Certification Practice Statement
certSIGN ROOT CA G2

Version 2.29

Date: 10 June, 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	The person who made the change
1.0	28 February 2017	First version publishing	Information Security Officer
2.0	15 March 2017	Second version, after interim audit	Information Security Officer
2.1	3 April 2017	Minor update for clarification	Information Security Officer
2.2	5 February 2018	Annual review	Information Security Officer
2.3	7 May 2018	CPS aligned with requirements GDPR	PKI Policies Manager
2.4	18 September 2018	Update for clarification *"Uniqueness of names"* requirements	PKI Policies Manager
2.5	25 September 2018	Remote signature with RQSCD	PKI Policies Manager
2.6	1 November 2018	Update new remote signature non-qualified certificate profiles	PKI Policies Manager
2.7	5 November 2018	Update change headquarters	PKI Policies Manager
2.8	14 January 2019	Annual review	PKI Policies Manager
2.9	9 March 2019	Update with new certificate profiles (Trusted List)	PKI Policies Manager
2.10	1 April 2019	Update with new certificate profiles (dnQualifier)	PKI Policies Manager
2.11	8 April 2019	Minor update for clarification	PKI Policies Manager
2.12	22 July 2019	Update with new certificate profiles (PSD2)	PKI Policies Manager
2.13	31 January 2020	Annual review	PKI Policies Manager
2.14	3 February 2020	Update with new seal certificate profiles	PKI Policies Manager
2.15	15 April 2020	Multiple minor updates to comply with BR 1.6.9 & Mozilla requirements	PKI Policies Manager
2.16	31 July 2020	Add OID with pseudonym	PKI Policies Manager
2.17	30 September 2020	CAB BR 1.7.2 CRL/OCSP	PKI Policies Manager
2.18	7 January 2021	Update CA schema with OIDs	PKI Policies Manager
2.19	29 January 2021	Annual Review	PKI Policies Manager
2.20	31 January 2022	Annual review	PKI Policies Manager
2.21	31 January 2023	Annual review	PKI Policies Manager
2.22	31 July 2023	Updates acc. CABF BR v2.0.0	PKI Policies Manager
2.23	31 January 2024	Annual review	PKI Policies Manager
2.24	15 August 2024	Update OCSP profile & others	PKI Policies Manager
2.25	15 January 2025	Annual review	PKI Policies Manager
2.26	30 April 2025	Minor updates	PKI Policies Manager
2.27	15 January 2026	Annual review	PKI Policies Manager
2.28	31 January 2026	Add Web CA G2	PKI Policies Manager
2.29	10 June 2026	Add cross certs	PKI Policies Manager

This document was created and is the property of:

Owner	Author	Date created
BU Trust Services	Information Security Officer	December 2016

Distribution List

Destination	Date distributed
Public-Internet	February 2017
Public-Internet	March 2017
Public-Internet	April 2017
Public-Internet	February 2018
Public-Internet	May 2018
Public-Internet	September 2018
Public-Internet	November 2018
Public-Internet	November 2018
Public-Internet	January 2019
Public-Internet	March 2019
Public-Internet	April 2019
Public-Internet	July 2019
Public-Internet	January 2020
Public-Internet	February 2020
Public-Internet	April 2020
Public-Internet	July 2020
Public-Internet	September 2020
Public-Internet	January 2021
Public-Internet	January 2022
Public-Internet	January 2023
Public-Internet	July 2023
Public-Internet	January 2024
Public-Internet	August 2024
Public-Internet	January 2025
Public-Internet	April 2025
Public-Internet	January 2026
Public-Internet	June 2026

This document was approved by:

Version	Name	Date
1.0	Policies and Procedures Management Body	February 2017
2.0	Policies and Procedures Management Body	March 2017
2.1	Policies and Procedures Management Body	April 2017
2.2	Policies and Procedures Management Body	February 2018
2.3	Policies and Procedures Management Body	May 2018
2.4	Policies and Procedures Management Body	September 2018
2.5	Policies and Procedures Management Body	September 2018
2.6	Policies and Procedures Management Body	November 2018
2.7	Policies and Procedures Management Body	November 2018
2.8	Policies and Procedures Management Body	January 2019
2.9	Policies and Procedures Management Body	March 2019
2.10	Policies and Procedures Management Body	April 2019
2.11	Policies and Procedures Management Body	April 2019
2.12	Policies and Procedures Management Body	July 2019
2.13	Policies and Procedures Management Body	January 2020
2.14	Policies and Procedures Management Body	February 2020
2.15	Policies and Procedures Management Body	April 2020
2.16	Policies and Procedures Management Body	July 2020
2.17	Policies and Procedures Management Body	September 2020
2.18	Policies and Procedures Management Body	January 2021
2.19	Policies and Procedures Management Body	January 2021
2.20	Policies and Procedures Management Body	January 2022

2.21	Policies and Procedures Management Body	January 2023
2.22	Policies and Procedures Management Body	July 2023
2.23	Policies and Procedures Management Body	January 2024
2.24	Policies and Procedures Management Body	August 2024
2.25	Policies and Procedures Management Body	January 2025
2.26	Policies and Procedures Management Body	April 2025
2.27	Policies and Procedures Management Body	January 2026
2.28	Policies and Procedures Management Body	January 2026
2.29	Policies and Procedures Management Body	June 2026

Content

1 Introduction

The **Certification Practice Statement for certSIGN ROOT CA G2** (hereinafter referred to as **CPS ROOT CA G2 or CPS**) details the certification policy and practices that certSIGN applies for the issuance of digital certificates by the Root CA G2 for subordinate certification authorities.

