Certification Practice Statement
certSIGN Public 2023 RSA CA

Version 2.0

Date: 17 April, 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	Reason	Responsible
1.0	15 December 2023	First version publishing	PKI Policies Manager
1.1	31 January 2024	Annual Review	PKI Policies Manager
1.2	31 March 2024	Add 3k and 4k key sizes	PKI Policies Manager
1.3	15 August 2024	Extend Linter max chars	PKI Policies Manager
1.4	11 November 2024	Remove 2024 bits keys	PKI Policies Manager
1.5	15 January 2025	Annual Review	PKI Policies Manager
1.6	20 February 2025	Miscelaneous updates	PKI Policies Manager
1.7	30 May 2025	Add Test certificates	PKI Policies Manager
1.8	25 July 2025	Add usage with NIF	PKI Policies Manager
1.9	15 January 2026	Annual Review	PKI Policies Manager
2.0	17 April 2026	Update for Management of RSS	PKI Policies Manager

This document was created and is the property of:

Owner	Author	Date created
BU Trust Services	PKI Policies Manager	December 20016

Distribution List

Destination	Date distributed
Public-Internet	December 2023
Public-Internet	January 2024
Public-Internet	March 2024
Public-Internet	August 2024
Public-Internet	November 2024
Public-Internet	January 2025
Public-Internet	February 2025
Public-Internet	May 2025
Public-Internet	July 2025
Public-Internet	January 2026
Public-Internet	April 2026

This document was approved by:

Version	Name	Date
1.0	Policies and Procedures Management Body	December 2023
1.1	Policies and Procedures Management Body	January 2024
1.2	Policies and Procedures Management Body	March 2024
1.3	Policies and Procedures Management Body	August 2024
1.4	Policies and Procedures Management Body	November 2024
1.5	Policies and Procedures Management Body	January 2025
1.6	Policies and Procedures Management Body	February 2025
1.7	Policies and Procedures Management Body	May 2025
1.8	Policies and Procedures Management Body	July 2025
1.9	Policies and Procedures Management Body	January 2026
2.0	Policies and Procedures Management Body	April 2026

Content

1 Introduction

The **Certification Practice Statement for certSIGN Public 2023 RSA CA** (hereinafter referred to as CPS Public 2023 RSA CA or CPS) details the certification policies, procedures, and security controls implemented by certSIGN, as a Qualified Trust Service Provider (QTSP), for the issuance of digital certificates by the Public 2023 RSA CA subordinate certification authority. This document also specifies the policy and security controls, applied by certSIGN, as a Qualified Trust Service Provider, when operating remote Qualified Signature Creation Devices (QSCDs) within the certSIGN Server Signing Application Service (SSAS), for the creation, maintenance, life-cycle management and use of signing keys to create digital signatures.

The structure and content of the CPS Public 2023 RSA CA are compliant to RFC 3647, ETSI EN 319 401, ETSI EN 319 411-1, and ETSI TS 119 431-1.

certSIGN complies with Regulation (EU) 1183/2024 (eIDAS2) and with Romanian Law no.214/2024 on the issuance of electronic signatures/seals, time-stamping,the provision of trust services based on them, and on the qualified service for the management of remote qualified electronic signature/seal creation devices.

1.1 Overview

certSIGN, Subscribers, Subjects and associated Relying Parties must adhere to the **CPS** for the issuance of non-qualified certificate for authentication and signing, non-qualified certificate for encryption, and for non-qualified certificates for electronic seals. Also, this document describes the general rules for providing certification services such as: Subject's registration, public key certification, certificates rekey and certificate revocation. Also it describes the rules for the certSIGN qualified service for the management of remote qualified electronic signature/seal creation devices.

certSIGN ensures that remote signature creation data remain under the sole control of the signatory, supported by strong authentication and secure cryptographic controls as required by ETSI TS 119 431-1.

1.2 Document name and identification

The title of this document is **Certification Practice Statement certSIGN Public 2023 RSA CA**, hereinafter referred to as **CPS Public 2023 RSA CA** or **CPS**.

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

1.3 PKI participants

The CPS Public 2023 RSA CA regulates the most important relations between entities belonging to certSIGN, the advisory teams (including auditors) and its customers (users of the services provided):

- certSIGN Public 2023 RSA CA
- Registration Authority,
- Repository,
- Online certificate status protocol (OCSP Authority),
- Subjects,
- Subscribers,

- Relying Parties,
- Relevant suppliers for certSIGN regarding issuance and management of digital certificates and devices.
- Policies and Procedures Management Body
- Auditors

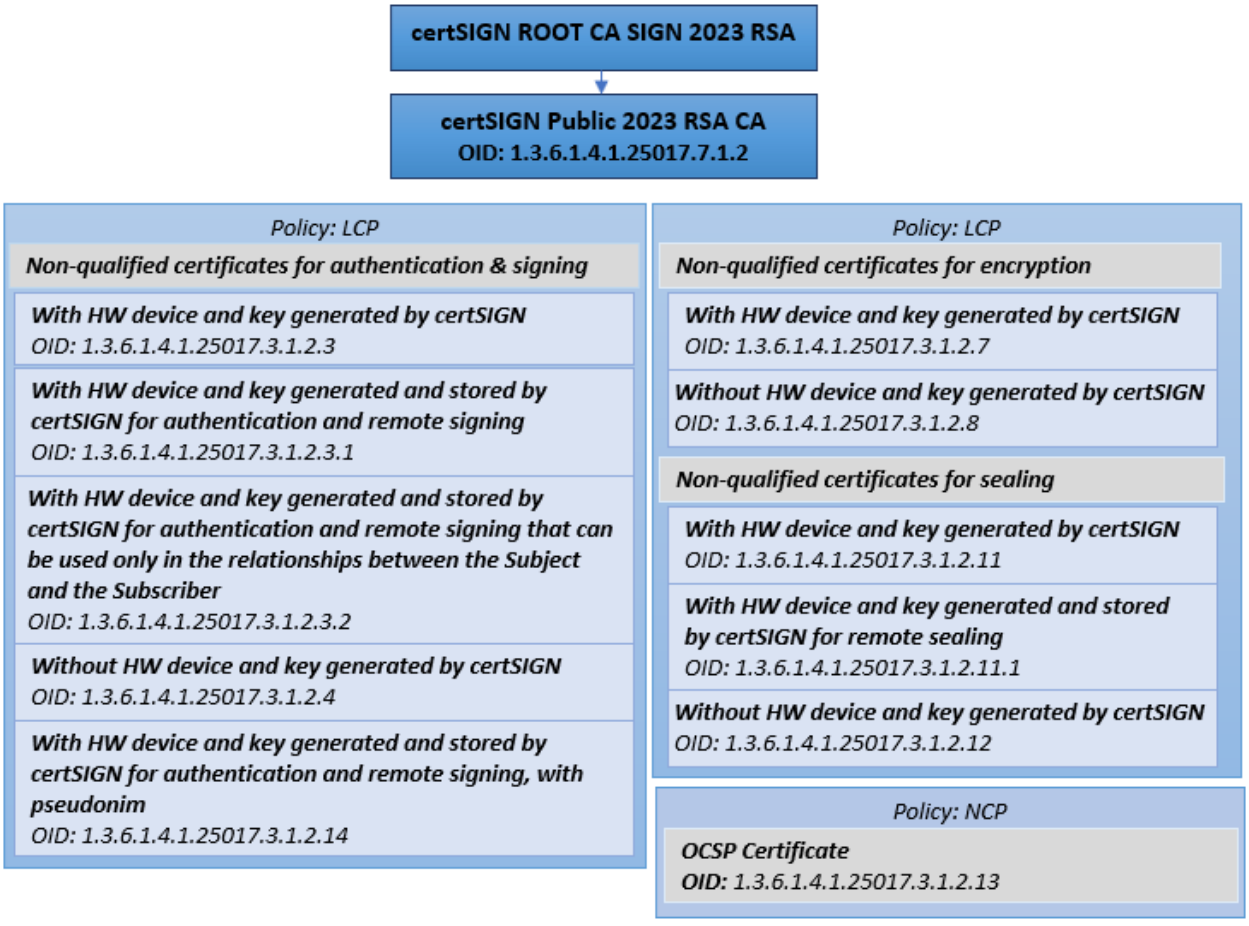
certSIGN provides certification services for every natural or legal entity accepting the regulations of the present CPS. The purpose of the CPS herein (that include key generation procedures, certificate issuing procedure and information system security) is to ensure the users of certSIGN services that the declared levels of credibility related to the issued certificates comply with the Certification Authorities' practices.

This CPS applies also to:

- All organizational units, personnel, and systems involved in delivering the remote (Q)SCD service.
- The lifecycle of remote (Q)SCD keys, from generation through use and deactivation.
- The interfaces, physical and logical security measures, and operational controls.

1.3.1 Certification authorities

certSIGN Public 2023 RSA CA is a Subordinate Certification Authority for the certSIGN domain. It is subordinated to the certSIGN ROOT CA G2. certSIGN Public 2023 RSA CA is identified by the following OID: 1.3.6.1.4.1.25017.7.1.2.



Before the activity started, **certSIGN Public 2023 RSA CA** sent a request to the Primary Certification Authority, **certSIGN ROOT CA G2** for registration and public key certificate issuance.

1.3.2 Registration authorities

The Registration Authority receives, verifies and approves or rejects the registration and certificate issuance, certificate rekey and revocation requests. Verification of applications intends to authenticate (based on the documents enclosed in the applications) both the Subscriber/Subject and the data specified in the request. The Registration Authority may also submit applications to the corresponding Certification Authority in order to cancel a request or revoke a certificate.

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 clauses 6.4.4, 6.5.6, 6.5.7 and 6.8.4 of ETSI 319 411-1.

1.3.3 Subscribers

Subscriber

Subscribers are legal entities or natural persons who submit a request to certSIGN for the issuance of a certificate, further used when signing the Subscriber Agreement.

The Subscribers may be:

- Natural persons - in this case, the Subscriber is the Subject of the certificate issued by certSIGN,
- Legal entities who enter into a contractual agreement with certSIGN for issuing certificates to Subjects (e.g., self-employed, employee),
- Legal entities who enter into a contractual agreement with certSIGN for issuing certificates for electronic seal.

Subscribers may request the certificate issuance, revocation or rekey on behalf of the Subject they are responsible for. A Subscriber undertakes to immediately notify certSIGN upon (suspicion of) private key compromise;

Subject

The subject is the entity to which a certificate is issued and is identified in a certificate as the holder of the private key associated with the public key from the certificate.

The subject can be:

- The Subscriber, if he requests the certificate for himself,
- A natural person for whom the Subscriber requests the certificate, the latter having a legally binding agreement or acting as his/her employer
- A legal entity for whom the Subscriber requests the certificate for electronic seal.

A Subject undertakes to:

- Immediately notify certSIGN upon (suspicion of) private key compromise;
- Submit requests for renewal of keys and/or certificates to certSIGN in due time;
- Protect the confidentiality of their private key is protected as per this document;

- Ensure that access to use of their private key is controlled according to this document.

1.3.4 Relying parties

A Relying Party can be any entity that uses certSIGN services and takes decisions based on the correctness of the connection between a Subject's identity and the public key.

A Relying Party is responsible for the way in which the current status of a Subject's certificate is verified. Such a decision shall be taken every time a Relying Party is willing to use a certificate to verify an electronic signature, to verify the identity of the source or the author of a message or to create a secure communication channel with the Subject of the certificate. A Relying Party shall use the information in a certificate (for example, identifiers and qualifiers of certification policy) to decide whether a certificate 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 Certification Authorities and Registration Authorities. The roles and responsibilities of PPMB are described in certSIGN internal documentation.

Services providers are external providers supporting certSIGN activities under a signed contractual agreement (i.e. courier companies).

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

1.4 Certificate usage

The certificate scope sets the purpose for which a certificate may be used. This scope is defined by two elements:

- One that defines the certificate applicability (for example: electronic signature, confidentiality),
- 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 certificate to be used for a certain purpose. The Relying Party shall decide, by taking into consideration the significant risk factor, what type of certificate issued by certSIGN meets the formulated requests. Subjects shall know the requests of the Relying Parties (for example, these requests might be published as a signature policy or as an information security policy) and then to request certSIGN to issue certificates corresponding to these requests.

1.4.1 Appropriate certificate uses

Certificates may be used in applications that satisfy at least the following conditions:

- Properly manage the public and private keys,
- Certificates and associated public keys are used in compliance with their declared purpose, confirmed by certSIGN,
- Have built-in mechanisms of certificate status verification, certification path creation and validation control (signature availability, expiration date etc.),

- Provides relevant information regarding certificates and their status for users.

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

It is the responsibility of the Subject to use the certificates according to this CPS. It is the Subject's or the Subscriber's responsibility to use software applications that correctly interprets, displays and uses the information and restrictions encoded in the certificates, such as but not limited to key usage, limited liability per transaction, etc.

A specific set of certificates, detailed in the Annex, are used by the certSIGN Server Signing Application Service (SSAS).
It is the responsibility of the Subscriber, the Subject and the Relying Party to decide for which purpose the certificates are considered trustworthy. A Relying Party must always take into account the level of assurance and other information in the CPS before deciding on the applicability of the certificate.

The certificates with pseudonym provide the lowest level of security in relation to individual identity, and it is recommended to be used only to provide the integrity of the data of documents signed with such certificates, under conditions considered low risk and where authentication of transactions is not necessary.
The use of the digital certificate in relation with ANAF by non-resident foreign citizens
For the use of the digital certificate in relation with the Romanian National Agency for Tax Administration (ANAF) by non-resident foreign citizens holding a tax identification number assigned by the tax authority (NIF), certSIGN confirms by the Confirmation Document the link between the digital certificate held and the NIF provided by the Subject for this purpose. certSIGN does not verify the authenticity of the NIF document submitted by the Subject, the responsibility for the correctness and veracity of the NIF document belongs to the Subject.

1.4.2 Prohibited certificate uses
Any usage of a certificate other than the usage explicitly allowed in the CPS, is prohibited.

