled. Segregation of duties and least privilege principles are in force. Position sensitivity based on duties determines the access levels, background screening and employee training and awareness.

Procedures are established and implemented for all trusted and administrative roles that have an impact on the provision of services.

5.3 Personnel control

certSIGN makes sure that the person performing his / her job responsibilities, arising from the acted role in TSP:

- Has graduated from at least the secondary school,
- Has understood and signed off an agreement describing his/her role in the system and his/her corresponding responsibilities,
- Has been subjected to advanced training on the range of obligations and tasks, associated with his/her position,
- Has been trained in the field of personal data protection and confidential and private information protection,
- Has signed off an agreement containing clauses related to the protection of certSIGN's sensitive information and confidentiality and privacy of Subscriber's data,
- Does not perform tasks which may lead to a conflict of interests.

Security roles and responsibilities, as specified in certSIGN's information security policy, are documented in job descriptions or in documents available to all concerned personnel.

5.3.1 Qualifications, experience and clearance requirements

certSIGN ensures that all employees involved in the delivery of certSIGN's TSP services are checked prior to employment regarding identity, trustworthiness, qualifications, expert knowledge, experiences and clearance needed and they are appropriate to be assigned trusted roles and to perform the related specific job function. Managerial personnel hold expertise and training in PKI technology and experience in information security management and risk management sufficient to carry out management functions.

5.3.2 Background check procedures

certSIGN ensures that the relevant checks are performed to prospective personnel by means of status reports issued by a competent authority, third-party statements or signed self-declarations.

5.3.3 Training requirements

Personnel performing roles and tasks arising from the employment in certSIGN have to complete the following trainings regarding:

- Requirements of PPPS,
- Procedures and security controls employed by the TSP
- Responsibilities arising from roles and tasks performed in the system,

Upon completion of the training, participants sign a document confirming their familiarization with PPPS, and acceptance of associated restrictions and obligations.

5.3.4 Retraining frequency and requirements

Trainings described in Chapter 5.3.3 have to be repeated or supplemented always in situations when significant modifications to certSIGN TSP operations are made.

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

certSIGN will take action against those responsible of policies or procedures violations, unauthorized actions, unauthorized use of authority and unauthorized use of systems. This

may include among others revocation of privileges, disciplinary actions, sanctions regulated by the Romanian labour laws, civil or criminal proceedings.

5.3.7 Independent contractor requirements

Contract personnel (external service, developers of subsystems or applications, etc.) are subjected to the same verification procedure as employees of certSIGN (see Chapters 5.3.1, 5.3.2 and 5.3.3). Additionally, when performing their task at certSIGN premises, contract personnel have to be escorted by a certSIGN employee, except those who have been cleared by the security officer and who can access internal classified information or in compliance with the laws in force.

5.3.8 Documentation supplied to personnel

certSIGN provides to personnel the following documents:

- PPPS,
- List of responsibilities and obligations associated with the acted role in the system
- Security policies and procedures

Other relevant documentation (operational procedures, work instructions, manuals) necessary for the staff to carry out their specific job functions related to the provision of certSIGN's Preservation Services is distributed during initial training, annual trainings and whenever otherwise appropriate.

5.4 Audit logging procedures

In order to manage efficiently the systems and applications used by certSIGN in its activity as a TSP services provider but also in order to audit the employees and customers actions, all the information about important, specific events generated by the systems and applications are recorded. That information, collectively known as logs is kept in such way that it can be accessed by the Relying Parties, auditors and state authorities at any time they need it, in order to provide evidence of the correct operation of the services for the purpose of legal proceedings or to detect attempts to compromise certSIGN's security. The recorded events are backed-up and kept in a secondary location.

Whenever possible the logs are created automatically. If this is not possible logs on paper will be used. Each record in a log created either automatically or by hand is preserved or disclosed during an audit, if required. The time accuracy of logs is ensured by a time server that is synchronized with at least two-time sources that can be GPS satellites or UTC (NIMB).

5.4.1 Types of events recorded

Every critical activity from certSIGN's security point of view is recorded in event logs and archived. The archives are stored on storage media that cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held. certSIGN event logs contain recordings of all activities generated by the software components within the system. These recordings are divided into three distinct categories:

- **System logs** – contain information about customer's requests and server's responses (or vice versa) at the level of the network protocol (for example http, https); the recorded data is: IP address of the station or server, performed operations (for example: searching, editing, writing etc.) and their results (for example the successful entry of a record in the database),

- **Errors** – contain information about errors at the network protocols level and at the applications' modules level;
- **Audit logs**– contain information specific for the TSP services, for example: registration, documents acceptance, preserving and augmenting, etc.

The above logs are common to every component installed on a server or on a workstation and have a predefined capacity. When this capacity is exceeded a log version is automatically created. The previous log is archived and deleted from the disk.

Every automatic or manual recording contains the following information:

- Event type,
- Event identifier,
- Event description,
- Date and time of the event occurrence,
- Identifier of the person in charge with the event.

All events relating to the QPS life-cycle are recorded.

All requests and reports relating to data updates, as well as the resulting action are logged.

All registration information, including the following, is recorded:

- Type of document(s) presented by the applicant to support registration;
- Record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable;
- Storage location of copies of applications and identification documents, including the signed Subscriber agreement
- Any specific choices in the Subscriber agreement (e.g. consent to services)
- Identity of entity accepting the application;
- Method used to validate identification documents,

In addition, certSIGN maintains internal logs of all security events and all relevant operational events in the whole infrastructure whatever the component service, including, but not limited to:

- Changes to the security policy
- Start and stop of systems;
- Outages;
- System crashes and hardware failures
- Firewall and router activities
- PKI system access attempts
- Physical access of personnel and other persons to sensitive parts of any secure site or area;
- Back-up and restore;
- Report of disaster recovery tests;
- Audit inspections;
- Upgrades and changes to systems, software and infrastructure;
- Security intrusions and attempts at intrusion.

Access to logs is exclusively allowed for the security officer, special appointed personnel, and auditors through email or formal-paper requests sent to the Security Officer.

The privacy of Subscriber information is maintained.

5.4.2 Frequency of processing log

Logs are processed continuously and/or following any alarm or anomalous event. Logs are regularly archived and backed-up.

5.4.3 Preservation period for audit log

Events' records are stored in files on the system disk until they reach the maximum allowed capacity. This whole time, they are available on-line, upon every authorized person's or process request. After exceeding the allowed capacity, journals are kept as archives and can be accessed exclusively off-line, from a certain workstation.

The archived journals of logs are kept at least 3 years.