The structure and content of the CPS ROOT CA G2 are in compliance with RFC 3647 recommendations, and latest versions of ETSI EN 319 411-1 and ETSI EN 319 411-2.

certSIGN complies with Romanian Law no.214/2024 on the use of electronic signatures, time-stamping and the provision of trust services based on them, and is conform with Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

1.1 Overview

certSIGN, Certification Authorities and associated Relying Parties' operation depend on the **CPS ROOT CA G2** for the issuance of digital certificates to subordinate certification authorities. Also, this document describes the general rules for providing certification services such as: Subject's registration, public key certification, key and certificates rekey and certificate revocation.

1.2 Document name and identification

The title of this document is **Certification Practice Statement certSIGN ROOT CA G2,** hereinafter referred to as **CPS ROOT CA G2** 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 ROOT CA G2 regulates the most important relations between entities belonging to certSIGN, advisory teams (including auditors) and customers (users of the services provided):

- Certification Authorities:
  - certSIGN ROOT CA G2
  - certSIGN Web CA
  - certSIGN Web CA G2
  - certSIGN Web CA G4 DV (cross)
  - certSIGN Web CA G4 OV (cross)
  - certSIGN Web CA G4 EV (cross)
- Registration Authority,
- Repository,
- Policies and Procedures Management Body
- Authorities that issue electronic confirmations of non-repudiation,
- Subjects,
- Subscribers,
- Relying Parties,
- Relevant suppliers for certSIGN regarding issuance and management of digital certificates

- Auditors

certSIGN provides certification services for every natural or legal entity accepting the regulations of the present CPS. The purpose of these practices (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.

1.3.1 Certification authorities

certSIGN ROOT CA G2 is the Primary Certification Authority for the certSIGN domain. All other Certification Authorities in this domain are subordinated to certSIGN ROOT CA G2 (Figure 1).

Currently, the following Certification Authorities are subordinated to certSIGN ROOT CA G2:

- certSIGN Web CA identified by the following OID: 1.3.6.1.4.1.25017.3.1.4
- certSIGN Web CA G2 identified by the following OID: 1.3.6.1.4.1.25017.3.1.5
- certSIGN Web CA G4 DV – cross-certificate with OID: 1.3.6.1.4.1.25017.10.1
- certSIGN Web CA G4 OV – cross-certificate with OID: 1.3.6.1.4.1.25017.10.2
- certSIGN Web CA G4 EV – cross-certificate with OID: 1.3.6.1.4.1.25017.10.3

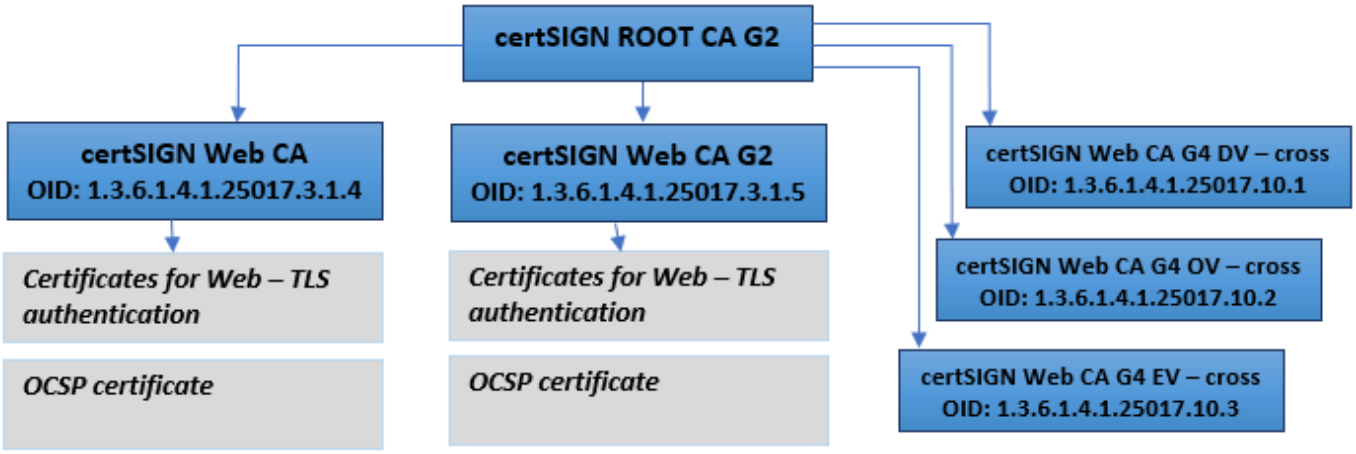

Figure 1: certSIGN ROOT CA G2 certification domain structure

The Primary Certification Authority, **certSIGN ROOT CA G2**, can register and issue certificates only to Certification Authorities and authorities that issue electronic confirmations of non-repudiation that belong to the certSIGN domain. Before beginning the activity, every subordinate Certification Authority shall send a request to the Primary Certification Authority, **certSIGN ROOT CA G2** for registration and public key certificate issuance (see also the procedures described in chapter 6.1 of this document).