1.5 Policy administration

1.5.1 Organization administering the document
The present document is administered by the Trust Service Provider certSIGN (TSP) through the Policies and Procedures Management Body (PPMB). The PPMB includes senior members of the management as well as the 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 Tax Register Number: J2006000484402 Tax registration code: RO 18288250 Registered office: 107A Oltenitei Street. building C1, ground floor, 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

Procedure for certificate problem reporting

Due to some errors, technical or procedural limitations or form other reasons, certificates may be misissued by certSIGN (e.g the issued certificate contains wrong information about the subject or the organization). Also, there may be cases when a certificate is used inappropriately (e.g. for criminal activities). If subscribers, relying parties or other third parties come across such situations, if they suspect private key compromise, or other kind of fraudulent activities, misuse of a certificate or inappropriate conduct or any other similar matters related to certificates issued by certSIGN, they can report those problems at the address revokecsgn@certsign.ro, informing the issuing CA of reasonable cause to revoke the certificate. certSIGN CA will begin investigation of a Certificate Problem Report within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

1. The nature of the alleged problem;
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
4. Relevant legislation.

certSIGN CA maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint. Certificate problem reports have to be submitted to the address revokecsgn@certsign.ro

1.5.3 Person determining CPS suitability for the policy

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

Table: 1.5.3 Person determining CPS suitability for the policy

1.5.4 CPS Approval Procedures

Policies and Procedures Management Body is responsible for the approval of the CPS.
The approval procedure is described in an internal instruction document.

Subjects/Subscribers shall comply only with the CPS in force, published at https://www.certsign.ro/en/repository/.

Subjects/ Subscribers who do not accept the new, modified terms and regulations of CPS are bound to make a suitable statement within 15 days of the date of the new CPS \version publication. This will lead to termination of the contract related to certification services provided and to the revocation of the issued certificate on its ground.

1.6 Definitions and acronyms

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 user'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 certificate issuer

Certification Authority Revocation List (CARL) – a revocation list with CA-certificates issued to certification authorities that are no longer considered valid by the certificate issuer

Certification Practice Statement (CPS) – a statement of practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates

Cross- certification – a certificate that is used in order to establish a reliable relationship between two certification authorities

Electronic signature – data in electronic form that are attached to or logically associated with other data in electronic form and which is used by the signatory to sign

Object identifier (OID) – alphanumeric / numeric identifier registered in accordance with the ISO/IEC 9834 standard and uniquely describing a specified object or its class.

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 the 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 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 (RA) - 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)

Short-term certificate - certificate whose validity period, i.e. the period of time from notBefore through notAfter, inclusive, is shorter than the maximum time to process a revocation request as specified in the certificate practice statement.

Subject (End Entity): 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
Test certificates – certificates that are issued only for the purpose of testing.
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;

CA Certification Authority
CPS Certification Practice Statement
CRL Certificate Revocation List
CARL Certification Authority Revocation List
DN Distinguished Name
HW Hardware
OCSP On-line Certificate Status Protocol
PKI Public Key Infrastructure
PPMB Policies and Procedures Management Body
QSCD Qualified Electronic Signature Creation Device
RA Registration Authority
RSA Rivest, Shamir, Adleman asymmetric cryptographic algorithm
S/MIME Secure MIME (Multipurpose Internet Mail Extensions)
TSP Trust Services Provider
UTC Coordinated Universal Time
DTBS/R Data To Be Signed Representation
SAD Signature Activation Data
SAM Signature Activation Module
SAP Signature Activation Protocol
SCA Signature Creation Application
SCAL Sole Control Assurance Level
SCDev Signature Creation Device
SIC Signer's Interaction Component
SSA Server Signing Application
TW4S Trustworthy System Supporting Server Signing

2 Publication and Repository Responsibilities

certSIGN publishes the CPS at least annually, even if there are no changes.

2.1 Repositories

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

- The Certificate Practice Statement for the CAs operated by certSIGN
- The Root CA and Subordinate CA certificates
- The certificates of the subjects
- The Certificate Revocation Lists
- Terms and conditions for the use of digital certificates

The Repository is managed and controlled by certSIGN., certSIGN undertakes to:

- Make all necessary efforts to ensure that all certificates published in the Repository belong to the Subjects' registered in certificates, and that all the Subjects have given their consent regarding these certificates,
- Ensure that the certificates of Certification Authorities, Registration Authority belonging to certSIGN domain as well as the Subject's certificates are published and archived on time,
- Ensure the publishing and archiving of the CPS, the recommended applications' lists and recommended devices,
- Provide access to information about the certificate status by publishing Certificate Revocation Lists (CRL), by means of OCSP servers or questions to HTTP,
- Provide constant access to information in the Repository for Certification Authorities, Registration Authority, Subjects and Relying Parties,
- Publish CRLs or other information in due time and in compliance with deadlines mentioned in the CPS,
- Ensure secure and controlled access to information in the Repository.

2.2 Publication of certification information

Upon issuing a digital certificate, the complete and accurate certificate is communicated by certSIGN to the subject for whom the certificate is being issued.

Certificates shall be available for publication only in those cases for which the subject's consent has been obtained, as described in the Terms and Conditions document.

For all issued certificates, the certificate status information is available through CRLs and the certificate validation services provided by certSIGN.

Availability

Availability of the document repository and the combined CRL 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 SA shall make best endeavours to reinstate availability of the service within 24 hours.

Expired certificates that were revoked before their expiration dates are not removed from the certificate revocation lists.

2.3 Time or frequency of publication

The information published by certSIGN is updated with the following frequency:

- CPS – see Chapter 1.5,
- Certificate of the Certification Authorities – after issuing a new certificate;
- Subjects' certificates – when the consent has been obtained, after every issue of a new certificate;
- Certificate Revocation List – is created either every 24 hours or when a certificate is revoked;
- 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 http://www.certsign.ro/repository is available for the public.

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

Subscribers, Subjects 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 the breach of information integrity in the Repository, CERTSIGN shall 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 Identification and authentication

3.1 Naming

3.1.1 Types of names

Certificates issued by certSIGN are in compliance with the X.509 v3 standard. This means that the TSP and the Registration Authority that acts on behalf of the issuer approve the Subject's name in compliance with the X.509 standard (with reference to X.500 series' recommendations). The names of the subjects and of certificate issuers in certSIGN certificates are in accordance with the structure of Distinctive Name (DN) - (also known as Directory Name structures), created according to the X.500 and X.520 recommendations.

To ensure an easy electronic communication with the Subject in certSIGN certificates, an additional name is used for the Subject. This name may also contain the Subject's e-mail address in compliance with the RFC 822 recommendations.

3.1.2 Need for names to be meaningful

The name included in Subject's Distinctive Name has a logical meaning in Romanian as well as in any other language using the Latin alphabet. The structure of the Distinctive Name approved / designated and checked by a Registration Authority depends on the Subject's type.

The DN has mandatory and optional fields in compliance with the RFC 5280 and X.520 recommendations.

The mandatory DN fields for natural persons, except for the certificates with OID 1.3.6.1.4.1.25017.3.1.2.14, are the following:

- C – international abbreviation for country name (RO – for Romania) – max length 2 characters
- SN – Surname[1] of the Subject – max length 128 characters
- G - First name of the Subject – max length 128 characters
- CN – Subject's name[2] – max length 128 characters
- Serial Number – unique serial number assigned to the Subject by the CA. The Serial number semantics is: First letter of surname + first letter of first name + index number – max length 64 characters

Mandatory DN fields for the certificates with OID 1.3.6.1.4.1.25017.3.1.2.14 are the following:

- C – international abbreviation for country name (RO – for Romania) – max length 2 characters
- P – Subject's Pseudonym – max length 128 characters
- CN – Subject's Pseudonym – max length 128 characters

[1] *For subjects whose country (C) is France (FR), if the name has been changed by marriage and both the original name and the name after marriage appear on the identity document, the surname on the certificate must be the name after marriage.*

[2] *For subjects where The Country (C) is France (FR) CN consists of the first given name (G) followed by the full family name (SN); for the others (C different from FR) CN consists of the full given name (G) followed by the full family name (SN).*

- Serial Number – unique serial number assigned to the Subject by the CA. The Serial number semantics is: First letter of each pseudonym world + index number – max length 64 characters

Optional DN fields for natural persons are the following:

- S – Residence County /district of the Subject – max length 128 characters
- L – residence city of the Subject – max length 128 characters
- Street – address of the Subject – max length 128 characters
- Phone – telephone number of the Subject – max length 32 characters.

Mandatory DN fields for natural persons affiliated to an organisation are the following:

- C – international abbreviation for country name (RO – for Romania) – max length 2 characters,
- O – official name of the Subscriber's organization, when the Subscriber is the employer of the Subject or there is a binding contract between them – max length 64 characters
- Organization Identifier – unique official identifier of the Subscriber as a legal entity – max length 64 characters
- SN – Surname[3] of the Subject – max length 128 characters,
- G – First name of the Subject – max length 128 characters,
- CN – Subject's name (first name, surname)[4] – max length 128 characters,
- SerialNumber – unique serial number assigned to the Subject by the CA. The semantics of the SerialNumber is: first letter of the surname + first letter of the first name + index number – max length 64 characters

Optional DN fields for natural persons affiliated to an organisation are:

- OU – department in the organisation – max length 64 characters,
- S – county/ district where the Subscriber is registered – max length 128 characters,
- L – city where the Subscriber is registered – max length 128 characters,
- Street – address of the Subscriber – max length 128 characters,
- T – job title – max length 64 characters,
- Field Phone – telephone number – max length 32 characters

Mandatory DN fields for legal entities are:

- C – international abbreviation for country name (RO for Romania) – max length 2 characters,
- O – official name of organisation – max length 64 characters,
- Organization Identifier – a unique official identifier of the Subscriber as a legal entity – max length 64 characters,

---

[3] *For subjects whose country (C) is France (FR), if the name has been changed by marriage and both the original name and the name after marriage appear on the identity document, the surname on the certificate must be the name after marriage.*

[4] *For subjects where The Country (C) is France (FR) CN consists of the first given name (G) followed by the full family name (SN); for the others (C different from FR) CN consists of the full given name (G) followed by the full family name (SN).*

- CN – specifies a formal or informal identification of the organisation – max length 128 characters

Optional DN fields for legal entities are:

- OU – department in the organisation – max length 64 characters,
- S – county/ sector where the organisation is registered – max length 128 characters,
- L – city of registration – max length 128 characters
- Phone – telephone number – max length 32 characters

The name of the Subject will be confirmed by an operator of the Registration Authority and will be approved by the Certification Authority. certSIGN ensures (within its field) DN uniqueness.

3.1.3 Anonymity or pseudonymity of subscribers

The use of pseudonyms is accepted exclusively for the certificates with OID 1.3.6.1.4.1.25017.3.1.2.14.

3.1.4 Rules for interpreting various name forms

The interpretation of the fields within the certificates issued by certTSIGN is done in accordance with the certificate profiles described in Certificates and CRL-s Profiles (Chapter 7). The special characters in the name are taken from the identity document: either from the MRZ or from the name fields, according to the standards specified in certSIGN's internal procedures. The creation and interpretation of the DN shall be performed according to the recommendations from Chapter 3.1.2.

3.1.5 Uniqueness of names

Name uniqueness is ensured through the use Serial Number of the Subject assigned by the CA. The semantics of the Serial Number for natural persons is: First letter of surname + First letter of first name+ index number. Index number is the sequential number of the prefix (as code + the first letters) in the database.

3.1.6 Recognition, authentication and role of trademarks

Not applicable.

3.2 Initial Identity Validation

Subscriber identification follows qualified trust service identity proofing requirements, including in-person or remote identification methods compliant with ETSI standards, like ETSI TS 119 461.

In the case of certificates with OID 1.3.6.1.4.1.25017.3.1.2.14, only the phone is verified.

3.2.1 Method to prove possession of private key

The possession of the private key, corresponding to the public key for which a certificate generation is requested, will be proved by sending the Certificate Signing request (CSR), per the RSA PKCS#10 standard, which will include the public key signed by the associated private key.

The request of presenting the possession proof of the private key does not apply if, on Subscriber ’s or Subject’s request, the key pair is generated by the Certification Authority or by the Registration Authority.

3.2.2 Authentication of organization identity

Authentication of organization's identity

Authentication of organization's identity is realized to prove that the legal person really exists.

When the legal entity enters into a contractual agreement with certSIGN for issuing standard certificates, the following copies of documents are required in order to identify the Subscriber (legal entity):

- Valid extract of the trade register (or the foreign equivalent for foreign companies registered under foreign law);
- Excerpt from the Register of associations and foundations (or equivalent for foreign associations and foundations)
- Official mandate, when the natural person representing the legal entity is not the legal administrator of the entity
- In the case of entities without legal personality, the identification of the Subject shall be made on the basis of the act of establishment or, in its absence, documents issued and signed by the legal representative of the public institution to which it is subordinated, attesting the identity of that institution, may be used.

The procedure described in this chapter will be applied every 6 years to verify the identity of the organization, starting with the date of issuing the first certificate under this CPS.

3.2.3 Authentication of individual identity

Identity documents required for individual identification must be valid and compliant with the minimum-security standards. These documents are:

- Identity document or passport, for Romanian citizens
- Identity document, Passport or an ID card issued by Romanian Authorities, for foreign citizens

Individual identity must be verified when:

- The individual is the Subject of a digital certificate issued by certSIGN.
- The individual is a legal entity that enters into a contract with certSIGN

Issuing Certification Authority	The Registration Authority identifies individuals using one of the following methods:
CERTSIGN Public 2023 RSA CA	By seeing the individual in person at the Registration Authority (optional)
	By a letter that shall contain a copy of the identity document
	In electronic format that shall contain copies of all original documents (recommended option)

Table 1: Requirements for the verification of individual identity

3.2.4 Non-verified subscriber information

The Subject or the Subscriber as the case may be is entirely responsible for providing up-to-date, accurate and correct information during the registration process.

In the case of OID: 1.3.6.1.4.1.225017.3.1.2.3.1 (with HW device and key generated and stored by certSIGN for remote signature and authentication), 1.3.6.1.4.1.225017.3.1.2.3.2 (with HW Device and key generated and hosted by certSIGN for remote-signature and authentication that can be used only in the relationships between the Subject and the

Subscriber) and OID 1.3.6.1.4.1.225017.3.1.2.14 the subject's telephone number (ownership) is verified by certSIGN or by third parties.

On all the other cases the e-mail address and telephone number represent non-verified Subject information.

3.2.5 Validation of authority
Not applicable.

3.2.6 Criteria for interoperation
Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key
Chapter 4.7 of this document describe the process.

3.3.2 Identification and authentication for re-key after revocation
The same process as for initial identity validation is used.