5.4.4 Protection of audit log

The log files are properly protected by an access control mechanism. Appropriate protection against modification and deletion of the audit logs is implemented such that no one may modify or delete audit records except after transfer to long-term media for archiving purposes. Only the security officer, special appointed personnel, or an auditor can review an event journal. The access to the events journal is configured in such way that:

- Only the above entities have the right to read the journal's records,
- The central log platform automatically archives or deletes files (after their archiving) that contain recorded events,
- It is possible to identify any integrity violation; this thing ensures that the records do not contain gaps or forgeries,
- No entity has the right to modify the content of a log.

Moreover, the log protection controls are in such a way implemented that, even after log archiving it is impossible to delete records or the log as a whole before the expiration of the log global preservation time.

5.4.5 Audit log backup procedures

certSIGN security policies require that the event journal should have a periodical backup. These backups are stored in auxiliary locations of certSIGN. Log files and audit trails are backed up according to internal procedures.

5.4.6 Audit collection system (internal vs. external)

All the logs generated by servers, network devices, security equipment, applications are continuously sent to a central platform, whose purpose is to:

- Collect
- Store
- Analyse
- Correlate
- Archive
- Long term Back-up

5.4.7 Notification to event-causing subject

Not applicable

5.4.8 Vulnerability assessments

The entire infrastructure is subject to vulnerability assessment as part of the internal risk assessment and risk management procedures of certSIGN.

In order to ensure that all of its assets, activities and services are secure, certSIGN has implemented, maintains and continuously improves an ISO 27001:2022 certified information security management system. In accordance with the requirements of this security framework, all security activities start with a risk assessment to identify and classify all the information assets, to evaluate the risks they are exposed to and to determine the required technical, managerial, organizational and procedural controls. certSIGN maintains an inventory of all information assets and assigns them a classification consistent with the risk assessment.

5.5 Records archival

It is required that all data and files related to registration of information associated with the system security, requests submitted by Subscribers, information about Subscribers, issued used metadata, and whole correspondence between certSIGN and the Subscribers should be subjected to archive.

The QPS archive contains active and expired metadata, including the deleted ones. QPS archive contains information about the Subscriber, the signed agreement, the moment when the service was activated and all the operations involved. The archive is used for dispute resolving regarding preserved documents electronically signed or sealed.

Backup copies are created and retained outside certSIGN location.

5.5.1 Types of data archived

The following data are subjected to a trustworthy archive, for at least 3 years after the termination of the contract that these records are based on:

- All metatada related to the QPS operations done during the contract execution
- The archived journals of logs
- Logs of all events relating to the life cycle of the preserved documents during the contract execution by certSIGN
- QPS services Subscriber agreement – this evidences will be kept according to the applicable laws
- Agreed terms and conditions regarding use of the QPS services

5.5.2 Preservation period for archive

See section 5.5.1 above. After expiration of the declared preservation period, archived data are destroyed.

5.5.3 Protection of archive

certSIGN ensures:

- Implementation of controls for archive data loss prevention
- Archive data confidentiality and integrity during its preservation period,

Archives are accessible only to the authorized personnel.

5.5.4 Archive backup procedures

Backup of archive data is made according to internal backup policies and procedures.

5.5.5 Requirements for time-stamping of records

certSIGN ensures that the precise time of archiving all events, records and documents mentioned above is recorded. This is accomplished through synchronization of all systems

with the time servers. The time accuracy is ensured by a time server that is synchronized with at least two-time sources that can be GPS satellites or UTC (NIMB).

5.5.6 Archive collection system (internal or external)

certSIGN archive collection systems are internal.

5.5.7 Procedures to obtain and verify archive information

Archives are accessible to the authorized employees of certSIGN and designated auditors. Records are retained in electronic or in paper-based format.

The Subscriber/Subject may get access to related registration records and other information relating to the Certificate Subject.

5.6 Compromise and Disaster Recovery

This chapter describes procedures carried out by certSIGN in abnormal situations (including natural disasters) to restore a guaranteed service level. Such procedures are executed in accordance with the Business Continuity and Disaster Recovery Plan of certSIGN.

5.6.1 Incident and compromise handling procedures

certSIGN has a process for crisis management implemented as a security incident management procedure in order to respond quickly and coordinated to incidents and to limit the impact of security breaches. Employees are assigned to trusted roles to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the procedure. Critical malfunctions are acted upon on the basis of the same procedure.

The security incident management procedure also specifies how to 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.

In case of security incident, internal procedures are used. The procedures include the notification of the Supervisory body, the National CSIRT or other competent authorities.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the Preservation Service has been provided, we will also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

All the security events logs are continuously analysed by automatic mechanisms in order to identify evidence of malicious activity and alert designated personnel of possible critical security events.

All incident and/or compromise events are documented, and any associated records are archived as described in section 5.5 of the PPPS.

certSIGN have an Incident Response Plan and a Disaster Recovery Plan, that include the Crisis Management Plan, and documented business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. certSIGN make its business continuity plan and security plans available to the CA's auditors upon request. The CA annually test, review, and update these procedures.

5.6.2 Recovery Procedures

Recovery procedures if computing resources, software and/or data are corrupted.

certSIGN's Security Policy, takes into consideration the following threats influencing availability and continuity of the provided services:

- Physical corruption to the computer system of certSIGN, including network resources corruption – this threat addresses corruptions originating from emergency situations,
- Software and application malfunction, rendering data inaccessible – such corruptions address operating system, users' applications and execution of malicious software, for example viruses, worms, Trojan horses,
- Loss of network services, important for certSIGN's activity. Its main site power failure and damages to the network connections,
- Corruption of part of the internal network infrastructure, used by certSIGN to provide services – the corruption may imply obstruction for the customers and denial (unintended) of services.

To prevent or limit results of the above threats:

- The Security Policy of certSIGN includes a Business Continuity and Disaster Recovery Plan,
- In the case of corruption restraining certSIGN functionality, within 48 hours an emergency facility will be activated, which should substitute all significant function of a TSP until the services of the primary facility are restored. The distance between the primary and the emergency facilities is large enough to avoid that the potential disasters occurring at the primary site could also affect the emergency site.
- Installation of updated software version in production is possible only after carrying out intensive tests on a testing environment, performed in strict accordance with disclosed procedures. Every modification in the system requires certSIGN security administrator's acceptance.
- certSIGN systems use applications for creating backup copies of data, allowing system recovery at any moment and audit to be performed. Backup copies include all the relevant data from security point of view.
- All the systems from the IT infrastructure used to provide trusted services are continuously monitored and all the security events are logged and analysed. Abnormal system activities that indicate a potential security violation, including intrusion into the systems and network are detected and reported as alarms to enable certSIGN to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.
- The sensitivity of any information collected or analysed is considered by protecting it from unauthorized access.
- In order to detect any discontinuity in the monitoring operations, the start-up and shutdown of the logging functions is also monitored
- The availability of all important components of the ICT infrastructure used for providing the trusted services as well the availability of critical services are also monitored.
- certSIGN addresses any critical vulnerability not previously addressed, within a period of 96 hours after its discovery. certSIGN prepares and implements a mitigation plan for the new vulnerabilities, if this is cost effective compared to their impact, or documents the decision that the vulnerability does not require remediation.