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 applicant and the data specified in the request. The Registration Authority may also submit applications to the corresponding Certification Authority in order to cancel a Subject's request and to withdraw his certificate.

The Registration Authority is operated by certSIGN.

1.3.3 Subscribers

The subscriber is certSIGN, as operator of certification authorities subordinated to certSIGN ROOT CA G2.

The Subjects can be either Certification Authorities or authorities that issue electronic confirmations of non-repudiation belonging to the certSIGN domain.

1.3.4 Relying parties

A Relying Party, using certSIGN's services, can be any entity that 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 to decide whether a certificate was used according to the stated purpose.

1.3.5 Other participants

Policies and Procedures Management Body 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 internal documentation.

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

Providers of Qualified Signature Creation Device: the provision of cryptographic modules is ensured by external providers supporting certSIGN activities under a signed contractual agreement.

1.4 Certificate usage

The certificate scope settles 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

certSIGN ROOT CA G2 can register and issue certificates only to Certification Authorities and authorities that issue electronic confirmations of non-repudiation belonging to the certSIGN domain.

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.),
- Provide 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.

1.4.2 Prohibited certificate uses

It is prohibited to use certSIGN certificates for other purposes than those stated and in applications that do not fulfill the minimum conditions specified in Chapter 1.4.1.

1.5 Policy administration

1.5.1 Organization administering the document

Name	S.C. certSIGN S.A. Office: 29 A Tudor Vladimirescu Avenue, AFI Tech Park 1, Bucharest, Romania Trade 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
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.
Subscribers shall adhere to the CPS implemented and published at: https://www.certsign.ro/en/document/certsign-root-ca-g2-certification-practice-statement/
Subscribers who do not accept new, modified terms and regulations of CPS shall make a suitable statement within 15 days of the date of the CPS new version approval. 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

Definitions

Auditor - person who assesses conformity to requirements as specified in given requirements documents

Authentication – electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed

Certificate - public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it

Certificate Revocation List (CRL) – signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

Certification Authority - authority trusted by one or more users to create and assign certificates

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

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

Cross-certification - certificate that is used to establish a trust relationship between two certification authorities

Electronic signature – data in electronic form which is 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 asymmetric keys belonging to a Subject and used only by that Subject. In the case of asymmetric key system, a private key describes 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 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 implementation and operation of certificate-based public key cryptography systems; PKI consists of hardware, software, databases, network resources, security procedures and legal obligation bonded 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 means 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 repealing Directive 1999/93/EC

Root CA - certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s)

Subject (End Entity): entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

Subordinate CA - certification authority whose Certificate is signed by the Root CA, or another Subordinate CA

Subscriber – legal or natural person bound by agreement with a trust service provider to any subscriber obligations

Trust service provider - a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider

Acronyms

CA Certification Authority
CPS Certification Practice Statement
CRL Certificate Revocation List
CARL Certification Authority Revocation List
DN Distinguished Name
NIMB National Institute of Metrology Bucharest
OCSP On-line Certificate Status Protocol
PKI Public Key Infrastructure
PPMB Policies and Procedures Management Body
QSCD Qualified Electronic Signature Creation Device
RSA Rivest, Shamir, Adleman asymmetric cryptographic algorithm
TSP Trust Services Provider
UTC Coordinated Universal Time

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: https://www.certsign.ro/en/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; therefore, 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 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 HTTP requests,
- Secure 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 issuance, a digital certificate is published within the repository.

For all issued certificates, the certificate status information is available through CRLs and the certificate validation services provided by certSIGN 24x7x365.

certSIGN conforms to the latest published version of the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates and to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates, published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

certSIGN hosts 3 web pages, with monthly automatic renewals, that allow Application Software Suppliers to test software with

Subscriber Certificates issued by certSIGN CAs, at https://testssl.certsign.ro

https://testssl-valid-evcp.certsign.ro

https://testssl-revoked-evcp.certsign.ro

https://testssl-expired-evcp.certsign.ro

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 shall make best endeavors to restore 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 annually or following specific events like:

- CPS updates,
- Certificate of the Certification Authorities – after issuing a new certificate;
- Certificate Revocation List is created either every 12 months or when a CA certificate is revoked;
- Fixing of non-conformities found by audits
- Additional information – after every update
- Whenever CA/Browser Forum issue new requests through its BR document that ask for a change of the certificate policy or practice.