3.4 Identification and authentication for revocation request
The following entities can send certificate revocation requests:

- The Subject who is the holder of the private key associated with the public key from the certificate shall send the revocation request using any of the following methods:
  - online, by filling in the Subject name, firstname and ID, selecting the certificate to revoke, and using the revocation code received from certSIGN, according to the instructions on site: https://www.certsign.ro/ro/resurse/revoca-certificat-eidas/. In this situation, the certificate is revoked after certSIGN receives the request.
  - In electronic format, by sending to revocare@certsign.ro an authenticated request signed with a qualified electronic signature created using a qualified digital certificate issued to the Subject (i.e. with the same Common Name). In this situation, the certificate is revoked after certSIGN verifies and validates the request.
  - By filling out and submitting the request, accompanied by an original identity document, before an employee of the Registration Authority, at one of the certSIGN work offices, that can be found at https://www.certsign.ro/ro/contact/. In this case, the certificate is revoked after certSIGN verifies and validates the request.
- The Subscriber who enters into a contractual agreement with certSIGN for issuing certificates to Subjects shall send the revocation request using any of the following methods:
  - Online, by sending an authenticated request. In this situation, the certificate is revoked after certSIGN receives the request.
  - In electronic format, by sending to revocare@certsign.ro a request signed with a qualified electronic signature or qualified electronic seal. In this situation, the certificate is revoked after certSIGN verifies and validates the request.
  - By filling out and submitting the request before an employee of the Registration Authority in this case, the certificate is revoked after certSIGN verifies and validates the request.

- The Registration Authority that can request the revocation either on behalf of a Subject or because it has information that justifies the certificate revocation, using the security mechanisms of the Registration Authority software
- Trusted roles associated to certSIGN Public 2023 RSA CA, under the supervision of the Policies and Procedures Management Body (PPMB), using the security mechanisms of the Certification Authority software

4 Certificate life-cycle operational requirements

This chapter describes the basic procedures that apply to all types of certificates issued by certSIGN Public 2023 RSA CA.
The detailed 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 are described in the internal confidential documentation.
certSIGN provides access to the following services:

a. Registration, certificate issuing, rekey;
b. Certificate revocation;
c. Verification of certificate validity.

4.1 Certificate application

4.1.1 Who can submit a certificate application

Natural persons

Certificate Requests can be requested by:

- Natural persons, in case of requesting the certificate for himself
- Natural person(s) (Subjects) for whom the Subscriber requested the certificate, having a legally binding agreement or acting as their employer.

The Subscriber and the Subject shall comply with the provisions and obligations set forth in the registration form, in the applicable Subscriber Agreement and the certificate services Terms and Conditions that incorporate this CPS and the PKI Disclosure Statements.

The Certification Authority only issues certificates in reply to a request from the Registration Authority operated by certSIGN or a delegated third party.

certSIGN archives the information related to the enrolment. The archive is maintained according to the requirements defined in the CPS and in the applicable legislation.

Legal Entities (Organizations)

certSIGN issues certificates for electronic seals to legal entities.
The Subject shall comply with the provisions and obligations set forth in the Subscriber Agreement and the certificate services Terms and Conditions that incorporate this CPS and the PKI Disclosure Statements.

The Certification Authority only issues certificates in reply to a request from the Registration Authority operated by certSIGN or a delegated third party.

certSIGN archives the information related to the enrolment. The archive is maintained according to the requirements defined in the CPS and in the applicable legislation.

4.1.2 Enrollment process and responsibilities

The enrolment process is handled by a specific entity referred to as the Registration Authority or RA which is operated directly by certSIGN or by relying on a third party.

certSIGN may delegate the identification of subjects to third parties that can provide identification methods / procedures that provide an equivalent level of assurance to the Registration Authority (see Chapter 3.2.3.).

In any event, certSIGN, as a trusted service provider, shall be liable, within the limits provided in this CPP, for the acts or omissions of all its agents, employees and collaborators involved in the registration process..

The RA is responsible for the verification of the following items:

- The claimed identity of the Subject/ Subscriber,
- The claimed attributes of the Subject/ Subscriber,
- The Subject's/ Subscriber's application for the requested certificate(s)

The enrolment process is performed in compliance with the rules and methods described in the present CPS and procedures of the RA and the applicable law.

The Subject/Subscriber is provided with the following information and documents:

- The Subscriber agreement
- The Terms and conditions
- The Online address for Certificate Terms and Conditions on the certificate use
- Online address for the CPS, notifications or other documents provided by the Subject (to be defined in the Subscriber Agreement)

By signing the Subscriber agreement and the terms and conditions the Subject/Subscriber accepts and understand the following:

- His responsibility that the information provided by to RA is correct, complete, valid and up to date,
- That certSIGN retains for 10 years from the date certificate expiry/revocation all the information related to the registration and enrolment, to the certificate request and to the certificate revocation.
- That, in case certSIGN (as CA and RA) ceases its activities, this data may be transferred to a third party,
- Acknowledges the rights, obligations and responsibilities of certSIGN and of other PKI Participants, as defined in the Subscriber Agreement and by national law,
- That the Subject/Subscriber has the obligation to inform certSIGN on any change or event that may affect the validity or the content of the certificate.

Enrolment Process

The enrolment process begins at the RA.
The responsibility of the RA entity is to collect and verify the required documents/information for the subsequent validation of the Subject's/ Subscriber's identity and attributes.

The RA operator performs a first verification of the documents and verifies that the collected information is complete and correct.

After the complete verification of the Subject's/ Subscriber's documents, the RA also informs the Subject/ Subscriber about his/her rights and obligations.

The RA verifies and completes the enrolment data. RA is responsible for the accuracy of the data that will be incorporated in the certificate request submitted to the CA. The RA is responsible for the correct registration/enrolment of Subjects/Beneficiaries and for supplying the CA with the correct content for the variable fields in the certificate.

4.2 Certificate application processing

certSIGN accepts requests for one or more subjects Requests may be sent on paper or by electronic means.

The certificate application is filled out in an electronic format:

- The Subscriber agreement, terms and conditions and a copy of the ID card[5] are sent by email and digitally signed with a valid qualified digital certificate (not revoked or expired) issued by certSIGN and sent to the Certification Authority.

The certificate application can be done:

- By Subject's personal attendance at the Registration Authority or at the Certification Authority, in which case the Subscriber agreement, the terms and conditions are hand signed and a copy of the identity document[5] is submitted.
- The Subject submits to the RA the filled out and hand signed subscriber agreement, terms and conditions and a copy of the identity document[5].

4.2.1 Performing identification and authentication functions

The RA performs identification and authentication according to the procedure defined in chapter 3.2. and in the internal confidential documentation.
RA collects and validates the Subject's and Subscriber's identity information and attributes information.

4.2.2 Approval or rejection of certificate applications

Approval or rejection of certificate applications is undertaken by the RA. The RA validates each request and may reject a certificate request if the request does not comply with the rules and standards governing certSIGN Public 2023 RSA CA or for other reasons, at the discretion of and under the responsibility of the RA.

4.2.3 Time to process certificate applications

certSIGN does not issue certificate immediately upon application registration. Certificates have to be issued by the Certification Authority by approving the certificate request after it has been validated by RA.

Certificates are stored on a hardware device or on software keystore compliant to PKCS#12 and Java Keystore. The device may be provided to the entity by certSIGN after the process of key generation or the entity may have its own key generation device.

[5] The ID card copy is NOT required on issuing certificates with OID 1.3.6.1.4.1.25017.3.1.2.14; The Subscriber agreement is NOT required for test certificates.

The delivery process of certificates may take several hours or several days, but no more than 5 working days, and it depends on the availability of the Subject to receive or collect the hardware device that stores the digital certificate or to receive the PKCS#12 in an electronic format.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The certificate is issued by the CA only after receiving a certificate request from the RA. The CA and the RA are integrated systems and communicate over closed network connections. The CA only processes requests that are originated from the trusted RA of certSIGN.
The CA ensures the uniqueness of each certificate it issues using the SerialNumber field of each certificate.

4.3.2 Notification to Subscriber by the CA of issuance of certificate

The CA uses the following methods to inform a Subject about the certificate issuance:

- When the keys are generated on the hardware device by the Subject, the CA sends an e-mail to the Subject using the e-mail address provided during the application. The e-mail informs the Subject about the issuance of the certificate and provides information that allows the Subject to obtain the certificate and load it on the hardware device.
- When the keys are generated on the hardware device by certSIGN the certificate is either delivered in person to the Subject or it is sent, using postal or courier services, to the Subject. The confidential activation data (i.e. PIN code) required to access the hardware device is sent using a tamper-evident envelope.
- When the keys are generated in PKCS#12 by certSIGN, RA sends an e-mail to the Subject using the e-mail address provided during the application. The e-mail that informs the Subject about the issuance has the PKCS#12 certificate attached. The associated confidential activation data (i.e. passphrase for PKCS#12 certificate) are transmitted to the Subscriber using an out-of-band channel.

Confidential activation data (PIN) are necessary in order to be able to use the private keys stored on a hardware device. When certSIGN supplies the hardware device, the confidential activation data (PIN) is generated and delivered to a system that allows maintaining the necessary confidentiality.

Every certificate issued is published in certSIGN Repository. The certificate publication is equivalent with the notification of other Relying Parties about the fact that a certificate was issued for a Subject.
certSIGN may use "Test certificates' that are certificates with a usage limited only to testing, that have a validity of maximum 30 days, and are identified by the Common Name attribute starting with the "TEST" text. The "Test certificate" will be issued by a certSIGN Registration Operator, using certSIGN procedure for test certificates. The "Test certificate" may be revoked after the testing period on request.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The certificate shall be considered accepted by the Subject after the first use or after the period of time defined in the Terms and conditions, whichever event occurs first.

The RA and the Subject have the right to reject the certificate, provided at least one of the following objections applies:

- The information in the certificate is incorrect,
- The information in the certificate became invalid since the date of registration,
- The hardware device shows signs unauthorized use
- The hardware device malfunctions or cannot be activated,
- The envelope containing the confidential activation data (i.e. PIN code) required to access the hardware device shows signs of unauthorized access,

Obligations of the Subject and the RA in case of rejection:

- The hardware device is returned to the RA
- The RA requests revocation of the certificate
- The RA executes the revocation of the certificate

4.4.2 Publication of the certificate by the CA

See chapter 2.

4.4.3 Notification of certificate issuance by the CA to other entities

The certificate issuance is notified by certSIGN to other entities through the publication of the certificate in the repository, as described in chapter 2.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The Subject is personally responsible for:

- Using the keys only for the intended purpose as defined in the CPS and as encoded in the certificates
- Private keys corresponding to qualified certificates issued under this CPP will only be used to create electronic signatures or electronic seals
- Using tools that can correctly interpret the key usage as encoded in the certificate and that respect the key usage conditions
- Correct usage of the hardware device
- Not sharing the hardware device with another person
- Setting confidential activation data (i.e. PIN code) which are unique and which comply with the guidelines given in the CPS
- Keeping this confidential information confidential
- Safe storage of any document or medium containing transcripts of part or all of the associated confidential activation data (i.e. PIN code)
- Separation of storage for the hardware device and the associated confidential activation data (i.e. PIN code)
- Non-disclosure of the confidential activation data (i.e. PIN code) to another person.

The private key generated by certSIGN

When generating the private key for the Subject, certSIGN undertakes to:

- Initialize the hardware device and its confidential activation data (i.e. PIN code)

- Safe delivery of the hardware device to the subject;
- Safe delivery of confidential data initially associated (i.e. PIN code) to the Subject.

The Subject is bound by the obligations and conditions provided in the Subscriber agreement referencing this CPS. The Subject will protect the hardware device and any associated confidential activation data (i.e. PIN code) or other information against loss, theft, disclosure, compromise or modification.

certSIGN issues certificates for keys stored on the hardware device:
- The private key cannot be extracted from the cryptographic device
- The private key is under the (exclusive) control of the subject via secret activation data (e.g. PIN).
This secret activation data (e.g. PIN code) is transmitted to the Beneficiary using an out-of-band channel and is modified by the Subject.

The private key generated by the Subscriber

When the private key is generated by the Subscriber, the Subject is bound by the conditions and obligations mentioned in Subscriber Agreement, which include this CPS. The Subject shall protect the hardware device or the p12 container, and the certificates with any associated confidential activation data (i.e. PIN code) or other information against loss, theft, disclosure, compromise or modification.

Subscriber private key generated and hosted by certSIGN

When the private key is generated and hosted by certSIGN, there is a technical control in place to ensure that the certificate is valid at the time of use of the private key.

4.5.2 Relying party public key and certificate usage

certSIGN assumes that all user software will be compliant with X.509, and other applicable standards that enforce the requirements and requirements set forth in this CPS. certSIGN does not guarantee that any third party's software will support or enforce such controls or requirements, and all relying parties are advised to seek appropriate technical or legal advice. Parties that rely on a certificate check the digital signature at any time, by checking the validity of a certificate by means of an OCSP service at http://ocsp.certsign.ro or a relevant CRL published by certSIGN.

Partner entities are warned that an unverified digital signature cannot be assigned as a valid signature of the Subscriber.

The final decision on whether to trust a verified digital signature is the exclusive part of the trust party. Trusting a digital signature should only take place if:

- The digital signature was created during the operation of a valid certificate and can be verified by sending a validated certificate;
- The Partner entity verified the revocation status of the certificate by sending it to the relevant CRL and the certificate was not revoked.
- The Partner Entity understands that a digital certificate is issued to a Subscriber for a particular purpose and that the private key associated with the digital certificate can

be used only in accordance with the usages specified in this CPS and contained in the certificate.

The trust in the certificate is accepted as reasonable if the conditions stipulated in the CPS and in the contract concluded with the Partner Entity are fulfilled. If the assurances provided by certSIGN are not fulfilled in accordance with the provisions of this CPS, the partner entity must obtain additional insurances.

The guarantees are valid only if the steps detailed above have been performed.

Trusting a digital signature that cannot be verified can lead to risks that the partner entity assumes entirely and which certSIGN does not assume in any way.

4.6 Certificate renewal

Not applicable.

4.7 Certificate Re-key

4.7.1 Circumstance for certificate re-key

RA uses the same processes as for a newly requested certificate.

4.7.2 Who may request certification of a new public key

certSIGN always informs Subjects (at least 30 days before) about the forthcoming of the expiry period.

Rekeying is performed when a Subject holding a valid (not revoked and not expired) digital certificate generates a new key pair (or requests certSIGN to generate such a key pair) and requests the issuance of a new certificate to confirm the possession of a new created public key.
Certificate rekeying is performed only upon Subject's request and shall be preceded by the submission of a request on a corresponding form filled out by the Subscriber /Subject.