5.6.3 Business continuity capabilities after a disaster

certSIGN has established in a Business Continuity and Disaster Recovery Plan (BC&DRP) all the necessary measures to ensure full recovery of its trusted services in case of a disaster, or a disruption of any important ICT component or service longer that the established Maximum Tolerable Downtime. Any such measures are compliant with the ISO/IEC 27001 and 27002 standards. For each component or service operations will be restored within the Maximum Tolerable Downtime established in the continuity plan.

All data from the systems required to resume TSP operations are backed up and stored in a remote and safe place, suitable to allow services to timely go back to operations in case of incident/disasters.

Back-up copies of essential information and software are realized regularly. Adequate back-up facilities are provided to ensure that all essential information and software can be recovered following a disaster or media failure. Back-up arrangements are regularly tested to ensure that they meet the requirements of business continuity plans.

Backup and restore functions are performed by the relevant trusted roles.

Following a disaster, where practical, steps will be taken to avoid repetition of a disaster.

5.7 QPS termination

certSIGN has an up-to-date termination plan used to minimize disruptions to Subscribers and Relying Parties which might arise from a decision of a TSP to cease QPS operation. The plan includes obligations to notify in advance all Subscribers subjected to QPS termination and transition of responsibilities (services provided to the Subscribers, databases, etc.), in compliance with the regulations in force to another TSP.

Requirements associated to duty transition

Before a QPS ceases its activity, certSIGN TSP will:

- Inform (at least 30 days in advance) the following about the decision to terminate its services: all Subscribers who hold active (unexpired and not terminated) agreements signed with certSIGN TSP and other entities with which certSIGN has agreements or other form of established relations, among which relying parties, other trust service providers and relevant authorities such as supervisory bodies. In addition, this information will be made available to other relying parties;
- Transfer its obligations to a reliable party for maintaining all information necessary for the operation of the QPS services for a reasonable period.
- Where possible, make arrangements to transfer provision of QPS services for the existing customers to another trusted service provider.

certSIGN will maintain or transfer to a reliable party its obligations to make available its QPS services for a reasonable period.

In case certSIGN will terminate its activities without a partially or full transfer of its activities, will initiate the termination procedure for the contracts signed with the implied partners and/or supliers.

certSIGN has an arrangement to cover the costs to fulfil these minimum requirements in case it becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

QPS takeover by the successor of the terminated TSP

In order to ensure the continuity of QPS services for Subscribers, the terminating TSP may sign a contract with another TSP offering similar services to take over, under pre-determined conditions, the specific QPS data and activities.
By taking over the QPS, the successor to the TSP that ceases activity takes over the rights and obligations of this authority with regard to the management of the documents remaining in preservation.
After notification of termination of the QPS services by the certSIGN TSP, the Subscriber has the decision whether to accept the continuation of the services with the new TSP or to withdraw from the agreement with certSIGN.
The QPS file of the terminating TSP shall be handed over to the new TSP in case of termination of the certSIGN TSP.

5.8 Supply chain

certSIGN documented and implemented processes and procedures to manage the information security risks associated with the use of supplier's products or services. They are detailed in the internal certSIGN policy for the management of the third -party providers (" *Politica de Management al Serviciilor Furnizate de Terti*").

The process and the procedures implemented are managing the information security risks associated with the information and communication technologies products and services supply chain, as requested in ETSI EN 319 401 #7.14.

When certSIGN makes use of other parties, including trust service component providers, to provide parts of its service through subcontracting, outsourcing or other third party arrangements, it maintains overall responsibility for conformance with the supply chain policy, its information security policy and the requirements defined in the trust service policy.

certSIGN review the supply chain policy and monitor, review, evaluate and manage changes in the cybersecurity practices of direct suppliers or service providers at planned intervals or after an incident related to the provision of services from direct suppliers or service providers.

6 Technical security controls

certSIGN QPS uses reliable systems and equipment protected against modification for the management of the whole life-cycle of electronic documents.
The capacity demands are continuously monitored and the future capacity demands are estimated, so that the necessary availability of processing and storage needs is ensured.

6.1 Activation data

6.1.1 Activation data generation and installation

Activation data are used in two basic cases:

- As an element of one or multi-factor authentication procedure (so called authentication phrase, e.g. password, PIN number, etc.),

- As a part of the shared secret.

All operators and TSP administrators, as well as other persons performing the roles described in Chapter 5.2 use secure credentials (tokens/cards) to identify and authenticate themselves for their roles. Their private keys that are generated on qualified electronic signature devices or HSM smartcards by certSIGN are associated with user activation data (PIN code) being securely personalized and distributed. certSIGN ensures that operators' and administrators' activation data are securely managed and protected by such participants through applicable internal procedures made available to these participants.

Shared secrets used for TSP private key protection are generated in accordance with the requirements presented in Chapter 6.2 and retained inside cryptographic cards. The cards are protected by a PIN number. Shared secrets become activation data after their activation, i.e. providing the correct PIN number protecting the card. certSIGN ensures that activation data associated to TSP private keys and operations are securely generated, managed, stored and archived as described in the relevant sub-section of sections 6.1 and 6.2. The installation and recovery of the TSP's key pairs in a secure cryptographic device shall require simultaneous control of at least two employees in trusted roles.

When the keys are generated on the QSCD by certSIGN, the QSCD where the private key and the digital certificate are stored is either delivered in person to the Subscriber or is sent to him using postal or courier services. The secret activation data (i.e. PIN code) required to access the QSCD are sent using a tamper-evident envelope.

6.1.2 Activation data protection

Activation data protection includes activation data control methods preventing from their disclosure. Activation data protection control methods are selected depending on whether they are authentication phrases or whether control is enforced on the basis of private key or on its activation data distribution into shared secrets.

Activation data used for private key activation shall be protected by means of cryptographic controls and physical access controls. Activation data shall be memorized (not written down) by the entity being authenticated. If the activation data are written down, the level of their protection should be the same as data protected by the usage of a cryptographic card. Several unsuccessful attempts to access the cryptographic module should result in its blockage. Stored activation data shall never be retained together with the cryptographic card.

The Subscribers are responsible for the secure management and protection of their activation data (i.e. PIN code).

The secret activation data (i.e. PIN code) received from certSIGN shall be immediately changed by the Subscriber after receiving it.

6.1.3 Other aspects of activation data

Not applicable

6.2 Computer security controls

This chapter describes certSIGN's computer security controls.

The Subject is responsible for his/her own computer security controls. These aspects are not covered in the subchapters bellow.

6.2.1 Specific computer security technical requirements

Security mechanisms protecting computer systems are executed at the level of operating systems, applications and physical protections.