2.4 Access controls on repositories

All information published by certSIGN in the Repository at the address https://www.certsign.ro/en/repository/ is available for the public. The repository is publicly and internationally available 24*7*365.
certSIGN implemented logical and physical protection mechanisms against unauthorized 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 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 reestablish 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

The structure and use of names in certificates comply with X.500, RFC5280, and CABF Baseline Requirements (and EV Guidelines, if applicable).

certSIGN does not allow domains in Internationalized Domain Name (IDN) for certificates.

3.1.1 Types of names

Certificates issued by certSIGN are in compliance with the X.509 v3 standard. This means that the certificate issuer 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). Basic names of the Subjects and of the certificate issuers placed in certSIGN's certificates are in compliance with the Distinctive Names – DN – (also known as directory names), created following X.500 and X.520 recommendations. Within DN, it is possible to define attributes of Domain Name Service (DNS). This allows the Subjects to use two types of names: DN and DNS simultaneously. This is a very important option in case of issuing certificates to servers administrated by the Subject.

3.1.2 Need for names to be meaningful

The names used in certificates are chosen so that:

- It is clear that the certificate is a CA certificate,
- The purpose of the CA is clear,
- It includes an unambiguous identification of the legal entity of the Subscriber.

The names CA certificates issued will include the following name information:

OrganizationIdentifier = VATRO-18288250

O= certSIGN SA

C= RO

Many software applications use the commonName field to show a choice of certificates to the end user. To help the end user choose the appropriate certificate, the commonName field may also contain plain wording describing the intended usage of the certificate (i.e. "Qualified CA").

commonName	Meaningful name of the subordinate CA
organizationName	Official registered name of the Subscribing CA as a corporation or organization
countryName	The two-letter ISO 3166-1 country code for the country in which the CA's place of business is located
OrganizationIdentifier	An official unique identifier of the Subscriber as a corporation or organization (as formatted in ETSI EN 319 412-1)

The name of the Subject shall be confirmed by PPMB and approved by Root CA. certSIGN ensures (within its domain) the uniqueness of the DN-s.

3.1.3 Anonymity or pseudonymity of subscribers

certSIGN does not issue anonymous but may issue pseudonymous end-user certificates.

3.1.4 Rules for interpreting various name forms

The interpretation of the fields within the certificates issued by certSIGN is done in accordance with the certificate profiles described in Certificates and CRL-s Profiles presented in Chapter 7 of this document. The creation and interpretation of the DN shall be performed according to the recommendations from Chapter 3.1.2 of this document.

3.1.5 Uniqueness of names

Name uniqueness is ensured through the use SerialNumber of the Subject assigned by the CA. The semantics of the SerialNumber is: First letter of surname + First letter of first name+index number. Index number is the sequential number of the prefix(ca code + initials) in the database.

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.2 Initial identity validation

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.

3.2.2 Authentication of organization identity

certSIGN ROOT CA G2 is a Primary Certification Authority for the certSIGN domain. Any other Certification Authority subordinated to certSIGN ROOT CA G2 is operated by the same legal entity.

Therefore, Authentication of Legal Entity's Identity is not needed.

Certificate Requests are done by trusted roles associated to certSIGN Root CA G2, under the supervision of the Policies and Procedures Management Body (PPMB).

3.2.3 Authentication of individual identity

Not applicable

3.2.4 Non-verified subscriber information

Not applicable.

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

Not applicable.

3.3.2 Identification and authentication for re-key after revocation

Not applicable

3.4 Identification and authentication for revocation request

Revocation Requests are done by trusted roles associated to certSIGN Root CA G2, with the approval of the Policies and Procedures Management Body (PPMB).

4 Certificate life-cycle operational requirements

This chapter describes the basic procedures that apply to all types of certificates issued directly by certSIGN Root CA G2.

4.1 Certificate application

4.1.1 Who can submit a certificate application

Certificate Requests are done by trusted roles associated to certSIGN Root CA G2, with the approval of the Policies and Procedures Management Body (PPMB).

4.1.2 Enrollment process and responsibilities

The enrolment process is handled by trusted roles associated to certSIGN Root CA G2, under the supervision of the Policies and Procedures Management Body (PPMB).
certSIGN provides the infrastructure and resources for the operation of certSIGN Root CA G2. certSIGN also provides supervision, support and auditing for all the processes and services of certSIGN Root CA G2.
certSIGN ensures a segregation of delivery processes for a QSCD and its associated activation data.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

certSIGN ROOT CA G2 is a Primary Certification Authority for the certSIGN domain. Any other Certification Authority subordinated to certSIGN ROOT CA G2 is operated by the same legal entity.

Therefore, identification and authentication functions are done by trusted roles associated to certSIGN Root CA G2, under the supervision of the Policies and Procedures Management Body (PPMB).

4.2.2 Approval or rejection of certificate applications

Approval or Rejection of a certificate application are done by trusted roles associated to certSIGN Root CA G2, under the supervision of the Policies and Procedures Management Body (PPMB).