4.7.3 Processing certificate re-keying requests

RA uses the same processes as for a newly requested certificate.

4.7.4 Notification of new certificate issuance to subscriber

RA uses the same notification processes as for a newly requested certificate.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

RA uses the same processes as for a newly requested certificate.

4.7.6 Publication of the re-keyed certificate by the CA

RA uses the same processes as for a newly requested certificate.

4.7.7 Notification of certificate issuance by the CA to other entities

The RA uses the same processes as for a newly requested certificate.

4.8 Certificate modification

certSIGN does not modify the issued certificates.

The Subject or the Subscriber, as the case may be, shall request certSIGN to revoke the certificate as soon as the information included in the certificate is no longer in line with the reality.

4.9 Certificate revocation and suspension

Certificates issued by certSIGN Public 2023 RSA CA can be revoked but they are never suspended. Certificate revocation is irreversible.

The revocation affects neither the transactions made before the revocation, nor the obligations resulting from abiding by the present CPS.

This chapter states the conditions necessary for a Certification Authority to revoke the certificate.

If a private key corresponding to a public key contained in a revoked certificate stays under the Subject's control, after revocation it should be safely stored until destroyed.

The short-term certificates are not revoked. In case of short-term certificates, the mechanism to notify problems is the same mechanism described in #1.5 at "Procedure for certificate problem reporting".

4.9.1 Circumstances for revocation

The certificate is revoked when:

- The information within the certificate has changed,
- A private key associated to a public key from the certificate was compromised or there is a serious reason to suspect it was compromised,
- The employment relationship or the legal binding agreements between the Subscriber and the Subject are concluded,
- The Subject, holder of the private key associated with the public key from the certificate, requests the revocation,
- Subjects/ Subscribers do not accept new, modified terms and regulations of CPS
- The Certification Authority terminates its activity; in this case all certificates issued by this Certification Authority before the stated period for services termination shall be revoked along with the certificate of the Certification Authority,
- The Subscriber delays or does not pay the value of the services provided by certSIGN Public 2023 RSA CA,
- The private key or the security of certSIGN Public 2023 RSA CA were compromised in a manner that threatens the certificates' credibility,
- The CA receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the certificate is no longer legally permitted.
- In other cases when the Subject does not comply with the rules of this CPS, Subscriber agreement, Terms and conditions or other agreements concluded between the parties related to the services provided by certSIGN Public 2023 RSA CA.

The compromised private key means:
(1) unauthorized access to the private key or a strong reason to suspect such a thing,
(2) private key loss or occurrence of a reason to suspect such a loss,
(3) stolen private key or occurrence of a reason to suspect such a robbery,

(4) accidental deletion of the private key.

4.9.2 Who can request revocation

The following entities can send certificate revocation requests:

- The Subject who is the holder of the private key associated with the public key from the certificate
- The Subscriber who enters into a Subscriber agreement with certSIGN for issuing certificates to Subjects
- The Registration Authority that can request the revocation either on behalf of a Subject or if it has information that justifies the certificate revocation
- Trusted roles associated to certSIGN under the supervision of the Policies and Procedures Management Body (PPMB)

The revocation request may target several certificates.

4.9.3 Procedure for revocation request

The submission of the revocation request is described in chapter 3.4.
The certificate revocation request shall precisely identify each certificate, shall contain the reason(s) for which the revocation is requested.
The information about the revoked certificates is listed in the Certificate Revocation List issued by certSIGN Public 2023 RSA CA.
A certificate revocation request takes place as follows:

- certSIGN verifies the revocation request, including that it is submitted by a legitimate entity. If the request is successfully verified, certSIGN Public 2023 RSA CA enters the information concerning the certificate revocation on the Certificate Revocation List (CRL);
- certSIGN notifies the Subject about the revocation or about the decision of request rejection along with the reasons for this rejection.

Whenever a certificate or a private key corresponding to a certificate to be revoked are stored on a hardware device, after the certificate revocation, the hardware device is deleted in highly secure conditions.
This action is performed by the owner of the hardware device - a natural person or a legal entity (a representative of such entity). The owner of the hardware device must keep it safe, to prevent theft or unauthorized use until the private key is erased.
If the certificate was issued in PKCS#12 and it is revoked, the Subject shall keep it secure, or securely delete (shred) all the copies to prevent unauthorized usage of the keys.

4.9.4 Revocation request grace period

certSIGN performs the revocation within 24 hours, to ensure that the time needed to process the revocation request and to publish the revocation notification (updated CRL) is as reduced as possible.

4.9.5 Time within which CA must process the revocation request

certSIGN guarantees a maximum period of 24 hours for processing a valid certificate revocation request, after certSIGN receives the request.

When sending an authenticated request using the revocation code received from certSIGN, the certificate is automatically revoked.

The information concerning the certificate revocation is stored in certSIGN database. The revoked certificates are placed in the Certificate Revocation List (CRL) in compliance with the CRL issuance frequency.

As an exception, if the revocation request cannot be confirmed or validated within 24 hours, certSIGN will not revoke the certificate and the justification will be recorded.

4.9.6 Revocation checking requirement for relying parties

Relying Parties shall use all the resources provided by certSIGN (CRL, OCSP) to verify the status of a certificate before relying on it.

4.9.7 CRL issuance frequency

Every Certification Authority part of certSIGN issues different Certificate Revocation Lists. A new CRL is published in the Repository immediately after every certificate revocation, or within maximum one day. The CRL's availability period is of 48 hours and it is updated daily.

The Certificate Revocation List (CRL) of the certSIGN Root CA 2023 RSA Authority is issued at least once a year, provided that certificates from one of the authorities subordinated to the certSIGN CA 2023 RSA authority are not revoked.

In case of certificate revocation of an authority affiliated to certSIGN this certificate is immediately published in the Certificate Revocation List.

4.9.8 Maximum latency for CRLs

The CRL of this CA and all its subordinated issuing CAs is issued according to chapter 4.9.7 and published without delay.

4.9.9 On-line revocation/status checking availability

OCSP responses are signed by an OCSP Responder whose certificate is signed by the CA that issued the certificate whose revocation status is being checked.

The OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-line revocation checking requirements

See chapter 4.9.6 of the current document.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements re key compromise

If a Subject knows or suspects that the integrity of his certificate's private key has been compromised, the Subscriber shall:

- Immediately cease using the certificate,
- Immediately initiate revocation of the certificate,
- Delete the certificate from all devices and systems,

Inform all Relying Parties that may depend on this certificate.

The compromise of the private key may have implications on the information protected with this key. The Subscriber must decide how to deal with the affected information before deleting the compromised key.

4.9.13 Circumstances for suspension
Not applicable

4.9.14 Who can request suspension
Not applicable

4.9.15 Procedure for suspension request
Not applicable

4.9.16 Limits on suspension period
Not applicable

4.10 Certificate status services

4.10.1 Operational characteristics
certSIGN's certificate status services are CRL and OCSP. Access to these services is made through the web site "www.certsign.ro". ocsp.certSIGN.ro". Certificate status services provide information on the status of valid certificates. The integrity and authenticity of the status related information is protected by a digital signature of the respective CA.

4.10.2 Service availability
Certificate status services are available 24 hours a day, 7 days a week.

4.10.3 Optional features
certSIGN certificate status services do not include or require any additional feature.

4.11 End of subscription
End of subscription occurs after:

- Successful revocation of the last certificate of a Subscriber/Subject,
- Expiration of the last certificate of a Subscriber/Subject.

certSIGN and all registration authorities must keep all data and documentation for a period of 10 years from certificate expiry/revocation.

4.12 Key escrow and recovery
certSIGN does not provide key escrow for certificates issued by certSIGN Public 2023 RSA CA.

4.12.1 Key escrow and recovery policy and practices
No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices
No stipulation.

5 Facility, management and operational controls

As a certificate 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 27001:2013 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 CA and RA 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 EN 319 411-1, Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

certSIGN, as a QTSP, maintains documented procedures covering personnel security, segregation of duties, incident management, and risk assessment in accordance with Clause 6 of ETSI TS 119 431-1.

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 CA and RA 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 CA and RA 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,
- CA operators' area
- RA operators and 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 CA and RA operations are also connected to UPSes. The main components of the physical security protection system are also connected to UPSes 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 retention period expires, paper and electronic media containing information significant for certSIGN security are destroyed. Security hardware modules are destroyed in compliance with the manufacturer's recommendations.

When no longer required, the HSMs will be zeroized to prevent any possibility of re-using the CA private keys, and returned to cryptographic inventory.

After cessation of operation, the tokens and cards of trusted roles will be destroyed.

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

5.1.8 Off-site backup

Copies of cryptographic cards are stored in safe-deposit box outside certSIGN primary location.

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 48 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 certification 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 CA 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 the following trusted roles to one or more individuals:

- **Security officer** – Overall responsibility for the implementation of the security practices and policies.
- **System administrator** – Authorized to install, configure and maintain the Certification Authority's trustworthy systems for registration, certificate generation, subject device provision and revocation management. Installs hardware and operating systems; installs and configures the network equipment.
- **System operator** – Responsible for operating the Certification Authority's trustworthy systems on a day to day basis. Authorized to perform system backup and recovery. Has access to Subjects' certificates; revokes Subjects' certificates; provides continuity of backup copies and archives of database and system logs creation; manages databases; has access to confidential information about Subjects/ 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**: Responsible for verifying information that is necessary for certificate issuance and approval of certification requests;
- **Revocation Officers:** Responsible for operating certificate status changes;
- **System Auditor** – Authorized to access archives and audit logs of the Certification Authority's trustworthy systems. Responsible for performance of internal audit, compliance of a Certification Authority with this CPS; this responsibility extends also to the Registration Authority, operating within certSIGN.
- **Signer**: is the end-user, authorized to use the TW4S by passing the SAD as part of the SAP in order to sign the document or the DTBS/R, which potentially can be passed through the SAP as well.
- **SCA**: is the app, used by the end-user, authorized to send the DTBS/R request to the TW4S in order to be signed by a signer.

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 related to certificates, of employees in trusted roles are monitored.

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 a Certification Authority or a Registration Authority:

- 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 between a Certification Authority and a Registration Authority acting on behalf of it.

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 certification 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 Certification Practice Statement,
- Procedures and security controls employed by the Certification Authority and the Registration Authority
- Responsibilities arising from roles and tasks performed in the system,

Upon completion of the training, participants sign a document confirming their familiarization with Certification Practice Statement, other relevant documentation 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 modification to certSIGN operations are made.

5.3.5 Job rotation frequency and sequence

No stipulation.

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 labor 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:

- CPS,
- 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 certification 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 certificate 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 and 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). The time used to record events as required in the audit log are synchronized with UTC at least once a day.

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 certification services, for example: registration and certification request, rekey request, certificate acceptance, certificate issuing and CRL 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.

certSIGN CA and each Delegated Third Party record events related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems. The CA and each Delegated Third Party record events related to their actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. certSIGN CA make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

The CA record at least the following events:

1. **CA certificate and key lifecycle events**, including:
   - Key generation, backup, storage, recovery, archival, and destruction;
   - Certificate requests, renewal, and re-key requests, and revocation;
   - Approval and rejection of certificate requests;
   - Cryptographic device lifecycle management events;
   - Generation of Certificate Revocation Lists;
   - Signing of OCSP Responses
   - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

2. **Subscriber Certificate lifecycle management events**, including:
   - Certificate requests, renewal, and re - key requests, and revocation;
   - All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
   - Approval and rejection of certificate requests;
   - Issuance of Certificates;
   - Generation of Certificate Revocation Lists;
   - Signing of OCSP Responses.
3. **Security events**, including:
   - Successful and unsuccessful PKI system access attempts;
   - PKI and security system actions performed;
   - Security profile changes;
   - Installation, update and removal of software on a Certificate System;
   - System start-up and shutdown, crashes, hardware failures, and other anomalies;
   - Relevant router and firewall activities (as described below);
   - Entries to and exits from the CA facility.

Every automatic or manual recording contains the following information:

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

Logging of router and firewall activities at a minimum include:

- Successful and unsuccessful login attempts to routers and firewalls;
- Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications;
- Logging of all changes made to firewall rules, including additions, modifications, and deletions;
- Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

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 Subject/ Subscriber agreement
- Any specific choices in the Subject/ Subscriber agreement (e.g. consent to publication of certificate)
- Identity of entity accepting the application;
- Method used to validate identification documents,

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

The privacy of subject 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 Retention Period for audit log

event logs are stored in files on the system disk until they reach the maximum allowed capacity. During this 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 10 years.

The CA and each Delegated Third Party retain:

1. CA certificate and key lifecycle management event records after the later occurrence of:
    - the destruction of the CA Private Key; or
    - the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1) after the expiration of the Subscriber Certificate;
3. Any security event records (as set forth in Section 5.4.1) after the event occurred

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 retention 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

- Analyze
- Correlate
- Archive
- Long term Back-up

5.4.7 Notification to event-causing subject

No stipulation.

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 27001:2013 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 Subjects/ Subscribers, information about Subjects/ Subscribers, issued certificates and CRL's, keys used by Certification and Registration Authorities, and whole correspondence between certSIGN and the Subject/ Subscribers should be subjected to archive.

The on-line Repository contains the active certificates and can be used to perform some external services of the Certification Authority, such as checking the validity of a certificate, publishing the certificates for their owners (restoring certificates) and authorized entities.

The archive contains expired certificates, including revoked certificates. Revoked certificate archive contains information about a certificate, reason of revocation, date when the certificate was placed on CRL. The archive is used for dispute resolving regarding old documents electronically signed by a Subject.

Backup copies are created and retained outside certSIGN location.

5.5.1 Types of records archived

The following data are subjected to a trustworthy archive:

- All certificates for a period of 10 years after their expiration
- The archived journals of logs are kept 10 years.
- Logs of issuance and revocation of certificates for a period of 10 years after issuance/revocation
- CRLs for 10 years after publishing
- The following for 10 years after any certificate based on these records ceases to be valid:
    - log of all events relating to the life cycle of keys managed by the CA, including any subject key pairs generated by the CA
    - signed terms and conditions regarding use of the certificate

5.5.2 Retention period for archive

See section 5.5.1 above. After expiration of the declared retention 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 retention 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 Key Changeover

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, certSIGN ceases using its expiring CA Private Key to sign Certificates (at least three years in advance of expiration) and uses the old Private Key only to sign CRLs. A new CA signing key pair is commissioned and all subsequently issued certificates and CRL's are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in chapter 6.1.4.

5.7 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 accepted Business continuity and disaster recovery plan.