Computers are configured with the following security mechanisms:

- Mandatory authenticated registration at operating system and applications level,
- Discretionary access control,
- Possibility of conducting security audit,
- The computer is accessible only to authorized personnel, performing trusted roles in certSIGN,
- Enforcement of duty segregation, arising from the role performed in the system,
- Identification and authentication of roles and personnel performing these roles,
- Prevention of an object re-use by another process after the object was released by an authorized process,
- Cryptographic protection of information exchange and protection of databases,
- Archival of operation history on the computer and of data required by audits,
- A secure path allowing reliable identification and authentication of roles and of personnel performing these roles,
- Key restoration methods (only for hardware security modules),
- Monitoring and alerting in case of unauthorized access.

The integrity of certSIGN systems and information is protected against viruses, malicious and unauthorized software.

Media used within certSIGN systems are securely handled to protect media from damage, theft, unauthorized access and obsolescence.

Media management procedures are implemented to protect against obsolescence and deterioration of media for the period of time for which records must be kept.

Sensitive data shall be protected against disclosure through re-used stored objects (e.g. deleted files) being accessible to unauthorized users. For that purpose, special software shall be used with secure deletion algorithms for storage media, HSMs shall be zeroized, secure cryptographic devices (tokens/cards) shall be formatted before reuse/, or physically destroyed at the end of their life cycle.

For all accounts capable of directly causing certificate issuance multi-factor authentication is enforced.

6.2.2 Computer security rating

certSIGN computer system complies with requirements described in ETSI Standards and CEN CWA 14167 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures).

6.3 Life cycle security controls

certSIGN uses trustworthy systems and products that are protected against modification and ensures the technical security and reliability of the processes supported by them.

6.3.1 System development controls

An analysis of security requirements is carried out in design and requirements specification stage of system development projects undertaken by certSIGN or on behalf of certSIGN in order to ensure that security is built into IT systems.

Every application, prior to be used for production within certSIGN, is installed so as to allow control of the current version and to prevent unauthorized installation of programs or forgery of existing ones.

Similar rules apply to hardware components replacement, as follows:

- Hardware is supplied in a manner that allows traceability and monitoring of the route of components to the place of their installation,
- Spare hardware delivery is carried out in a manner similar to delivery of original hardware; the replacement is carried out by trusted and trained personnel.

6.3.2 Security management controls

The purpose of security management control is to supervise certSIGN systems' functionality providing assurance that the system operates correctly and in accordance with the accepted and implemented configurations.

Controls applied to certSIGN system allow continuous verification of application integrity, of their version as well as authentication and verification of hardware origin.

6.3.3 Life cycle security controls

Change control policies and procedures are applied for releases, modifications and emergency software fixes of any operational software and changes in configurations applying certSIGN's security policy.

Current configuration of certSIGN systems, any change or new release, modification and emergency software fixes of any operational software are documented.

Configurations of Services support Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are reviewed on at least a weekly basis to determine whether any changes violated the CA's security policies

certSIGN implements internal security procedures for ensuring that:

- Security patches are applied within a reasonable time after they come available;
- Security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them;

The reasons for not applying any security patches are documented.

certSIGN implements an internal capacity management procedure which ensures that the capacity of ICT infrastructure for trusted services is monitored and that estimates of capacity requirements are made to ensure that adequate processing power and storage are available.

6.4 Network security controls

certSIGN protects its network and systems from attack. For that purpose and based on risk assessments and best practices we implement an integrated set of security controls:

a) Systems are segmented into networks or zones based on the functional, logical, and physical (including location) relationship between trustworthy systems and services. certSIGN applies the same security controls to all systems co-located in the same zone.

b) Access and communications between zones are restricted to those necessary for the operation of trusted services. Unnecessary connections and services are explicitly forbidden or deactivated. The established set of rules is reviewed on a regular basis.
c) All systems that are critical to the trusted services operation are kept in one or more secured zone(s)
d) Dedicated network for administration of IT systems and operational network are separated. Systems used for the administration of security policy implementation are not used for other purposes. The production systems for the trusted services are separated from systems used in development and testing (e.g. development, test and staging systems).
e) Communication between distinct trustworthy systems are established only through trusted channels that are logically distinct from other communication channels and provide secured identification of its end points and protection of channel data from modification or disclosure.
f) If a high level of availability of external access to a specific trusted service is required, the external network connection is redundant in order to ensure availability of the services in case of a single failure.
g) Regular vulnerability scan on public and private IP addresses identified by certSIGN is performed and evidence is recorded 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.
h) certSIGN trusted services undergo a penetration test on the related systems upon set up and after infrastructure or application upgrades or modifications that certSIGN considers to be significant. Evidence is recorded 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.

Servers and trusted workstations of certSIGN system are connected by a local network (LAN), divided into sub-networks provided with controlled access. Access from the Internet to any segment is protected by means of intelligent firewall.

Security controls are developed based on firewall and traffic filtering on the routers and Proxy services that protect certSIGN'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 certSIGN CA.

Means of protection of the network security accept only messages submitted with the use of http, https, NTP, POP3 and SMTP protocols. Events (logs) are recorded in system journals and allow supervision of the use of services provided by certSIGN.

certSIGN maintains and protects all TSP systems in at least one secure zone and has in place a security procedure that protects systems and communications between systems inside secure zones and high security zones.

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

certSIGN grants access to secure zones and high security zones only to trusted roles.

The **QPS** support system is in a high security zone.

6.5 Time-stamping

The time accuracy of logs is ensured by a time server that is synchronized with at least two-time sources that can be GPS satellites or UTC (NIMB).

7 Profiles, Formats, and Preservation Schemas

A preservation scheme (specification) must meet the following general requirements:

1. It is documented in sufficient detail so that interoperability between independent implementations is possible.
2. It is identified by a URI in accordance with IETF RFC 3986.
3. Specifies the applicable storage model in the storage system.
4. Specifies the set of preservation objectives supported by the preservation scheme.
5. Specify the set of mandatory and optional operations supported.
6. Describes the process for generating and validating evidence of preservation – detailed in #3.6 Process for validating proofs of retention
7. For preservation WOS or WTS, the expected evidence duration is based on the estimation of the suitability of the RSA cryptographic algorithm according to ETSI TS 119 312 V1.4.3 #8 and #9 .
8. Describe how the maintenance of the preservation evidence takes place – described in #3.7 The process of re-auditing preservation evidence
9. Specify the required or recommended formats of input and output parameters and associated data transformations, if applicable, for the implementation of the preservation system.

7.1 Preservation scheme with signature completion and storage

- ProfileIdentifier:

Base profile:

o Qualified - pds+wst (OID: 1.3.6.1.4.1.25017.5.2.1)

The profile is identified by the base-profile with the preservation duration in years appended to it. (For Ex. 1.3.6.1.4.1.25017.5.2.1.40 = Qualified pds+wst for 40 years).