4.2.3 Time to process certificate applications

The delivery process of certificate requests may take several hours, depending on the approval of the Policies and Procedures Management Body (PPMB) and the implementation of Key Ceremony procedures.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

After receiving, processing and approval of a request, the Certification Authority issues a certificate. After the certificate is issued, certSIGN will publish it in the corresponding repositories. The issued certificates' availability period depends on the certificate's type and the Subject's category and is compliant with the time frames listed in Table 6.3.2.1.
Certificate issuance by the Root CA G2 require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.
certSIGN has implemented its own Linting tool for certificates, which also uses external Linting tools to test the technical compliance of each artifact to be signed before signing it.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The notification on the issuance of a certificate by certSIGN Root CA G2 is implicit and is specified in the internal documentation.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Acceptance of a certificate is done by trusted roles associated to certSIGN Root CA G2, under the supervision of the Policies and Procedures Management Body (PPMB).

4.4.2 Publication of the certificate by the CA

See chapter 2 of the present document.

4.4.3 Notification of certificate issuance by the CA to other entities

Every issued certificate is published in certSIGN's Repository. The certificate publication is equivalent to the notification of other entities (i.e. Relying Parties) about the fact that a certificate was issued for a subordinate CA.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

certSIGN protect the private keys from access by unauthorized personnel or other third parties.
certSIGN uses private keys only in accordance with the usages specified in the key usage extension.
See Sections 1.4.1, 6.1.7 and 7.1.

4.5.2 Relying party public key and certificate usage

certSIGN assumes that all user software will be compliant with X.509, the SSL/TLS protocol, and other applicable standards that enforce the requirements and requirements set forth in this CPS. certSIGN does not warrant 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.

Relying Parties shall use the private keys and certificates:

- In compliance with their stated purpose in the present CPS and in compliance with the certificate content (fields *keyUsage* and *extendedKeyUsage*),
- In compliance with the provisions of the agreement between the Subject/ Subscriber and certSIGN,
- Only after their status and the signature of the issuing Certification Authority are verified.

Relying on an unverifiable digital signature or SSL/TLS session may result in risks that the relying party assumes in whole and which certSIGN does not assume in any way.

4.6 Certificate renewal

certSIGN allows CA certificates renewal only in special conditions, with PPMB approval.

4.7 Certificate re- key

certSIGN allows CA certificates re-key only in special conditions, with PPMB approval.

4.8 Certificate modification

certSIGN allows CA certificates modification only in special conditions, with PPMB approval.

4.9 Certificate revocation and suspension

Certificates issued by certSIGN Root CA G2 can be revoked but they are never suspended. Certificate revocation is irreversible.
CA certificate revocation implies the revocation of all certificates issued by the CA.
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.

4.9.1 Circumstances for revocation

Reasons for Revoking a Subordinate CA Certificate
The Issuing CA, certSIGN ROOT CA G2, will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:
1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise and/or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.
In any other situation where the Beneficiary does not comply with this CPP, the Contractual Agreement, the Terms and Conditions, or other agreements entered into between the parties regarding the services provided by certSIGN CA.
A compromised private key refers to:
(1) unauthorized access to the private key or a strong reason for suspecting 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.
The revocation request is done by trusted roles associated to certSIGN Root CA G2, under the supervision of the Policies and Procedures Management Body (PPMB).

4.9.2 Who can request revocation

Policies and Procedures Management Body (PPMB) is the only entity allowed to request the revocation of a certificate issued by certSIGN Root CA G2.

Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

4.9.3 Procedure for revocation request

The certificate revocation is done by trusted roles associated to certSIGN Root CA G2, under the supervision of the Policies and Procedures Management Body (PPMB).
The information about the revoked certificates is placed in the Certificate Revocation List issued by the corresponding certification authorities.
The CA maintains a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

The CA provides Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA publicly disclosed the instructions through the online website and in section 1.5.2 of this CPS.

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

Within 24 hours after receiving a Certificate Problem Report, certSIGN will investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.
After reviewing the facts and circumstances, certSIGN work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation will not exceed the time frame set forth in Section 4.9.1.1.
certSIGN will consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. 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 they didn't receive the goods they ordered);
5. Relevant legislation.

As an exception, if the revocation request cannot be confirmed within the duration specified in para #4.9.1, certSIGN will not revoke the certificate and the justification will be recorded.

4.9.6 Revocation checking requirements for relying parties

Relying Parties shall use all the resources made available by certSIGN through its repository to verify the status of a Certificate any time before relying on it.

4.9.7 CRL issuance frequency

The Certificate Revocation List (CRL) for certSIGN Root CA G2 is issued at least yearly under the condition that there are no certificate revocations of one of the subordinate CA authorities issued by certSIGN Root CA G2.
In case of certificate revocation of an authority affiliated to certSIGN this certificate is immediately published in the Certificate Revocation List (in max 24 hours).
certSIGN ROOT CA G2 continues issuing CRLs until one of the following is true:
- all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; OR
- the corresponding Subordinate CA Private Key is destroyed.