5.7.1 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 certification 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 analyzed 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 CPS.

certSIGN maintains the same incident response process to detect, respond to, and notify relevant parties of security incidents affecting the remote QSCD service.

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.

5.7.2 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 Certification Authority 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 certification and timestamp services are continuously monitored and all the security events are logged and analyzed. 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 analyzed is taken into account 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 certification services as well the availability of critical services is also monitored.

certSIGN addresses any critical vulnerability not previously addressed, within a period of 48 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.

5.7.3 Entity private key compromise procedures

Compromise of the CA private key(s) or of the associated activation data implies immediate revocation of the certificate of the compromised key(s).

In case of Certification Authorities (affiliated with certSIGN) private key compromise or suspicion of such compromise the following actions will also be taken:

- Notification of the compromise to all Subjects/ subscribers and other entities with which certSIGN has agreements or other form of established relations, among which relying parties and other trust services providers. In addition, this information will be made available to other relying parties by means of mass media and electronic mail
- Notification of the general public through several channels, including a message on the certSIGN's CA repository and web site, a press release in the media
- A certificate corresponding to the compromised key is placed on Certificate Revocation List
- All the certificates signed by the corrupted CA are revoked and a suitable reason for revocation is submitted

- The Certification Authority generates a new key pair and a new certificate
- New certificates for Subject are generated
- The new certificates for Subjects are submitted to them free of charge
- If a Certificate is revoked because of CA key compromise, certSIGN Root CA 2023 RSA will issue a new CRL within 24 hours after receiving notice of the compromise and publish online CRLs immediately.

When a private key associated to a public key from the certificate was compromised or there is a serious reason to suspect it was compromised, the Subject or the Subscriber, as the case may be, shall request certSIGN to revoke the certificate.

The previous paragraph is also applicable in case PKI algorithms or associated parameters being compromised or if they become insufficient for the remaining intended usage.

5.7.4 Business continuity capabilities after a disaster

certSIGN has established in a Business Continuity and Disaster Recovery Plan all the necessary measures to ensure full recovery of its 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 CA operations are backed up and stored in a remote and safe place, suitable to allow certification 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.

The BCP & DRP plans address also the compromise, loss or suspected compromise of a CA's private key or the compromise of the PKI algorithms as a disaster and the planned processes are in place.

Business continuity and disaster recovery plans also ensure availability and integrity of the remote QSCD service.

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

5.8 CA or RA termination

certSIGN has an up-to-date termination to minimize disruptions to Subjects/ Subscribers and Relying Parties which might arise from a decision of a Certification Authority to cease operation. The plan includes obligations to notify in advance all Subjects/ Subscribers of the authority that certified the Certification Authority subjected to termination (if such exists) and transition of responsibilities (services provided to the Subjects/ Subscribers, databases, etc.), in compliance with the regulations in force to another Certification Authority.

Requirements associated to duty transition

Before a Certification Authority ceases its activity, it will:

- Inform (at least 30 days in advance) the following about the decision to terminate its services: all Subjects/ Subscribers who hold active (unexpired and unrevoked) certificates issued by this authority 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;
- Revoke the unexpired certificates that have been issued.
- Transfer its obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the certification services for a reasonable period, unless it can be demonstrated that certSIGN do not hold any such information. The information refers to registration information, revocation status for unexpired certificates that have been issued. and event log archives for their respective period of time as indicated to the Subjects/ Subscriber and relying party
- Destroy CA private keys, including backup copies, or withdrawn them from use, in such a manner that the private keys cannot be retrieved;
- Where possible, make arrangements to transfer provision of certification services for the existing customers to another certification service provider

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

In case certSIGN will terminate its activities without a partially or full transfer of its activities, it will revoke the impacted certificates one month after having notified Subscriber and/or Subjects and 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.

Certificate issuance by the successor of terminated Certification Authority

To provide continuity of certificate issuance services for Subjects, a terminated Certification Authority may sign an agreement with another Certification Authority that provides similar services related to the issuing of replacement certificates for the valid certificates of the terminated certification authority.

Issuing a replacement certificate, the successor of the terminated Certification Authority takes over the rights and obligations of the terminated Certification Authority related to the management of the certificates which remain in usage.

The archive of the Certification Authority ceasing its service has to be turned over to the primary Certification Authority – certSIGN ROOT CA 2023 RSA in the case of termination of services of certSIGN Public 2023 RSA CA.

5.9 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

6.1 Key pair generation and installation

This Chapter describes the procedures for generation and management of a cryptographic key pair of a Certification Authority, including the associated technical requirements. Appropriate security controls are in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle. Those security measures protect also the activation data of the cryptographic keys, the repositories, the Private Keys and activation data for the Private Keys of subject CAs, and other PKI Participants, and other critical security parameters.

Procedures for key management apply to secure storage and usage of the keys being held by their owner. Particular attention is attached to the generation and protection of certSIGN's private keys, influencing secure operation of the whole public key certification system.

Remote QSCD operations are protected by certified cryptographic modules, secure key generation, non-extractable key storage, and approved cryptographic algorithms.

certSIGN Public 2023 RSA CA owns at least one certificate signed by **certSIGN ROOT CA SIGN 2023 RSA**. The private key corresponding to the public key contained in the certificate is used exclusively to sign the public keys of the Subjects and the Certificate Revocation List necessary for the functioning of the CA.

An electronic signature is created by means of RSA algorithm in combination with SHA-2 cryptographic digest.

certSIGN issues certificates for keys stored on hardware devices or in software format.

6.1.1 Key pair generation

certSIGN has a documented procedure for conducting CA key pair generation for CA. This procedure indicates the following:

- Roles participating in the ceremony (internal and external from the organization);
- Functions to be performed by every role and in which phases;
- Responsibilities during and after the ceremony; and
- Requirements of evidence to be collected during the ceremony.

After the key ceremony certSIGN will produces a key ceremony report proving that it is carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. This report shall be signed by the trusted role responsible for the security of the certSIGN's key management ceremony (e.g. security officer) as witness that the report correctly records the key management ceremony while carried out.

In all cases, certSIGN:

- Generates the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the Certification Practice Statement;
- Logs its CA key generation activities; and
- Maintains effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certification Practice Statement and (if applicable) its Key ceremony Script.

The keys of **certSIGN Public 2023 RSA CA** as well as the keys of other subordinated authorities and the subsequent certification of the public keys, are undertaken in a physically secured environment by personnel in trusted roles under, at least, dual control:

- At least three employees in trusted roles
- The security officer
- At least one representative of Policies and Procedures Management Body (PPMB)
- A Master of Key Ceremony
- At least one independent or external auditor

Key pairs of **certSIGN Public 2023 RSA CA** are generated on designated, authenticated workstations and connected to hardware security modules, complying with the requirements of FIPS 140-2 Level 3 or ISO/IEC 15408 EAL 4. They are permanently retained encrypted on these devices.

certSIGN Public 2023 RSA CA's key pair generation process is similar to the accepted procedure for key pair generation in certSIGN, as described above. Actions executed while performing key pair generation are recorded, dated and signed by each person present during the generation. The records are retained for the needs of audits and common system reviews.

Registration Authority operators possess only keys to authenticate all their actions. These keys are generated by the operator (in the presence of the security officer) by means of authenticated software supplied by a Certification Authority and on a QSCD.

CA key pair generation is performed using the RSA algorithm with a 4096 bits key length.

Before expiration of its CA certificate which is used for signing subject keys, the CA will generate a new certificate for signing subject key pairs and will apply all the necessary actions to avoid disruption to the operations of any entity that may rely on the CA certificate. The new CA certificate will also be generated and distributed in accordance with this CPS. These operations should be performed with a suitable time range between the certificate expiry date and the last certificate signed to allow all parties that have relationships with certSIGN (subjects, Subscriber, relying parties, CAs higher in the CA hierarchy, etc.) to acknowledge

this key changeover and to implement the required operations in order to avoid any inconvenience and malfunction. This does not apply to the case in which we would cease our operations before our own certificate-signing or certificate expiration date.

The Subjects' keys are generated by the Subject or by certSIGN, either using hardware devices () or in software formats (p12 container conforming to PKCS12 standard).

CERTSIGN provides technical and non-technical procedures to securely delete subjects' private keys after they have been generated by the CA and delivered to the subject.

6.1.2 Private key delivery to Subscriber

Private key generated by certSIGN

When the keys are generated on the hardware device by certSIGN, the hardware device where the digital certificate is stored is either delivered in person to the Subject or is sent, using postal or courier services, to the Subject. The confidential activation data (i.e. PIN code) required to access the hardware device is sent using a tamper-evident envelope.

When the keys are generated in PKCS#12 by certSIGN, RA sends an e-mail to the Subject using the e-mail address provided during the application. The e-mail that informs the Subject about the issuance has the PKCS#12 certificate attached. The associated confidential activation data (i.e. passphrase for PKCS#12 certificate) are transmitted to the Subscriber using an out-of-band channel.

certSIGN provides technical and non-technical procedures to safely delete the subject private keys after being generated by the CA, and being delivered to the subject.

Private key generated by Subject

When the keys are generated by Subject, it is the Subject's responsibility to use the appropriate hardware device or software tool for generating software format keys, conforming to the requirements of the present CPS. certSIGN rejects a certificate request which is not conforming to the requirements of the present CPS.

6.1.3 Public key delivery to the certificate issuer

Subjects submit their generated public keys as an electronic request whose format has to comply with protocols of PKCS#10 (CSR).

Submission of a public key does not apply in the case where a key pair is generated on Subject/ Subscriber's demand by certSIGN, which issues a certificate for the generated key pair.

6.1.4 CA public key delivery to relying parties

CA signature verification (public) keys is made available to relying parties in a manner that ensures the integrity of the CA public key and authenticates its origin.

The public keys of a Certification Authority issuing certificates to Subjects are distributed solely under the form of certificates complying with the ITU-T X.509 v.3 recommendations. In the case of certSIGN Public 2023 RSA CA Certification Authority, certificates are signed.

certSIGN Certification Authorities publish their certificates by placing them in the publicly available repository of certSIGN https://www.certsign.ro/en/repository/

certSIGN Certification Authorities certificates may be delivered to Relying Parties together with the software (operating systems, web browsers, email clients, etc.), which allows usage of services offered by certSIGN.

Certificates repository enforces access control upon certificates addition, deletions or upon modification of related information.

6.1.5 Key sizes

certSIGN Public 2023 RSA CA uses a 4096-bit key for CRL signing.

The digital certificates issued by certSIGN Public 2023 RSA CA may use 3072-bit RSA keys or 4096-bit RSA keys.

The digital certificates are signed using RSA algorithm in combination with SHA-2 cryptographic digest.

certSIGN reserves the right to introduce other algorithms and protocols than RSA with SHA-2 or longer key lengths in the future. This may include Elliptic Curve algorithms instead of RSA and other hash algorithms.

6.1.6 Public keys parameters generation and quality checking

certSIGN has a documented procedure for conducting CA key pair generation for all CAs, including, certSIGN Public 2023 RSA CA.

For Subject keys there is no specific policy implemented regarding public keys parameters generation and parameter quality checking.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Allowed key usage purposes are described in the KeyUsage field (see Chapter 7.1.1.2) of the standard extension of a certificate complying with X.509 v3. This field has to be verified by the Subscriber's application managing the certificates.

Usage of bits of KeyUsage field has to comply with the following rules:

a) digitalSignature: certificate intended for electronic signature verification,
b) nonRepudiation: certificate intended to provide a non-repudiation service by private individuals, as well as for purposes other than those described under f) and g). NonRepudiation bit may be set only in a public key certificate intended to verify electronic signatures and should not be combined with the purposes described at points c)-e) and connected with providing confidentiality,
c) keyEncipherment: intended to encrypt symmetric algorithm keys, providing data confidentiality,
d) dataEncipherment: intended to encryption of Subject's data, other than those described in c) and e),
e) keyAgreement: intended for protocols of key exchange,
f) keyCertSign: public key is used for electronic signature verification in certificates issued by entities providing certification services,
g) cRLSign: public key is used for verification of electronic signatures on revoked and suspended certificates lists issued by entities that provide certification services,
h) encipherOnly: may be used solely with keyAgreement bit to indicate its purpose of data encryption in key exchange protocols,

i) decipherOnly: may be used solely with keyAgreement bit to indicate its purpose of data decryption in key exchange protocols.

6.2 Private key protection and cryptographic module engineering controls

Every Subject, Certification Authority operator and Certification Authority generates and stores his/her/its private key employing a reliable system that prevents private key loss, disclosure, modification or unauthorized access. If a Certification Authority generates a key pair on an authorized Subject/ Subscriber 's demand, it has to deliver it in a secure manner to the Subject and enforce the Subject to protect his/her/its private key.

certSIGN uses appropriate secure cryptographic devices to perform CA key management tasks. These cryptographic devices are also known as Hardware Security Modules (HSMs).

Hardware and software mechanisms that protect CA private keys are adequately documented. HSMs are prepared, distributed and managed in compliance with the following technical standards:

- ETSI EN 319 401
- ETSI EN 319 411-1

Measures are taken so that the secure cryptographic devices are not tampered with during shipment and storage at certSIGN's premises.

HSMs do not leave the secure environment of the CA secured premises. In case HSMs require maintenance or repair that cannot be performed within CA secured premises (under dual control of more than one employee in a trusted role), they are securely decommissioned.

Between usages sessions, HSMs are kept securely within the CA secure premises.

The CA private keys remain under n out of m multi-personnel control. CA custodians are assigned the task to activate and deactivate CAs private keys. CAs keys are then active for defined time periods.

The CA private signing keys stored on the CA's secure cryptographic device shall be destroyed upon device retirement.

6.2.1 Cryptographic module standards and controls

certSIGN Public 2023 RSA CA is using hardware keys protection which is complying at least with FIPS 140-2 level 3 or Common Criteria EAL 4 standards. CA key pair generation shall be carried out within a secure cryptographic device which is a trustworthy system complying at least with FIPS 140-2 level 3 or Common Criteria EAL 4 standards.

The Subjects' keys are generated by the Subject or by certSIGN, either using hardware devices or in software formats.

6.2.2 Private key (n out of m) multi-person control

Multi-person control of a private key applies to private keys of **certSIGN Public 2023 RSA CA** used for certificate and CRL signing.

The dual access control is achieved by delivering secrets to authorized operators. The secrets are stored on cryptographic cards or tokens, protected by a PIN code and transferred authenticated to their owner.

Shared secret transfer procedure has to include: key generation and distribution process, acceptance of delivered secret and resulting responsibilities for its safekeeping.