- Operation:

o Mandatory operation

- PreservePO
- RetrievePO
- DeletePO

o Optional operations

- RetrieveTrace

- Policy:

o Applied preservation evidence creation policy and a recommended preservation evidence validation policy can be advertised in the applicable profile/policy element with type equal to the following URI:
http://uri.etsi.org/19512/policy/preservation-evidence

- ProfileValidityPeriod:

o as contracted

- PreservationStorageModel:

o "WithStorage" preservation storage model, corresponding to the WithStorage value within the PreservationStorageModel element.

- PreservationGoal:

o the extension over long periods of time of the validity state of digital signatures, which is indicated by the URI: http://uri.etsi.org/19512/goal/pds
o complementing/augmenting the evidence presented, which is indicated by the URI: http://uri.etsi.org/19512/goal/aug

- EvidenceFormat:

o complete the signature corresponding to the signature format, which is announced in the Profile/EvidenceFormat element with the following URI:
http://uri.etsi.org/ades/PAdES/document-time-stamp

- Specification:

o https://www.certsign.ro/repository/

- Description:

o The PreservePO function of the current preservation system distinguishes only one type of use case, namely: signature and signed data are in the same object.
o The PreservePO service checks that all validation data required for signature validation are available, adds them to the signature and protects them with a timestamp corresponding to the specific signature format. The Preservation Service chooses a hash algorithm to protect the validation data, the signature and the signed data appropriate to the state of the art.
o Proofs are included in the signature.
o The signature format specific standard specifies how to validate the appropriate evidence.
o Based on the monitoring of cryptographic algorithm characteristics according to an appropriate cryptographic policy, e.g. ETSI TS 119 312, the preservation service performs a signature completion/enhancement according to the specific preservation proof format.

- **SchemeIdentifier:**
  o http://uri.etsi.org/19512/scheme/pds+wst+aug
- **ExpectedEvidenceDuration:**
  o Not applicable
- **PreservationEvidenceRetentionPeriod:**
  o N/A
- **Extension:**
  o N/A

7.2 Preservation scheme with signature completion and temporary storage

- **ProfileIdentifier**:
  Base profile:
  o Qualified - pds+wts (OID: 1.3.6.1.4.1.25017.5.2.2)
  The profile is identified by the base-profile with the preservation duration in years appended to it. (For Ex. 1.3.6.1.4.1.25017.5.2.2.40 = Qualified pds+wts for 40 years).
- **Operation**:
  o Mandatory operation
  - PreservePO
  - RetrievePO

  o Optional operations
  - RetrieveTrace
- **Policy**:
  o Applied preservation evidence creation policy and a recommended preservation evidence validation policy can be advertised in the applicable profile/policy element with type equal to the following URI: http://uri.etsi.org/19512/policy/preservation-evidence
- **ProfileValidityPeriod**:
  o as contracted
- **PreservationStorageModel**:
  o "WithTemporaryStorage" preservation storage model, corresponding to the WithTemporaryStorage value within the **PreservationStorageModel** element.
- **PreservationGoal**:
  o the extension over long periods of time of the validity state of digital signatures, which is indicated by the URI:http://uri.etsi.org/19512/goal/pds.
  o complementing/augmenting the evidence presented, which is indicated by the URI: http://uri.etsi.org/19512/goal/aug
- **EvidenceFormat**:

o complete the signature corresponding to the signature format, which is announced in the Profile/**EvidenceFormat** element with the following URI: http://uri.etsi.org/ades/PAdES/document-time-stamp

- **Specification:**
  - o https://www.certsign.ro/repository/
- **Description:**
  - o The PreservePO function of the current preservation system distinguishes only one type of use case, namely: signature and signed data are in the same object.
  - o The PreservePO service checks that all validation data required for signature validation are available, adds them to the signature and protects them with a timestamp corresponding to the specific signature format. The Preservation Service chooses a hash algorithm to protect the validation data, the signature and the signed data appropriate to the state of the art.
  - o Proofs are included in the signature.
  - o The signature format specific standard specifies how to validate the appropriate evidence.
  - o Based on the monitoring of cryptographic algorithm characteristics according to an appropriate cryptographic policy, e.g. ETSI TS 119 312, the preservation service performs a signature completion/update according to the specific preservation proof format.
- **SchemeIdentifier**:
  - o http://uri.etsi.org/19512/scheme/pds+wts+aug
- **ExpectedEvidenceDuration**:
  - o according to contract
- **PreservationEvidenceRetentionPeriod**:
  - o 96 hours
- **Extension:**
  - o N/A

7.3 Preservation scheme with signature completion and without storage

- **ProfileIdentifier**:

Base profile:

- o Qualified - pds+wos (OID: 1.3.6.1.4.1.25017.5.2.3)

The profile is identified by the base-profile with the preservation duration in years appended to it. (For Ex. 1.3.6.1.4.1.25017.5.2.3.40 = Qualified pds+wos for 40 years).

- **Operation**:
  - o Mandatory operation
    - PreservePO
  - o Optional operations
    - RetrieveTrace
- **Policy:**
  - o Applied Preserve Evidence Creation Policy and a recommended Preserve Evidence Validation Policy can be advertised in the applicable profile/policy element, with type equal to the following URI: http://uri.etsi.org/19512/policy/preservation-evidence
- **ProfileValidityPeriod**:
  - o as contracted
- **PreservationStorageModel**:
  - o the "without storage" preservation storage model, corresponding to the WithoutStorage value within the **PreservationStorageModel** element.
- **PreservationGoal**:

o the extension over long periods of time of the validity state of digital signatures, which is indicated by the URI:http://uri.etsi.org/19512/goal/pds
o complementing/augmenting the evidence presented, which is indicated by the URI: http://uri.etsi.org/19512/goal/aug

- **EvidenceFormat**:
  o complete the signature corresponding to the signature format, which is announced in the Profile/**EvidenceFormat** element with the following URI: http://uri.etsi.org/ades/PAdES/document-time-stamp
- **Specification:**
  o https://www.certsign.ro/repository/
- **Description:**
  o The PreservePO function of the current preservation system distinguishes only one type of use case, namely: signature and signed data are in the same object.
  o The PreservePO service checks that all validation data required for signature validation are available, adds them to the signature and protects them with a timestamp corresponding to the specific signature format. The Preservation Service chooses a hash algorithm to protect the validation data, the signature and the signed data appropriate to the state of the art.
  o Proofs are included in the signature.
  o The signature format specific standard specifies how to validate the appropriate evidence.
  o Based on the monitoring of cryptographic algorithm characteristics according to an appropriate cryptographic policy, e.g. ETSI TS 119 312, the preservation service performs a signature completion/update according to the specific preservation proof format.
- **SchemeIdentifier**:
  o http://uri.etsi.org/19512/scheme/pds+wos+aug
- **ExpectedEvidenceDuration**:
  o according to contract
- **PreservationEvidenceRetentionPeriod**:
  o N/A
- **Extension:**
  o N/A

7.4 General data preservation and storage scheme

- **ProfileIdentifier**:
  Base profile:
  o Qualified - pgd+wst (OID: 1.3.6.1.4.1.25017.5.2.4)

The profile is identified by the base-profile with the preservation duration in years appended to it. (For Ex. 1.3.6.1.4.1.25017.5.2.4.40 = Qualified pgd+wst for 40 years).