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

The availability of the on-line revocation/status checking is specified below, in 4.10.2

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

The CA supports an OCSP capability using the GET method for certificates issued in accordance with current CA/B Forum Baseline Requirements.
For the status of certificates issued by certSIGN ROOT CA, the CA updates information provided via an Online Certificate Status Protocol at least

- Every twelve months and
- Within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder does not respond with a "good" status for such certificates.
certSIGN monitors the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.
The OCSP responder provides definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC6962].
A certificate serial number within an OCSP request is one of the following three options:

1. "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or
2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by
    a. the Issuing CA;
    b. a Precertificate Signing Certificate [RFC6962] associated with the Issuing CA;
3. "unused" if neither of the previous conditions are met

Also, 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

Not applicable.

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" and "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.
Revocation entries on a CRL or OCSP Response are not removed until after the Expiry Date of the revoked Certificate.

4.10.2 Service availability
The CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of two seconds or less under normal operating conditions.
The CA maintains an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

The 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.

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

4.11 End of subscription

Not applicable.

4.12 Key escrow and recovery

Not applicable.

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
- ETSI EN 319 411-2, Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 421, Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates
- CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates
- CA/Browser Forum Network and Certificate System Security Requirements

The CA developed, implemented, and maintained a comprehensive security program designed to:

- Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
- Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
- Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
- Comply with all other security requirements applicable to the CA by law.

The Certificate Management Process includes:

- physical security and environmental controls;
- system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
- network security and firewall management, including port restrictions;
- user management, separate trusted-role assignments, education, awareness, and training;
- logical access controls, activity logging.

The CA's security program includes an annual Risk Assessment that:

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes;
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the Risk Assessment, the CA developed, implemented, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.
The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan takes into account then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

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 Officer**: Responsible for entering the information that is necessary for certificate issuance and approval of certification requests;
- **Revocation Officer:** Responsible for operating certificate status changes;
- **Validation Specialist**: Responsible for verifying the information entered for the issuance of certificates and for approving certification applications;
- **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.

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, in relation to certificates, by 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 view point 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:

- basic Public Key Infrastructure knowledge,
- 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 modifications to certSIGN operations are made.

All personnel in Trusted Roles maintain their skill levels consistent with the CA's training and performance programs.

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, 5.3.3 and 5.4.1). 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 or disclosed during an audit, if required. The time accuracy of logs is ensured by a time server that is synchronized with at least two time sources that can be GPS satellites or UTC (NIMB). 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 work station 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,
- Description of the entry,
- 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

Events' records 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 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.

The Risk Assessment is updated at least once a year and:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

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 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.

The business continuity plan includes the elements specified in CAB Forum BR section 5.7.1.

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 are 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

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 as a disaster and the planned processes are in place.

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 plan 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 does 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 withdraw 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 Subscribers 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.

By 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 G2 (in the case of termination of services of the following authorities, certSIGN Web CA, certSIGN Web CA G2) or to the institution that the contract was signed with (in the case of termination of services of certSIGN ROOT CA G2).

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.

certSIGN ROOT CA G2 Certification Authority owns at least one self-signed certificate. The private key corresponding to the public key contained in the self-signed certificate is used exclusively to sign the public keys of the Certification Authorities **certSIGN Web CA** and **certSIGN Web CA G2**, by signing the operational certificates and the Certificate Revocation List necessary for authorities' functioning. A similar purpose is intended for private keys held by each authority: **certSIGN Web CA** and **certSIGN Web CA G2** corresponding to public keys included in the certificates issued by **certSIGN ROOT CA G2** for each authority.

Key pairs owned by each Certification Authority should allow certificate and CRL signing – a public key associated with a private key authenticated with a self-signed certificate (in case of **certSIGN ROOT CA G2**) or certificate (in case of **certSIGN Web CA/ certSIGN Web CA G2**).

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

6.1.1 Key pair generation

certSIGN has a documented procedure for conducting CA key pair generation for all CAs, whether root CAs or subordinate CAs, including CAs that issue certificates to end users. 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 produce a key ceremony report proving that it was 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 all participants, specifically:

- For ROOT CA G2: by the trusted role responsible for the security of certSIGN's key management ceremony (security officer) and a trustworthy person independent of certSIGN's management (Qualified Auditor) as witness that the report correctly records the key management ceremony while carried out, following the Key Ceremony script, and using the implemented controls to ensure the integrity and confidentiality of the Key Pair.

- For subordinate CAs: 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, the CA:

- 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 Web CA**, **certSIGN Web CA G2** 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 and split knowledge:

- 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 and external Qualified Auditor

Key pairs of Certification Authorities operating within certSIGN 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.

Certification Authorities' 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 carried out within a secure cryptographic device which is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 or FIPS PUB 140-2 level 3.

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, subscribers, 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.

6.1.2 Private key delivery to subscriber

Not applicable

6.1.3 Public key delivery to the certificate issuer

Not applicable

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 ROOT CA G2 Certification Authority, certificates are self-signed.

certSIGN Certification Authorities publish their certificates by placing them in the publicly available repository of certSIGN: https://www.certsign.ro/en/resources/chain-of-trust-g2/.