Acceptance of secret shared by its holders

Every shared secret holder, before receiving his/her secret, should verify the correctness of a created secret and its distribution. Each part of the shared secret has to be transferred to its holder on a cryptographic card or token protected by a PIN number assigned by the holder and known only to him/her. The reception of the shared secret and its appropriate creation is confirmed by signature on an appropriate form, whose copy is retained in the Certification Authority archives and by the secret holder.

Protection of shared secret

Holders of shared secret have to protect their share from being disclosed. The holder declares that he/she:

- Will not reveal, copy or share the secret with any other party and that he/she will not use the share in an unauthorized manner,
- Will not reveal (directly or indirectly) that he/she is the holder of the secret,

Availability and erasure (transfer) of the shared secret

The holder of a shared secret should allow access to his/her share to authorized legal entities (in an appropriate form, signed by the holder upon delivery of the share) only after authorization of secret transmission. This situation should be recorded in the security system as an appropriate transaction log.

In the case of natural disasters, the holder of the secret should attend himself/herself in the emergency recovery site of certSIGN, according to instructions submitted by the share issuer. The shared secret should be delivered by the holder to the emergency recovery site personally in a manner allowing share usage for restoration of certSIGN activity to its normal state.

Responsibilities of shared secret holder

The shared secret holder should perform his/her duties and obligations according to the requirements of this Certification Practice Statement and in a deliberate and responsible manner in any possible situation. A shared secret holder should notify the issuer of the shared secret in case of theft, loss, unauthorized disclosure or security violation immediately after the incident occurrence. A shared secret holder cannot be accused of neglecting his/her duties due to reasons that are beyond his/her control. On the other hand, he is responsible for inappropriate disclosure of the secret or for omitting to notify the issuer of the secret about the security violation of the secret, resulting from the holder's mistake, negligence or irresponsibility.

Multi person control does not apply to Subject's private key.

6.2.3 Private Key escrow

Private keys of Certification Authorities are not subject to custody.

Subject's private keys are not subject to custody.

6.2.4 Private key backup

Certification authorities operating within certSIGN create a backup copy of their private key. Copies are used in case of execution of standard or emergency key recovery procedure (e.g.

after disaster). When outside the secure cryptographic device, the CA private key is protected in a way that ensures the same level of protection as provided by the secure cryptographic device. The copies of the private keys are protected by shared secrets.

certSIGN does not retain copies of Certification Authority operator private keys.

The CA private signing key are backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. The number of personnel authorized to carry out this function is kept to a minimum and consistent with the CA's practices.

Copies of the CA private signing keys are subject to the same or to a greater level of security controls as keys currently in use.

Private key backup does not apply to Subject's private key.

6.2.5 Private key archival

Private keys of Certification Authorities used for electronic signature creation are not archived – they are destroyed immediately after termination of performance of cryptographic operation employing such keys or after expiry of the associated public key certificate or after its revocation.

6.2.6 Private Key transfer into or form a cryptographic module

The operation of entering a private key into a cryptographic module is carried out in the following cases:

- Upon creation of backup copies for private keys stored in a cryptographic module, it may be occasionally necessary (e.g. in the case of module corruption or malfunction) to enter a key pair into a different security module,
- When it is necessary to transfer a private key from the operational module, used by the entity for standard operations, to another module; the situation may occur in the case of module failure or decommissioning.

Entry of a private key into the security module is a critical operation, therefore measures and procedures, preventing key disclosure, modification or forgery are implemented during execution of the operation.

Introducing a private key into a security hardware module of the Certification Authority **certSIGN Public 2023 RSA CA** requires the restoration of the key on HSM in the presence of a corresponding number of shared secret owners that protect the module containing the private keys. Due to the fact that the Certification Authority can retain an encrypted copy of its private key, the keys may also be transferred between modules.

6.2.7 Private key storage on cryptographic module

certSIGN uses Hardware Security Modules (HSMs) to perform CA key management tasks. Measures are taken so that the secure cryptographic devices are not tampered during shipment and while they are stored at certSIGN's premises.

Access controls shall be in place to ensure that the keys are not accessible outside the dedicated secure cryptographic devices where the CA private signing keys and copies are stored.

HSMs do not leave the secure environment of the CA secured premises.

Between usages sessions, HSMs are kept securely within the CA secure premises.

The CA private keys remain under n out of m multi-personnel control. CA custodians are assigned the task to activate and deactivate the CAs private keys. CAs keys are then active for defined time periods.

Operators use qualified electronic signature creation devices (tokens/cards). Keys are always generated on the devices and never leave them. The secure devices are protected from producers to certSIGN, on storage while at certSIGN and while distributed.

Subject private key may be stored on hardware cryptographic devices. The embedded microchip protects private keys and other security related information against attacks.

6.2.8 Method of activating the private key

All private keys of **certSIGN Public 2023 RSA CA** are entered into the module after their generation, import in an encrypted form from another module or after restoration from shared secrets. Activation of private keys is always preceded by the operator's authentication. The authentication is carried out on the basis of a cryptographic card held by the operator.

When delivered by certSIGN, Subject private key may be accessed only by using confidential activation data (i.e. PIN code).

6.2.9 Method of deactivating private key

certSIGN Public 2023 RSA CA private key deactivation method applies to key deactivation after their usage or upon completion of every session during which the key was used (e.g. application logoff).

When stored on hardware cryptographic devices the Subject's private key may be deactivated by disconnecting the cryptographic device from the computer or from any other device.

When stored in software format, Subject's private key deactivation depends on the configuration of the software storing it.

6.2.10 Method of destroying private key

At the end of their lifetime, the CA private keys are destroyed by trusted CA roles in the presence of more than one representative of the Policies and Procedures Management Body (PPMB) in order to ensure that these private keys cannot ever be retrieved or used again.

The CA private key can be destroyed by deleting all HSM Cards (Operator and Administrator). Furthermore, the HSMs allow device zeroization by physical access and settings on the device. This reinitializes the device and overwrites all of the data on it with binary zeros. In cases when this zeroization or re-initialization procedure fails, certSIGN will crush, shred and/or incinerate the device in a manner that destroys the ability to extract any secret.

These hardware modules are treated in a secure manner as described in the documented key destruction internal procedures. Associated records are securely archived. The Policies and Procedures Management Body (PPMB) authorizes the CA private key destruction and assigns the personnel for the task.

Every private key destruction is recorded in the event journal.

The Subject is responsible for the private key destruction. For keys stored on hardware cryptographic devices this can be done either using the device's middleware initialization

features or by physically destroying the device. For keys stored in software format the Subject shall delete (shred) all the copies to prevent unauthorized usage of the keys.

6.2.11 Cryptographic module rating

See above.

6.3 Other aspects of key pair management

certSIGN shall use appropriately the CA private signing keys and shall not use them beyond the end of their life cycle.

CA signing key(s) used for generating certificates and certificate revocation lists shall not be used for other purposes.

The certificate signing keys shall only be used within physically secured premises.

The use of the CA's private key shall be compatible with the hash algorithm, the signature algorithm and the signature key length used for generating certificates, in line with current practices (the selected key length and algorithm for CA signing key are RSA 4096 bits in agreement with requirements in ETSI TS 119 312 for the CA's signing purposes)

All copies of the CA private signing keys shall be destroyed at the end of their life cycle.

The attributes of the **certSIGN Public 2023 RSA CA** certificate shall be compliant with the defined key usage as stipulated in the Recommendation ITU-T X.

6.3.1 Public key archival

certSIGN archives its own CA public keys and all the public keys certified by certSIGN Public 2023 RSA CA under the form of X509 certificate containing the key,

See chapter 5.5 for archival conditions.

6.3.2 Certificate operational periods and key pair usage periods

Usage period of public keys is defined by the value of the validity field of every public key certificate. It is also the validity period applied to a private key. The maximum usage period of Subject's keys cannot exceed the validity period of a certificate.

The validity period of certSIGN Public 2023 RSA CA certificate is 7 years.

The validity period of a Subject certificate is up to 3 years.

Usage periods of certificates and the related private keys may be shortened in the case of revocation of a certificate.

Generally, the validity start date of a certificate matches the date of its issuance. It is not allowed to set this date in the future or in the past.

6.4 Activation data

For remote (Q)SCD, signature activation requires multi-factor authentication ensuring sole control by the signatory, as required by ETSI TS 119 431-1 Clause 7.

6.4.1 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.

Registration Authority and Certification Authority operators and 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 RA and CA 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 Certification Authority 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 CAs 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 CA's key pairs in a secure cryptographic device shall require simultaneous control of at least two employees in trusted roles.

When the Subjects generate the private keys, it is their responsibility to generate also the activation data (i.e. PIN code).

When the keys are generated by certSIGN, reasonable security measures are in place to send the activation data (i.e. PIN code) to the Subject (see #6.1.2).

6.4.2 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.

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

6.4.3 Other aspects of activation data

No stipulation

6.5 Computer security controls

Tasks of Registration Authorities and Certification Authorities operating within certSIGN are carried out by means of trusted hardware and software.

6.5.1 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.

6.5.2 Computer security rating

certSIGN computer system complies with requirements described in ETSI Standards: ETSI EN 319 401(General Policy Requirements for Trust Service Providers) and CEN CWA 14167 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures).

6.6 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.

6.6.1 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.

6.6.2 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.

6.6.3 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 Issuing 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 certification services is monitored and that estimates of capacity requirements are made to ensure that adequate processing power and storage are available.

6.7 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 certification 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 certification 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 certification 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 certification 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 certification 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 on the basis of firewall and traffic filtering on the routers and Proxy services that protect certSIGN's internal network domains from unauthorized access including access by Subjects/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 CA 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 CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

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

The **certSIGN Public 2023 RSA CA** system is in a high security zone.

6.8 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 Certificate, CRL and OCSP profile

Certificate profiles and Certificate Revocation List (CRL) profile comply with the format described in ITU-T X.509 v.3 standard, while the profile of OCSP complies with the requirements of RFC 6960. Information stated below describes the meaning of respective certificate fields, CRL and OCSP, applied standard and private extensions used by certSIGN.

7.1 Certificate profile

Profile of basic fields for CERTSIGN Public 2023 RSA CA certificate in described in Table 7.1.

Field name	Value or value's constraint	
Version	3	
Serial Number	10014c29b26fd49dd2a7	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	CommonName (CN)=	certSIGN ROOT CA SIGN 2023
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
Not before	Dec 12 09:33:53 2023 GMT	
Not after	Dec 12 09:33:53 2030 GMT	
Subject (Distinguished Name)	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-18288250
	Common Name (CN) =	CERTSIGN Public 2023 RSA CA
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
Subject Public Key Info	4096 bits RSA key	
Signature	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	

Table 7.1. Profile of the basic fields for CERTSIGN Public 2023 RSA CA

Profile of basic fields for certificates issued by CERTSIGN Public 2023 RSA CA is described in Table 7.2.

Field name	Value or value s constraints	
Version	Version 3	
Serial Number	Unique value greater than zero (0) for all certificate issued by Certification Authorities within CERTSIGN. It contains a random value of 8 bytes. A hardware cryptographic module is used for generating this value.	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-18288250
	Common Name (CN) =	CERTSIGN Public 2023 RSA CA
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
Not before	Universal Time Coordinated based.	

Field name	Value or value s constraints
Not after	Universal Time Coordinated based.
Subject (Distinguished Name)	Encoded in accordance with RFC 5280, may contain fields presented in Chapter 3.1.2.
Subject Public Key Info	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key); RSA key size is presented in Chapter 6.1.5.
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.

Table 7.2. Profile of the basic fields of certificates issued by CERTSIGN Public 2023 RSA CA

7.1.1 Version number(s)

All certificates issued by CERTSIGN are X.509 version 3.

7.1.2 Certificate extensions

Certificate extensions for CERTSIGN Public 2023 RSA CA are described in Table 7.3.

Extension	Value or Value constraint	Extension status
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl.certsign.ro/certsign-rootcasign2023rsa.crt	Non-critical
Basic Constraints	Subject type=CA, Path length constraint=0	Critical
Key Usage	keyCERTSIGN (bit 5), cRLSign (bit 6)	Critical
Authority Key Identifier	8FC8D655EA3600BDB008D9A70FBA88818A4119B5	Non-critical
Subject Key Identifier	8BC9B01408769D200B559070BEB9992A4EC0684E	Non-critical
Certificate Policies	Certificate Policies [1] Certificate Policy: Policy Identifier=All issuance policies [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution Points	http://crl.certsign.ro/certsign-rootcasign2023rsa.crl	Non-critical

Table 7.3. Extensions of CERTSIGN Public 2023 RSA CA certificate

Certificates extensions for End-Entity certificates are described in Table 7.4.1 and 7.4.2

Extension	Value or Value constraint	Extension status
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl.certsign.ro/certsign-publicca2023rsa.crt	Non-critical
Key Usage	digitalSignature (bit 0) and nonRepudiation (bit 1)	Critical
Authority Key Identifier	8FC8D655EA3600BDB008D9A70FBA88818A4119B5	Non-critical
Subject Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	Non-critical
Certificate Policies	Certificate Policies [1] Certificate Policy: Policy Identifier=0.4.0.2042.1.3 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2] Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.3.1.2.{3, 3.1, 3.2, 4, 11, 11.1, 12, 14} [2,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2,2]* Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=The certificate can be used only in the relationships between the subject and the subscriber. *This extension is present only in certificates with OID 1.3.6.1.4.1.25017.3.1.2.3.2	Non-critical
CRL Distribution Points	http://crl.certsign.ro/certsign-publicca2023rsa.crl	Non-critical
Subject Alternative	Other Name: RFC822 Name and Principal Name (UPN)	Non-critical

Extension	Value or Value constraint	Extension status
Name	*This extension is optional*	
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2), and Document Signing (1.3.6.1.4.1.311.10.3.12)	Non-critical

Table 7.4.1 Extensions of the signing certificates for End-Entity

Extension	Value or Value constraint	Extension status
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl.certsign.ro/certsign-publicca2023rsa.crt	Non-critical
Key Usage	keyEncipherment (bit 2) and dataEncipherment (bit 3)	Critical
Authority Key Identifier	8FC8D655EA3600BDB008D9A70FBA88818A4119B5	Non-critical
Subject Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	Non-critical
Certificate Policies	Certificate Policies [1] Certificate Policy: Policy Identifier=0.4.0.2042.1.3 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2] Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.3.1.2.{7, 8} [2,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution Points	http://crl.certsign.ro/certsign-publicca2023rsa.crl	Non-critical
Subject Alternative Name	Other Name: RFC822 Name and Principal Name (UPN) *This extension is optional*	Non-critical

Table 7.4.2 Extensions of the encryption certificates for End-Entity

Certificate extensions for OCSP certificates are described in Table 7.5.