- **Operation**:
  o Mandatory operation
    - PreservePO
    - RetrievePO
    - DeletePO
  o Optional operations
    - RetrieveTrace
- **Policy:**
  o Applied preservation evidence creation policy and a recommended preservation evidence validation policy can be advertised in the applicable profile/policy element with type equal to the following URI: http://uri.etsi.org/19512/policy/preservation-evidence

- **ProfileValidityPeriod**:
  - o as contracted
- **PreservationStorageModel**:
  - o "WithStorage" preservation storage model, corresponding to the WithStorage value within the **PreservationStorageModel** element.
- **PreservationGoal**:
  - o evidence of the long-term existence of the data object presented to the preservation service, indicated by the URI: http://uri.etsi.org/19512/goal/pgd
  - o completion/update of the evidence submitted, which is indicated by the URI: http://uri.etsi.org/19512/goal/aug
- **EvidenceFormat**:
  - o complete the signature corresponding to the signature format, which is announced in the Profile/**EvidenceFormat** element with the following URI: http://uri.etsi.org/ades/PAdES/document-time-stamp
- **Specification:**
  - o https://www.certsign.ro/repository/
- **Description:**
  - o The current preservation scheme provides evidence of the long-term existence of the data object by signing the data object and then filling in the signature corresponding to the signature format
  - o The PreservePO function of the current preservation scheme distinguishes only one type of use case, namely: the signature and the signed data are in the same object.
  - o The PreservePO service checks that all validation data required for signature validation are available, adds them to the signature and protects them with a timestamp corresponding to the specific signature format. The Preservation Service chooses a hash algorithm to protect the validation data, the signature and the signed data appropriate to the state of the art.
  - o Proofs are included in the signature.
  - o The signature format specific standard specifies how to validate the appropriate evidence.
  - o Based on the monitoring of cryptographic algorithm characteristics according to an appropriate cryptographic policy, e.g. ETSI TS 119 312, the preservation service performs a signature completion/enhancement according to the specific preservation proof format.
- **SchemeIdentifier**:
  - o http://uri.etsi.org/19512/scheme/pgd+wst+aug
- **ExpectedEvidenceDuration**:
  - o Not applicable
- **PreservationEvidenceRetentionPeriod**:
  - o N/A
- **Extension:**
  - o N/A

7.5 General data preservation scheme and temporary storage

- **ProfileIdentifier**:

Base profile:

- o Qualified - pgd+wts (OID: 1.3.6.1.4.1.25017.5.2.5)

The profile is identified by the base-profile with the preservation duration in years appended to it. (For Ex. 1.3.6.1.4.1.25017.5.2.5.40 = Qualified pgd+wts for 40 years).

- **Operation**:
  - o Mandatory operations

- PreservePO
- RetrievePO

o Optional operations

- RetrieveTrace

- **Policy:**
  - o Applied preservation evidence creation policy and a recommended preservation evidence validation policy can be advertised in the applicable profile/policy element with type equal to the following URI: http://uri.etsi.org/19512/policy/preservation-evidence
- **ProfileValidityPeriod**:
  - o as contracted
- **PreservationStorageModel**:
  - o "WithTemporaryStorage" preservation storage model, corresponding to the WithTemporaryStorage value within the **PreservationStorageModel** element.
- **PreservationGoal**:
  - o evidence of the long-term existence of the data object presented to the preservation service, indicated by the URI URI: http://uri.etsi.org/19512/goal/pgd
  - o completion/augmentation of the submitted evidence, which is indicated by URI: http://uri.etsi.org/19512/goal/aug
- **EvidenceFormat**:
  - o complete the signature corresponding to the signature format, which is announced in the Profile/**EvidenceFormat** element with the following URI: http://uri.etsi.org/ades/PAdES/document-time-stamp
- **Specification:**
  - o https://www.certsign.ro/repository/
- **Description:**
  - o The current preservation scheme provides evidence of the long-term existence of the data object by signing the data object and then filling in the signature corresponding to the signature format
  - o The PreservePO function of the current preservation scheme distinguishes only one type of use case, namely: the signature and the signed data are in the same object.
  - o The PreservePO service checks that all validation data required for signature validation are available, adds them to the signature and protects them with a timestamp corresponding to the specific signature format. The Preservation Service chooses a hash algorithm to protect the validation data, the signature and the signed data appropriate to the state of the art.
  - o Proofs are included in the signature.
  - o The signature format specific standard specifies how to validate the appropriate evidence.
  - o Based on the monitoring of cryptographic algorithm characteristics according to an appropriate cryptographic policy, e.g. ETSI TS 119 312, the preservation service performs a signature completion/update according to the specific preservation proof format.
- **SchemeIdentifier**:
  - o http://uri.etsi.org/19512/scheme/pgd+wts+aug
- **ExpectedEvidenceDuration**:
  - o according to contract
- **PreservationEvidenceRetentionPeriod**:
  - o 96 hours
- **Extension:**
  - o N/A

7.6 General data preservation scheme and no storage

- **ProfileIdentifier**:
  Base profile:
    o Qualified - pgd+wos (OID: 1.3.6.1.4.1.25017.5.2.6)

The profile is identified by the base-profile with the preservation duration in years appended to it. (For Ex. 1.3.6.1.4.1.25017.5.2.6.40 = Qualified pgd+wos for 40 years).

- **Operation**:
    o Mandatory operation
        - PreservePO
    o Optional operations
        - RetrieveTrace
- **Policy:**
    o Applied Preserve Evidence Creation Policy and a recommended Preserve Evidence Validation Policy can be advertised in the applicable profile/policy element, with type equal to the following URI:
    http://uri.etsi.org/19512/policy/preservation-evidence
- **ProfileValidityPeriod**:
    o as contracted
- **PreservationStorageModel**:
    o the "without storage" preservation storage model, corresponding to the WithoutStorage value within the **PreservationStorageModel** element.
- **PreservationGoal**:
    o evidence of the long-term existence of the data object presented to the preservation service, indicated by the URI: http://uri.etsi.org/19512/goal/pgd
    an addition/augmentation of the submitted evidence, which is indicated by the URI: http://uri.etsi.org/19512/goal/aug
- **EvidenceFormat**:
    o complete the signature corresponding to the signature format, which is announced in the Profile/**EvidenceFormat** element with the following URI:
    http://uri.etsi.org/ades/PAdES/document-time-stamp
- **Specification:**
    o https://www.certsign.ro/repository/
- **Description:**
    o The current preservation scheme provides evidence of the long-term existence of the data object by signing the data object and then filling in the signature corresponding to the signature format
    o The PreservePO function of the current preservation scheme distinguishes only one type of use case, namely: the signature and the signed data are in the same object.
    o The PreservePO service checks that all validation data required for signature validation are available, adds them to the signature and protects them with a timestamp corresponding to the specific signature format. The Preservation Service chooses a hash algorithm to protect the validation data, the signature and the signed data appropriate to the state of the art.
    o Proofs are included in the signature.
    o The signature format specific standard specifies how to validate the appropriate evidence.
    o Based on the monitoring of cryptographic algorithm characteristics according to an appropriate cryptographic policy, e.g. ETSI TS 119 312, the preservation service performs a signature completion/update according to the specific preservation proof format.
- **SchemeIdentifier**:
    o http://uri.etsi.org/19512/scheme/pgd+wos+aug