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

The sizes of the keys deployed by Certification Authorities, Registration Authority operators and Subjects are presented in Table 6.1. Only these algorithms and key sizes are permitted for the CAs listed in the table, according to latest version of ETSI TS 119 312:

Key owner	Primary algorithm and key usage		
	RSA for certificate and CRL signing	**RSA for message signing**	**RSA for key exchange**
certSIGN ROOT CA G2	4096 bit	-	-
certSIGN Web CA	4096 bit	-	-
certSIGN Web CA G2	4096 bit	-	-
certSIGN Web CA G4 DV	4096 bit	-	-
certSIGN Web CA G4 OV	4096 bit	-	-
certSIGN Web CA G4 EV	4096 bit	-	-

Table 6.1. Size of keys used

6.1.6 Public keys parameters generation and quality checking

certSIGN has a documented procedure for conducting CA key pair generation for certSIGN Root CA G2. The verification procedures include steps checking that the value of the public exponent is an odd number equal to 3 or more. The modulus must have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

Additionally, the public exponent is in the recommended range, between $2^{16}+1$ and $2^{256}-1$.

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 Subjects' application managing the certificates.

Private Keys corresponding to Root CA G2 Certificates may be used to sign Certificates for:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs;
3. Certificates for OCSP Response verification.

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

- ETSI EN 319 411-2
- CA/B Forum Baseline Requirements

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

The Subject is using hardware key 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.

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 Root CA G2** 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 a 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 disaster 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.

6.2.3 Private Key escrow

Private keys of Certification Authorities are not subjected 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.

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 from 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 ROOT CA G2** 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.

certSIGN protect its Private Key in Hardware Security Modules (HSMs) that have been validated as meeting at least FIPS 140-2 level 3, or FIPS 140-3 level 3, or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats..

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.

6.2.8 Method of activating the private key

All private keys of **certSIGN ROOT CA G2** 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. After the card is inserted into the cryptographic module and after typing the PIN number, the private key remains active until the card is removed from the module.

6.2.9 Method of deactivating private key

Private key deactivation method applies to key deactivation after their usage or upon completion of every session during which the key was used.

Deactivation of a private key is carried out when the card is removed from the module.

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.

6.2.11 Cryptographic Module Rating

See above (6.2.2).

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 ROOT CA G2 certificate (self-signed 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. See section 5.5 of the CPS for archival conditions.

The purpose of public key archive is to create the possibility verify an electronic signature after a certificate is removed from the repository. It is extremely important when providing non-repudiation services, such as timestamp services or certificate status verification services.

Archival of public keys involves archiving certificates containing these keys.

Every authority issuing certificates archives public keys of Subjects to whom certificates were issued. Certification Authority public keys are archived together with private keys, in the manner described in Chapter 6.2.5.

Public key archives should be protected against unauthorized addition, insertion, modification or unauthorized erasure of the key to or from the archive. The protection is enforced with authentication of the archiving entity and authorization of their requests.

The security administrator performs the review of public key archive integrity twice a year. The purpose of this verification is to make sure that there are no gaps in the archive, and certificates stored in the archive had not been modified. Mechanisms verifying the integrity of the archive take into consideration the fact that the archives retention period may be longer than the security means used to create the archives.

Public keys are retained in the digital certificate archive for a period of at least 10 years.

6.3.2 Certificate operational periods and key pair usage periods

Usage period of public keys is defined by the value of the field validity of every public key certificate. It is also the validity period applied to a private key. The maximum period of use of Subject's keys cannot exceed twice the life of a certificate, which is mentioned below.

Standard values of maximum usage period of Certification Authority certificates are listed in Table 6.3.2.1

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

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.

Key owner	Main purpose of key usage
	RSA for certificate and CRL signing
certSIGN ROOT CA G2	25 years
certSIGN Web CA	10 years
certSIGN Web CA G2	7 years
certSIGN Web CA G4 DV	max 7 years
certSIGN Web CA G4 OV	max 7 years
certSIGN Web CA G4 EV	max 7 years

Table 6.3.2.1 Maximum usage period of CA certificates

6.4 Activation data

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.

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.

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 319 411-2 (Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates).

6.6 Life cycle technical 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 Root CA system is in a high security zone with physical separation, and is either offline or, when online, it is physically air-gapped.

According to certSIGN internal Procedure for the management of technical vulnerabilities, the timeframes established for remediating vulnerabilities, are as follows:

- 48 hours – for "Critical" severity
- 96 hours – for "High" severity
- 30 days - for "Medium" severity
- 180 days - for "Low" severity.

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 profiles

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

7.1 Certificate profile

Profile of basic fields for certSIGN ROOT CA G2 certificate in described in Table 7.1.

Field name	Value or value's constraint	
Version	3	
Serial Number	110034b64ec6362d36	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Department (OU)=	certSIGN ROOT CA G2
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Not before (validity period beginning date)	Feb 6 09:27:35 2017 GMT	
Not after (validity period end date)	Feb 6 09:27:35 2042 GMT	
Subject (Distinguished Name)	Department (OU)=	certSIGN ROOT CA G2
	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 ROOT CA G2

Profile of basic fields for certificates issued by certSIGN ROOT CA G2 is described in Table 7.2.