Extension	Value or Value constraint	Extension status
Key Usage	digitalSignature (bit 0)	Critical
Authority Key Identifier	8BC9B01408769D200B559070BEB9992A4EC0684E	Non-critical
Subject Key Identifier	3c767c4a3c2d6c5a82c02d62f92e1789e555f0b6	Non-critical
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	Non-critical
OCSPNoCheck	-	Non-critical

Table 7.5. Extensions of the certificates for OCSP certificates

7.1.3 Algorithm object identifiers

SubjectPublicKeyInfo

The SubjectPublicKeyInfo field indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier, with an explicit NULL parameter.
The AlgorithmIdentifier for RSA keys is byte - for - byte identical with the following hex - encoded bytes: 300d06092a864886f70d0101010500.
For ECDSA, the identifiers and encodings specified in #7.1.3.1.2 from CABF BR will be used.

Signature AlgorithmIdentifier

All objects signed by a certSIGN CA Private Key conform to the CABF BR #7.1.3.2, RSA or ECDSA requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier - derived type in the context of signatures. In the case of certSIGN, the algorithm used is sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

7.1.4 Name forms

See section 3.1 Naming.

7.1.5 Name constraints

See section 3.1 Naming.

7.1.6 Certificate policy object identifier

Certificates policy object identifiers used at certSIGN Public 2023 RSA CA level are described in Table 7.6 and Table 7.7.

Certification Policy Name	Policy identifier
CERTSIGN Public 2023 RSA CA	{CERTSIGN}. {id-policy}(3). {id-cp} (1). {id-Public-CA}(2) . *subpolicy ID=1.3.6.1.4.1.25017.3.1.2. subpolicy ID* See below *subpolicyID* values.

Table 7.6. Policies identifiers and their names

CA Level	Type	Name and OID
CERTSIGN Public 2023 RSA CA 1.3.6.1.4.1.25017.3.1.2	Non-qualified certificate	*Non-qualified certificate for authentication and signing* ▪ with HW Device and key generated by CERTSIGN - .3 ○ with HW Device and key generated and hosted by certSIGN for remote-signature and authentication-3.1 ○ with HW Device and key generated and hosted by certSIGN for remote-signature and authentication that can be used only in the relationships between the Subject and the Subscriber-3.2 ▪ without HW Device and key generated by CERTSIGN -.4 ▪ with HW Device and key generated and hosted by certSIGN for remote-signature and authentication, with pseudonym -.14 *Non-qualified certificate for encryption* ▪ with HW Device and key generated by CERTSIGN -.7 ▪ without HW Device and key generated by CERTSIGN - .8 *Non-qualified certificate for electronic seal* ▪ with HW Device and key generated by CERTSIGN - .11 ○ with HW Device and key generated and hosted by certSIGN for remote-seal -11.1 ▪ without HW Device and key generated by CERTSIGN -.12 *OCSP certificate - .13*

Table 7.7 Certificate policy object identifiers

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

certSIGN issue certificates with a policy qualifier within the Certificate Policies extension. This extension contains a CPS pointer qualifier that points to the CPS.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL profile

certSIGN Public 2023 RSA CA uses full and complete CRL, that is a CRL whose scope includes all Certificates issued by the CA.

nextUpdate field indicates the date by which the next CRL will be issued. For CRLs covering Subscriber Certificates, at most 10 days after the ***thisUpdate***. For other CRLs, at most 12 months after the ***thisUpdate***.

revokedCertificates field is present if the CA has issued a Certificate that has been revoked and the corresponding entry has yet to appear on at least one regularly scheduled CRL beyond the revoked Certificate's validity period. The CA will remove an entry for a corresponding Certificate after it has appeared on at least one regularly scheduled CRL beyond the revoked Certificate's validity period.

CRL profile is described in Table 7.8.

Field name	Value or value constraints	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-18288250
	Common Name (CN) =	CERTSIGN Public 2023 RSA CA
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
ThisUpdate	Date of CRL issuance	
NextUpdate	Date of next expected CRL update	
Revoked Certificates	List of revoked certificates	

Table 7.8 CRL profile for CERTSIGN Public 2023 RSA CA

7.2.1 Version number(s)

All CRLs issued by CERTSIGN are X.509 version 2.

7.2.2 CRL and CRL entry extensions

CRL extensions for CERTSIGN Public 2023 RSA CA are described in Table 7.9.

Extension	Value or Value constraints	Extension status
Authority Key Identifier	8BC9B01408769D200B559070BEB9992A4EC0684E	Non-critical
CRL Number	monotonically increasing sequence number	Non-critical
ExpiredCertsOnCRL	Generalized Time	Non-critical

Table 7.9. Extensions of CERTSIGN Public 2023 RSA CA CRL

serialNumber is byte-for-byte identical to the ***serialNumber*** contained in the revoked Certificate.

revocationDate is the date and time revocation occurred.

The CA updates the revocation date in a CRL entry when it is determined that the private key of the Certificate was compromised prior to the revocation date that is indicated in the CRL entry for that Certificate. Backdating the revocationDate field is an exception to best practice described in RFC 5280 (Section 5.3.2); the revocationDate field support implementations that process the revocationDate field as the date when the Certificate is first considered to be compromised.

Extension	Value or Value constraint	Extension status
serialNumber	serialNumber of the revoked certificate	Non-critical
revocationDate	date of the certificate compromission/revocation	Non-critical
crlEntryExtensions	reason for revocation	Non-critical
CRL Reason	*Revocation reason code*	*Non-critical*

Table 7.10. revokedCertificates Component for certSIGN Public CA

CRL entry extensions (crlEntryExtensions) supported by certSIGN contain the following fields: **ReasonCode**: code of the reason for revocation. This field is non-critical, allowing determination of the certificate revocation reason. The following reasons of certificate revocation are allowed:

1. No reason provided or unspecified (RFC 5280 CRLReason #0)
   - When the reason codes do not apply to the revocation request, the subscriber MUST NOT provide a reason code other than "unspecified".
2. keyCompromise (RFC 5280 CRLReason #1)
   - The certificate subscriber choose the "keyCompromise" revocation reason when they have reason to believe that the private key of their certificate has been compromised, e.g. an unauthorized person has had access to the private key of their certificate.
3. affiliationChanged (RFC 5280 CRLReason #3)
   - The certificate subscriber choose the "affiliationChanged" revocation reason when their Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.
4. superseded (RFC 5280 CRLReason #4)
   - The certificate subscriber choose the "superseded" revocation reason when the Certificate is being replaced because: the Subscriber has requested a new Certificate, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with the requirements or the CA's CPS.
5. cessationOfOperation (RFC 5280 CRLReason #5)
   - The certificate subscriber choose the "cessationOfOperation" revocation reason when the Subscriber no longer have the rights to use the Certificate prior to the expiration of the Certificate.
6. privilegeWithdrawn (RFC 5280 CRLReason #9)[6]

[6] *The privilegeWithdrawn reasonCode does not need to be made available to the certificate subscriber as a revocation reason option, because the use of this reasonCode is determined by the CA operator and not the subscriber.*

- The CRLReason privilegeWithdrawn is intended to be used when there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the certificate subscriber provided misleading information in their certificate request or has not upheld their material obligations under the subscriber agreement or terms of use.

The Subscriber Agreement inform Subscribers about the revocation reason options listed above and provide explanation about when to choose each option. Revocation requests templates, that the CA provides to the Subscriber, allow for these options to be easily specified when the Subscriber requests revocation of their Certificate, with the default value being that no revocation reason is provided (i.e. the default corresponds to the CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL).

7.3 OCSP profile

The protocol of on-line certificate status verification (OCSP) allows certificate status evaluation.

OCSP service is provided by certSIGN on behalf of all affiliated Certification Authorities. OCSP server, which issues certificate status confirmations, employs a special key pair for each Subordinate CA and Root CA, generated exclusively for this purpose.

OCSP server certificate has to contain the extension extKeyUsage, described in RFC 5280.

This extension should be set as non-critical and means that a Certification Authority issuing the certificate to the OCSP server confirms with its signature delegation of the authorization to issue certificate status conformation (of this authority's Subscribers).

As well, OCSP server certificate contains the OCSPNoCheck extension, described by RFC 6960. This extension must be declared non-critical which means that an OCSP client receives a response signed with the private key associated to this certificate can trust the OCSP server certificate status, without being necessary to check its revocation status.

The entity receiving a confirmation issued by the OCSP server must support the standard response format with **id-pkix-ocsp-basic** identifier.

Information about certificate status is included in **certStatus** field of **SingleResponse** structure. This may have one of the following three main values:

- GOOD – indicates the valid status of certificate

- REVOKED – indicates that the certificate was issued and revoked or the certificate was not issued in accordance with the RFC 6960

- UNKNOWN – indicates that there is not enough information to determine the certificate status

When the OCSP answer contains an error code (message), the answer is not digitally signed (RCF 6960).

7.3.1 Version number(s)

OCSP server operating within certSIGN issues certificate status confirmations in accordance with the RFC 6960. The only allowable value of the version number is 0 (it is an equivalent of v1 version).

7.3.2 OCSP extensions

In compliance with RFC 6960, certSIGN OCSP server accepts the following extension:

Nonce – binding a request and a response to prevent reply attacks. **Nonce** is included in **requestExtension** of the **OCSPRequest** and repeated in the field **responseExtension** of the **OCSPResponse**.

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

certSIGN activities supporting the delivery of the services presented by CPS Public 2023 RSA CA are audited at least every 12 months, forming a continuous, unbroken sequence, of audited periods.

The audit verifies the compliance with the present CPS and ETSI 319 401 and ETSI 319 411 technical standards.

certSIGN submits also to periodic audits and supervision in accordance with ETSI TS 119 431-1 and competent supervisory body requirements.

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.

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 certification services provider and the conformity of our certification services towards the criteria from Regulation 910/2014 and its implementing acts we follow the requirements from the ETSI EN 319 403 standard

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 operations and services specified in by CPS Public 2023 RSA CA.

Internal and external assessment/audits are carried out in compliance with the international accepted rules and regulations applied to the Certification Authorities and concern:

- system configuration management
- certSIGN's physical security,

- procedures of Subscriber's identity verification,
- certification services and procedures of service delivery,
- security of software applications and network access,
- security of certSIGN's personnel,
- event journals and procedures for system monitoring,
- data archiving and restoration,
- archiving procedures,
- records concerning the modification of configuration parameters for certSIGN,
- records concerning verifications and analysis carried out for software applications and hardware devices.

For Delegated Third Parties which are not Enterprise RAs, the CA obtains an audit report, that provides an opinion whether the Delegated Third Party's performance complies with the CA's Certification Practice Statement. If the opinion is that the Delegated Third Party does not comply, then the CA will not allow the Delegated Third Party to continue performing delegated functions.

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

Fees for certification and other services are published in the list of fees available at the address http://www.certsign.ro . Prices are set according to the internal price policy.

Services provided by certSIGN are set as follows:

- **Individual certification services** – the price is set for every service in part, for example, for an individual certificate sold or a smaller number of certificates,
- **Certification services packages** – the price is set for packages of services rendered to a single entity,
- **Subscription services** – the price is set for services rendered periodically; the value of the amounts paid depends on the type and number of services accessed and it is used mainly for time stamping and certificate status verification services by means of OCSP protocols,
- **Indirect services –** the price is set for every service rendered to its clients by a certSIGN partner whose activity is based on certSIGN's infrastructure.

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

9.1.1 Certificate issuance and renewal fees

Prices are formed according to the internal price policy.

9.1.2 Certificate access fees

Free service.

9.1.3 Revocation or status information access fees

Prices are formed according to the internal price policy.

9.1.4 Fees for other services

Prices are formed according to the internal price policy.

9.1.5 Refund policy

Payments may be reimbursed according to the applicable contractual conditions.

9.2 Financial Responsibility

9.2.1 Insurance coverage

certSIGN has professional insurance policies in place and will cover damages that may arise from certification services for persons building their ethics on the legal effects of certificates issued by certSIGN Public 2023 RSA CA within the limits set by this CPP, contractual agreements entered into, as applicable.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

certSIGN benefits from insurance covering professional responsibilities, as shown above.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

All information related to the Subject / 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 Subject, a Subscriber, a Partner Entity, and certSIGN are based on trust.

A third party may have access only to public information available in certificates. Other data delivered in applications sent to certSIGN will not be willingly disclosed to a third party under any circumstance (except for legal situations).

A party will be exonerated from the liability of disclosing confidential data if:

a) the information was known to the contracting party before it was received by the other contracting party; or

b) the information was disclosed after obtaining the written consent of the other party;or

c) the party was legally forced to disclose the information.

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 also other entities that perform certification activities are committed to keep the information secret both during and after employment. There are considered private and confidential information:

- Information provided by Subjects/ Subscribers in addition to information that shall be sent to perform the certification services; in those situations, disclosing the information received requires the prior written consent of the information owner or in others conditions according to the law.
- Information supplied by/to Subjects/ Subscribers (for example, the content of contracts concluded with Subjects/ Subscribers or Relying Parties, bank accounts, registration applications, issuing, rekeying, certificate revocation – except for the information included in certificates or from the Repository, in compliance with the present CPS); 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 Subject),
- 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 certification 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 certification services and planned registration rules.

Persons responsible for keeping the confidentiality of information and who obey the rules regarding information management bear the liability according to laws in force.

Disclosure of Certificate Revocation Reason

If a certificate was revoked upon the request of an authorized party, other than the Subject or the Subject, information about the revocation and the related reasons are disclosed to both parties.

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

All information required for proper functioning of certification services are not considered confidential or private. It particularly concerns information included in a certificate by the issuing Certification Authority, in accordance with specifications in Chapter 7. A Subject/ Subscriber that applies for obtaining a certificate is aware of the type of information included in the certificate and agrees with their publishing.

Part of the information provided by or to the Subject/ Subscriber might be made available to other entities only with the written consent of the Subject/ Subscriber and for the stated purpose in the contract concluded with the Subject/ Subscriber.

9.3.3 Responsibility to protect confidential information

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

9.4 Privacy of personal information

In providing trusted services, certSIGN processes the personal data of the Subject / 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 certification services.

9.4.1 Privacy Plan

In the provision of certification services, certSIGN acts as a personal data controller according to paragraph 7 of art. 4 of the Regulation no. 679/2016.