- **ExpectedEvidenceDuration**:
  - according to contract
- **PreservationEvidenceRetentionPeriod**:
  - N/A
- **Extension:**
  - N/A

8 Compliance audit and other assessments

certSIGN is a trust service provider under the Regulation (EU) 910/2014.

In respect to the conformity audits and the competence, consistent operation and impartiality of conformity of assessment bodies that evaluate and certify our conformity as trust services provider and the conformity of our trusted services towards the criteria from Regulation 910/2014 and its implementing acts we follow the requirements from the ETSI EN 319 401 standard.

8.1 Frequency or circumstances of assessment

certSIGN activities supporting the delivery of the services presented by PPPS are audited at least every 24 months.

The audit verifies the compliance with the present PPPS, ETSI 319 401 and ETSI 119 511 technical standards.

On demand audits may be realized at certSIGN's sole discretion, on the request of the Supervisory body, as defined in the Regulation EU 910/2014, or to demonstrate compliance with specific industry, legal or business requirements.

8.2 Identity/qualifications of assessor

The assessment will be performed by a Conformity Assessment Body, as defined in the EU Regulation 910/2014.

8.3 Assessor's relationship to assessed entity

The Conformity Assessment Body is an independent auditor, not affiliated directly or indirectly with certSIGN.

8.4 Topics covered by assessment

The planned audits cover, but are not limited to, all aspects of certSIGN QPS operations and services specified in by PPPS.

8.5 Actions taken as a result of deficiency

The Conformity Assessment Body shall report the detected deficiencies and non-conformities to PPMP. certSIGN and the Conformity Assessment body analyse together the findings of the report and agree on a corrective plan and on a time frame to implement it.

A follow-up audit may be carried out, to verify the remediation actions.

8.6 Communication of results

The Conformity Assessment Body communicates the audit report to the Management of certSIGN and to PPMB.

9 Other business and legal matters

9.1 Fees

Trusted services fees and the types of services charged are published in the list of fees available at the address https://www.certsign.ro. Prices are set according to the internal price policy.

Payments will be made in cash, by payment order, or bank cards in compliance with the legal provisions in force.

9.2 Financial Responsibility

certSIGN takes financial responsibility to fulfil all its obligations defined in the present document and the service agreement concluded with the Client. In order to cover the costs associated with the termination of the service activity and to sustain reliability certSIGN meets the legal requirements for qualified trust service providers.

9.2.1 Insurance coverage

certSIGN benefits from insurance covering professional liabilities.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

All information related to the Subscriber / Partner Entities that certSIGN processes are obtained, stored and processed in accordance with the provisions of Regulation (EU) No. 910/2014. Relationships between a Subscriber, a Partner Entity, and certSIGN are based on trust.
Data delivered in applications sent to certSIGN will not be willingly disclosed to a third party under any circumstance (except for legal situations).
Disclosing any piece of information to the parties involved in fulfilling their obligations will be made in a confidential manner and will cover only information necessary to fulfil the obligations.
Types of Information Considered Confidential and Private

certSIGN, its employees and other entities that perform trusted activities are committed to keep the information secret both during and after employment. There are considered private and confidential information:

- Information provided by Subscribers in addition to information that shall be sent to perform the trusted services; in those situations, disclosing the information received requires the prior written consent of the information owner or in other conditions according to the law.
- Information supplied by/to Subscribers (for example, the content of contracts concluded with Subscribers or Relying Parties, bank accounts, applications – except for the information from the Repository, in compliance with the present PPPS); part of the information mentioned above can be disclosed only with the approval and for the purpose specified by the owner of the information (for example the Subscriber),
- Records of system transactions (all types of transactions, as well as data for transactions control, the so-called system transactions logs)
- Record of events (logs) related to preservati services, kept by certSIGN,
- Results of internal and external audits, if they are a threat for certSIGN's security,

- Emergency plans,
- Information about measures taken to protect hardware devices and software applications, information about management of the preservati services and planned registration rules.

Disclosure of Non-Public Information to Law Enforcement Officials

Confidential information can be disclosed to law enforcement officials only after fulfilling all formalities requested by the Romanian laws in force.

9.3.2 Information not within the scope of confidential information

certSIGN will be exonerated from the liability of disclosing confidential data if:
a) the information is known to certSIGN before it was received by the Subscriber;or
b) the information is disclosed after obtaining the written consent of the Subscriber;or
c) certSIGN is legally obliged to disclose the information.

9.3.3 Responsibility to protect confidential information

certSIGN, its employees and also the entities that perform trusted activities are committed to keep the information secret both during and after the agreement period.

9.4 Privacy of personal information

In providing trusted services, certSIGN processes the personal data of the Subscriber in accordance with the requirements of Regulation (EU) No. 910/2014 and in compliance with the internal provisions of Regulation No. 679/2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and other provisions of Union common law on data protection.

The purpose of processing personal data is to provide trusted services.

9.4.1 Privacy Plan

In the provision of preservationservices, certSIGN processes personal data in accordance with the Regulation no. 679/2016 and other legal provisions of the Union or internal law regarding data protection.

The security measures required by Regulation (EU) no. 910/2014 and Regulation no. 679/2016 are implemented by certSIGN to ensure that:

- Appropriate technical and organizational measures are taken to ensure the security of the processed data, to protect the rights of the natural persons and to respect the principles provided by Regulation no. 679/2016 and the provisions of Regulation (EU) no. 910/2014.
- Access to certSIGN services concerns only the processing of those identification data which are adequate, relevant and not excessive to grant access to the respective service.
- Confidentiality protection and registration data integrity: when exchanged with the subscriber, when exchanged between certSIGN system components as well as when stored.

9.4.2 Information Treated as Private

All Information that leads, directly or indirectly, to identification the natural person is personal information.

9.4.3 Information not Deemed Private

The information accessible through the Depositary is public information.