Security measures required by Regulation (EU) No 910/2014, Regulation No 679/2016 and the Romanian National Supervisory Authority in the field of personal data processing are implemented by certSIGN to ensure that:

- Appropriate technical and organizational measures are taken to ensure the security of the data processed, to protect the rights of the Subjects and to comply with the principles laid down in 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.
- the confidentiality and integrity of the registration data is ensured: when exchanged with the subscriber/subject, when exchanged between certSIGN system components as well as when stored.

9.4.2 Information Treated as Private

All Information that leads to identification the Subject is considered to be personal information.

9.4.3 Information not Deemed Private

The content of digital certificates and information accessible through the Depositary is public information.

9.4.4 Responsibility to Protect Private Information

certSIGN and its employees undertake to maintain the confidentiality of personal information during certification services and after certificate 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 and Consent to use Private Information

In the process of issuing a digital certificate Subjects / Beneficiaries are informed about the need to use their personal data for the service and the need for consent. If data Subjects do not agree to certSIGN processing their data, they cannot benefit from certification services.

Subjects / Beneficiaries also have the option of using the personal data for other purposes expressly communicated by certSIGN by contract or otherwise.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

certSIGN is relieved of liability for the disclosure of personal data of the Subjects / Beneficiaries 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 to:
  - auditors in the audits to which certSIGN is subject according to the provisions of Regulation (EU) no. 910/2014 under confidentiality;
  - the courier companies with which certSIGN has a contract, with the agreement of the Subject / Subscriber if he has opted to transmit the certificate to his / her home address or to another communicated address, respecting the same obligations regarding the security of personal data that he / has and certSIGN;
  - an empowered person to whom I outsource certain services;
  - affiliated companies certSIGN
- personal information appearing in certificates or in the Public Authorities (Depositary), with the agreement of the Subject / Subscriber;
- in any other circumstances warranted by prior notification of the Subject / Subscriber.

9.5 Intellectual property rights

All trademarks, patents, brand marks, licenses, 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, patents, brand marks, licenses, 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 CA representations and warranties

certSIGN issues X509 v3-compatible Certificates. certSIGN guarantees that all the requirements set out in the applicable CPS (and indicated in the Certificate in accordance with chapter 7) are complied with. It also undertakes the responsibility to ensure such compliance and provide these services in accordance with the CPS.

The sole guarantee provided by certSIGN is that its procedures are implemented in accordance with the CPS and the verification procedures in place at the time of issuance, and that all Certificates issued with an Object Identifier (OID) have been issued in accordance with the relevant procedures, and the CPS as applicable at the time of issuance.

9.6.2 RA representations and warranties

The RA has the obligation to comply scrupulously with the CPS, and with the certSIGN relevant internal procedures.

9.6.3 Subscriber representations and warranties

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

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

In particular, the Subject is liable towards Relying Parties for any use that is made of his / her QSCD, including the keys or Certificate(s).

9.6.4 Relying Party representations and warranties

Examples of Relying Parties' obligations and responsibilities include (without limitation):

- The successful performance of public key operations as a prerequisite for relying on a certSIGN Certificate
- The validation of a certSIGN Certificate by using the (CRLs) or certificate validation services provided by certSIGN
- The immediate termination of any reliance on a certSIGN Certificate if it has been revoked or when expired.
- Acknowledgement of the provisions of this CPP, guarantees and limits of liability of Certsign SA

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

Unless otherwise expressly provided in the CPS 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 Subject, 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 by certSIGN) certSIGN will be liable for:

- Any loss of profits;
- 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 certificates or digital signatures;
- Any other damages.

certSIGN is not liable to any person (beneficiary, subject, third party, partner entity, etc.) in case the data submitted when issuing certificates are false, inaccurate, incomplete or outdated or false identity documents are presented. certSIGN shall not be liable for damages incurred by the Beneficiary or third parties caused by the use of CERTSIGN issued certificates by the Subject.

In any case the liability of certSIGN in case of a claim for damages shall be limited to the value of the certificates involved in causing a damage.

9.9 Indemnities

certSIGN assumes no financial responsibility for Certificates, CRLs etc. used improperly or for illicit purposes.

9.10 Term and termination

9.10.1 Term

This CPS 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

This CPS 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 CPS will be communicated via the certSIGN web site upon termination. That communication will outline the provisions that may survive termination of this CPS 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 Certificates shall remain valid for the remainder of the validity periods of such Certificates.

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 CPS shall be in writing and shall be sent, except provided explicitly in the CPS to be transmitted in another form, either by

(i) registered mail, return receipt requested, postage prepaid,
(ii) an internationally recognized "overnight" or express courier service,
(iii) hand delivery
(iv) 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 via its Policies and Procedures Management Body (PPMB) for the approval and change of the present CPS. The CPS is reviewed at least once a year.

The only changes that the PPMB may make to these CPS specifications without notification are minor changes that do not affect the assurance level of this CPS, 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 CPS, 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.

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

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

9.12.2 Notification mechanism and period

All changes to the present CPS under consideration by the PPMB shall be disseminated to interested parties before or on publication. The effective date is indicated on the title page of the present CPS.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

All disputes associated with the present CPS will be resolved according to the Romanian laws.

9.14 Governing Law

The Romanian laws shall govern the enforceability, construction, interpretation, and validity of the present CPS (excluding any legal conflict that would cause the enforcement of national or international laws).

9.15 Compliance with applicable law

The present CPS and provision of certSIGN services are compliant to 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.

9.16.1 Entire Agreement

No Stipulation.

9.16.2 Assignment

No Stipulation.

9.16.3 Severability

No Stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No Stipulation.

9.16.5 Force Majeure

CA acts conforming to Romania Laws regarding Force Majeure.

9.17 Other Provisions

No stipulation.

10 Appendix – Specific Server Signing Application Service policy & practice statements

The Server Signing Application Service uses certificates dedicated for the remote signature:

Profile name	certSIGN OID	T&C
PCA ESIGN natural person with SCD and key generated by certSIGN for Remote Signature	1.3.6.1.4.1.25017.3.1.2.3.1	TC1
PCA ESIGN natural person with SCD and key generated by certSIGN for Remote Signature with Notice	1.3.6.1.4.1.25017.3.1.2.3.2	TC1
PCA SEAL with SCD and Key generated by certSIGN for Remote Signature	1.3.6.1.4.1.25017.3.1.2.11.1	TC2
PCA with SCD and key generated by certSIGN for remote signature and authentication with pseudonym	1.3.6.1.4.1.25017.3.1.2.14	TC1

The Terms and Conditions associated above are:

- TC1: certSIGN Public 2023 RSA CA - Terms and conditions for remote signature
- TC2: certSIGN Public 2023 RSA CA - Terms and conditions for seals

All the above certificates are compliant with (include) LSP Policy.
If any changes are made to the LSP ETSI default policy which affects the applicability then the policy identifier will be changed and a new policy will be added.

10.1 Lightweight SSAS Policy (LSP)

certSIGN Lightweight SSAS Policy is tailored to the organizational structure, operating procedures, facilities, and computing environment of certSIGN.

10.1.1 SP name and identification

certSIGN claims conformance to the latest version of **ETSI TS 119 431-1** via the following specific trust service policy OID: **LSP - Lightweight SSAS Policy - 0.4.0.19431.1.1.1**

itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) lightweight (1)

In the framework of the certSIGN LSP policy, the signer associated with the signing key can be:

- a natural person;
- a natural person identified in association with a legal person;
- a legal person (that can be an organization or a unit or a department identified in association with an organization).

The relationship between the signer and the subscriber is established and documented to correspond to the subject–subscriber relationship, in line with ***ETSI EN 319 411-1,*** clause 5.4.2***.***

10.1.2 Signing key generation

certSIGN complies with clause SRG_KM.1.1 of the latest version from EN 419 241-1, specifying the signing keys environment, as a trustworthy HSM system, which is ensured to be EAL 4 or higher, augmented by AVA_VAN.5 in accordance with ISO/IEC 15408. The HSM configuration is based on a certSIGN risk analysis and is taking into account physical and other nontechnical security measures.

certSIGN complies with clause SRG_KM.1.2 of the latest version from EN 419 241-1, specifying the cryptographic algorithms (RSA) and key lengths (3072, 4096), **corresponding to the appropriate level of security, which fulfils the security needs identified during the system design***.*

certSIGN complies with clause SRG_KM.1.3 of latest version from EN 419 241-1, specifying for key protection, that **the private or secret keys are NOT held outside the SCDev***.*

certSIGN complies with clause SRG_KM.1.4 of latest version from EN 419 241-1, specifying that the HSM is **initialised, before generating or containing any signing key, with technical mechanisms conform to HSM manual, that requires two operators in the process***.*

certSIGN complies with clause SRC_SKS.1.1 of the latest version from EN 419 241-1, specifying in the configurations the RSA algorithm parameters, **that can resist during the life time of the signer's certificate, conformant to the cryptographic suites recommendations like ETSI/TS 119 312 and SOG-IS-CRYPTO***.*

certSIGN complies with clause SRC_SKS.1.3 of the latest version from EN 419 241-1, specifying that the **Signer's signing key are NOT generated in advance.**

10.1.3 eID means or identity linking

N/A

10.1.4 Certificate linking

certSIGN complies with clause SRC_SKS.1.2 of latest version from EN 419 241-1, specifying certificate linking – it links signer's signing keys with the appropriate signer's public key certificate.

certSIGN complies with clause SRC_SKS.1.4 of latest version from EN 419 241-1, specifying certificate linking - a signing key will NOT be used before its public key certificate is linked by the QTSP.

certSIGN complies with clause SRC_SKS.1.5 of latest version from EN 419 241-1, specifying links protection – certSIGN protects the integrity of links between signer's signing key and public key certificate.

10.1.5 eID means provision

N/A.

10.1.6 Signing key life-cycle operational requirements.

10.1.6.1 Signature activation

certSIGN complies with clause SRC_SA.1.2 of latest version from EN 419 241-1, specifying authentication - SSA requires each signer to be successfully identified and authenticated before allowing any actions that can impact the sole control of any signing key.

certSIGN complies with clause SRC_SA.1.3 of latest version from EN 419 241-1, specifying protocol security - Protocols in use prevent man-in-the-middle attacks, replay attacks, and more generally any form of attacks where a malicious user can use authentication credentials which do not belong to him/her.

certSIGN complies with clause SRC_SA.1.4 of latest version from EN 419 241-1, specifying access control - Access controls ensure that a signer does not have access to sensitive system objects and any functions which gives the user control over another's signing key.

certSIGN complies with clause SRC_SA.1.5 of EN 419 241-1, specifying signing key control – certSIGN ensures that the DTBS/R provided under control of the signer is only signed by the signing key belonging to this signer.

certSIGN ensures that the public key certificate is valid before using the corresponding signing key.

Signing keys are usable in only those cases for which the signer's consent has been obtained.

certSIGN applies SRC_DSC.1.1 of the latest version from EN 419 241-1, specifying in the specific technical instructions the RSA algorithm parameters for signature creation.

10.1.6.2 Signing key deletion

certSIGN complies with clause SRG_KM.7.1 of latest version from EN 419 241-1 . If the public key certificate is revoked, the corresponding signing key will be destroyed.

certSIGN will destroy a signing key when requested by the signer.

10.1.6.3 Signing key backup and recovery

certSIGN complies with clause SRG_KM.2.1 of latest version from EN 419 241-1, specifying key backup. All private or secret keys (including signer's signing key, Infrastructure and Control Keys) are securely stored.

certSIGN complies with clause SRG_KM.2.2 of latest version from EN 419 241-1 [3], specifying backup protection. Wherever the private/secret key is protected by encryption, only cryptographic algorithms and algorithm parameters of equivalent or higher strength are used.

certSIGN complies with clause SRG_KM.2.3 of latest version from EN 419 241-1 [3], specifying backup controls. certSIGN ensures that backup, storage and restoration of private or secret keys (including signer's signing key, Infrastructure and Control Keys) are only performed by authorized personnel. Master keys used to protect both user and working keys are backed up, stored and reloaded under dual control.

The number of duplicated datasets do not exceed the minimum needed to ensure continuity of the service.

10.1.7 Audit logging procedures

certSIGN complies with clause SRG_AA.1 of latest version from EN 419 241-1, specifying audit data generation. At minimum, certSIGN logs:

— significant TW4S environmental, key management events (generation, usage and destruction) ;
— user signing events (e.g. successful signing with a signer's signing key and DTBS/R request management) ;
— user authentication during SAP;
— signer's SAD management;
— start up and shut down of the audit data generation function;
— changes of the audit parameters.

certSIGN complies with clause SRG_AA.2 of latest version from EN 419 241-1, specifying audit data availability by storing and archiving audit data appended to the existing records.
certSIGN complies with clause SRG_AA.3 of latest version from EN 419 241-1, specifying audit data parameters:
— Date and time of event;
— Type of event;
— Identity of the entity (e.g. user, administrator, process) responsible for the action;
— Success or failure of the audited event

certSIGN complies with clause SRG_AA.7 of latest version from EN 419 241-1, specifying that audit data integrity is preserved and checked periodically.

certSIGN complies with clause SRG_AA.8 of latest version from EN 419 241-1, specifying that for the time accuracy of audited events, a time source suitably synchronized with a standard time source is used.

10.1.8 Records archival

certSIGN retains the audit data records for ten years after any certificate based on these records ceases to be valid, within the constraints of applicable legislation.

10.1.9 Systems and security management

certSIGN complies with clause SRG_M.1 of latest version from EN 419 241-1, managing its security in order to operate a system that provides signature creation- see #5.2 above.

10.1.10 Systems and operations

certSIGN complies with clause SRG_SO.1 of latest version from EN 419 241-1, as certSIGN operation management functions are adequately secure:
— correctly and securely operated;
— deployed in such a way that the risk of systems failure is minimized;
— protected against viruses and malicious software to ensure the integrity of the systems and the information they process.

certSIGN complies with clause SRG_SO.2 of latest version from EN 419 241-1, as certSIGN systems are suitably synchronized with a standard time source. certSIGN ensures that its clock is synchronized with UTC within an accuracy of 1 second or better, using the NTP protocol.

10.1.11 Computer security controls

certSIGN complies with clause SRG_AA.6.1 of latest version from EN 419 241-1, regarding system monitoring – certSIGN systems generate a warning notifying in a timely manner unusual events which can have impact on the ability of the signing server system to meet the security requirements identified in ETSI TS 119 431-1.