9.4.4 Responsibility to Protect Private Information

certSIGN undertake to maintain the confidentiality of personal information during execution of trusted services and after their termination.

certSIGN will not disclose personal information to any third party, for any reason, unless it is required to do so by law or by the competent authorities.

9.4.5 Notice to use Private Information

In the QPS process Subscribers are informed about the need to use their person al data for the service.

Personal data can also be used for other purposes expressly communicated by certSIGN by contract or otherwise.

The Subscriber is responsible for the nature of the personal data contained in the preserved documents and for their processing in compliance with the legislation applicable to the protection of personal data.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

certSIGN is relieved of liability for the disclosure of personal data in the following situations:

- disclosure of personal information to the Surveillance Body in accordance with the applicable law;

- to the competent institutions and bodies, based on the public law obligations certSIGN has, in accordance with the legal provisions.

9.4.7 Other Information Disclosure Circumstances

Constitute exceptions to the obligation to keep the confidentiality of personal data that exonerate certSIGN of liability, the following situations:

- disclosure of personal information of the Subscribers to:

- auditors in the audits to which certSIGN is subject according to the provisions of Regulation (EU) no. 910/2014 under confidentiality;
- a third party who relies on the trusted services provided by certSIGN in relation to which the Subscriber uses these services
- an empowered person to whom certSIGN outsourced certain services;
- certSIGN affiliated companies

- in any other circumstances with prior notice to the Subscriber.

9.5 Intellectual Property Rights

All trademarks, denominations, patents, brand marks, licenses, applications, software, graphic images etc. used by certSIGN are and will be the intellectual property of their legal owners. certSIGN commits itself to mention this thing according to requests imposed by owners.

All trademarks, denominations, patents, brand marks, licenses, applications, software, graphic images etc., belonging to certSIGN are and remain its property, no matter if they are along with patents, utility models, copyright or not and cannot be reproduced or delivered to a third party without the prior written consent of certSIGN.

9.6 Representations and warranties

9.6.1 certSIGN representations and warranties

certSIGN guarantees that all the requirements set out in the PPPS are complied with. It also undertakes the responsibility to ensure such compliance and provide these services in accordance with the PPPS.

The sole guarantee provided by certSIGN is that its procedures are implemented in accordance with the PPPS and the applicable verification procedures.

9.6.2 Subscriber representations and warranties

The Subscriber accepts the Terms and Conditions relevant to the service provided by certSIGN.

The Subscriber agrees to the PPPS and to his/her relevant responsibilities, liabilities and obligations as provided in the relevant sections of the PPPS.

9.6.3 Relying Party representations and warranties

The Relying Parties decide based on their policies about the way of accepting and using the QPS preserved documents, signatures and/or Time Stamps. During the verification of the validity for keeping the security level guaranteed by the QPS Provider it is necessary for the Relying Party to act with caution, so it is particularly recommended to:

- comply with the requirements, regulations defined in the PPPS;
- use reliable IT environment and applications;
- take into consideration every restriction in relation to the usage which is included in the PPPS.

9.6.4 Representations and warranties of other participants

Not applicable.

9.7 Disclaimers of warranties

Unless otherwise expressly provided in the PPPS and in the applicable legislation, certSIGN disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except for when it came from an authorized source), and further disclaims any and all liability for negligence and lack of reasonable care on the part of Subscribers and Relying Parties.

9.8 Limitations of liability

Within the limit set by the Romania Law, in no event (except for fraud or wilful misconduct) certSIGN will be liable to Subscriber, Relying Party or third party for:

- Any loss of profits, income or business;
- Any loss of data;

- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of QPS services;
- Any other damages.

In any case, certSIGN's liability will be limited to the value of the preservation services for each preservation request and will not exceed the value of the services for the last 6 months prior to the occurrence of the damage in case of a claim for compensation, regardless of the number of preserved documents or preservation requests.

9.9 Indemnities

certSIGN takes no financial responsibility for improperly used of QPS preserved data. certSIGN responds and compensates only within the limits shown above in art. 9.8.

9.10 Term and termination

9.10.1 Term

This PPPS and any amendments hereto shall become effective after publication in the Repository and in accordance with section 9.12.2 and shall remain in effect perpetually until terminated in accordance with this Section 9.10.

9.10.2 Termination

The PPPS remains in force until replaced by a new version.

9.10.3 Effect of termination and survival

The conditions and effect resulting from termination of this PPPS will be communicated via the certSIGN web site upon termination. That communication will outline the provisions that may survive termination of this PPPS and remain in force. The responsibilities for protecting confidential information and private personal information shall survive termination, and the terms and conditions for all existing services shall remain valid for the remainder of the validity periods of such services.

9.11 Individual notices and communications with participants

All notices and other communications which may or are required to be given or sent pursuant to the PPPS shall be in writing and shall be sent, except provided explicitly in the PPPS, either by

(i) registered mail, return receipt requested, postage prepaid,
(ii) an internationally recognized "overnight" or express courier service,
(iii) hand delivery
(iv) facsimile transmission, deemed received upon actual delivery or completed facsimile, or
(v) in electronic format, signed with a qualified electronic signature and be addressed to certSIGN using the contact details provided in chapter 1.5.1 from the present document.

9.12 Amendments

9.12.1 Procedure for amendment

certSIGN is responsible, through its Policies and Procedures Management Body (PPMB) for the approval and change of the present PPPS. The PPPS is reviewed at least once a year.

The only changes that the PPMB may make to these PPPS specifications without notification are minor changes that do not affect the assurance level of this PPPS, e.g., editorial or typographical corrections, or changes to the contact details.

Errors, updates, or suggested changes to this document shall be communicated as identified in the present PPPS, section 1.5.4. Such communication will include a description of the change, a change justification, and contact information of the person requesting the change.

The PPMB shall accept, modify or reject the proposed change after completion of a review phase.

Any changes to the PPPS are approved by the PPMB and are announced to certSIGN's customers. Subjects/Subscribers shall comply only with the currently applicable PPPS.

9.12.2 Notification mechanism and period

All changes to the present PPPS under consideration by the PPMB shall be disseminated to interested parties for a period of minimum 2 days. The date of issuance and the effective date are indicated on the title page of the present PPPS.

9.13 Dispute resolution procedures

All disputes associated with the present PPPS will be settled according to the Romanian laws by Romanian courts in Romanian language.

9.14 Governing law

The Romanian laws shall govern the enforceability, construction, interpretation, and validity of the present PPPS (the exclusion of any conflict without giving effect to any conflict of law provision that would cause the application of other laws).

9.15 Compliance with applicable law

The present PPPS and provision of certSIGN services are compliant with relevant and applicable Romanian laws and Regulation EU 910/2014.

9.16 Miscellaneous provisions

certSIGN provides unlimited access to services for people with disabilities in accordance with current legislation and standards.