Field name	Value or value's constraint	
Version	Version 3	
Serial Number	Unique value greater than zero (0) for all certificate issued by Certification Authorities within certSIGN. Serial numbers are constructed using a database constrained unique incremental prefix which is concatenated to a 8 bytes random sequence. A hardware cryptographic module is used for generating the random value.	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished	Department (OU)=	certSIGN ROOT CA G2

Field name	Value or value's constraint	
Name)	Organization (O) =	certSIGN SA
	Country (C) =	RO
Not before (validity period beginning date)	Universal Time Coordinated based.	
Not after (validity period end date)	Universal Time Coordinated based.	
Subject (Distinguished Name)	Name (CN) =	Common Name of the CA
	Organization (O) =	Organization name
	Country (C) =	CA country
	OrganizationIdentifier (OID: 2.5.4.97)	Organization Identifier
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 at ROOT CA level

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 ROOT CA G2 are described in Table 7.3.

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=CA, Path length constraint=none	Critical
Key Usage	keyCertSign (bit 5), cRLSign (bit 6)	Critical
Subject Key Identifier	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	Non-critical

Table 7.3. Extensions of certSIGN ROOT CA G2 certificate

Certificates extensions for Subordinate CA are described in Table 7.4

Extension	Value or Value constraint	Extension status
Authority Key Identifier	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	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
Basic Constraints	Subject type=CA, Path length constraint=0	Critical
Key Usage	keyCertSign (bit 5), cRLSign (bit 6)	Critical
CRL Distribution	http://crl.certsign.ro/certsign-rootg2.crl	Non-critical

Extension	Value or Value constraint	Extension status
Points		
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=All issuance policies[1] [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
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://www.certsign.ro/certcrl/certsign-rootg2.crt	Non-critical
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)	Non-critical

Table 7.4. Extensions of the certificates for Subordinate Authorities certificates

Certificate extensions for OCSP certificates are described in Table 7.5.

Extension	Value or Value constraint	Extension status
Authority Key Identifier	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	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
Key Usage	digitalSignature (bit 0)	Critical
Extended 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

The field of signatureAlgorithm contains a cryptographic algorithm identifier used for electronic signature created by a Certification Authority on the certificate. In the case of certSIGN, algorithm used is sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

7.1.4 Name forms

The content of the name fields in certificates meet the requirements in section 3.1 of this document, and the current CAB Forum Baseline Requirements Certificate Policy.

[1] For Cross-CAs the "All issuance policies" is replaced with only one specific policy: DV, OV or EV.

Issuer Name for all possible certification paths is byte-for-byte identical with Subject Name of the Issuer certificate. Subject attributes do not contain only metadata such as '.', '-', and ' ' (i.e. space) to indicate that the value is absent, incomplete, or not applicable.

7.1.5 Name constraints

Not applicable.

7.1.6 Certificate policy object identifier

Certificates policy object identifiers used at Root CA level are described in Table 7.6.

Root CA Level	Type	OID
certSIGN ROOT CA G2	**CA certificates**	**2.5.29.32.0**
	OCSP certificate	**1.3.6.1.4.1.25017.3.1.1.1**

Table 7.6 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

CRL profile is described in Table 7.7.

Field name	Value or value's constraint	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer	Department (OU)=	certSIGN ROOT CA G2
	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 7.7 CRL profile for certSIGN ROOT CA G2

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 ROOT CA G2 are described in Table 7.8.

Extension	Value or Value constraint	Extension status
Authority Key Identifier	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	Non-critical
CRL Number	monotonically increasing sequence number	Non-critical

crlEntryExtensions	ReasonCode for revocation	Non-critical

Table 7.8. Extensions of certSIGN ROOT CA G2 CRL

The extensions from a CRL Entry (**crlEntryExtensions**) accepted by certSIGN, contain:

- **ReasonCode**: the code of the reason for revoking the certificate. This mandatory field is not critical and reveal the reason for revoking the certificate. The following revokation reasons are allowed:
  - **keyCompromise** – key compromise;
  - **cACompromise** – Certification Authority keycompromise;
  - **affiliationChanged** – Subscriber data changes;
  - **superseded** – certificate renewal;
  - **cessationOfOperation** – end using of the certificate;
  - **removeFromCRL** – removal of certificate from CRL list.

The ReasonCode **unspecified** is NOT allowed.

7.3 OCSP profile

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

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

The 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, the OCSP server certificate contains the OCSPNoCheck extension, described by RFC 6960. This extension must be declared non-critical, which means that an OCSP client receiving 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 the certificate status is included in the **certStatus** field of the **SingleResponse** structure. This may have one of the following three main values:

- GOOD – indicates the valid status of a certificate

- REVOKED – indicates that the certificate was issued and revoked or that 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 the 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**.

The field **revocationReason** within **RevokedInfo** of **CertStatus** is presentwith an allowed value as per section 7.2.2 above.

8 Compliance Audit and Other Assessments

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, and CA/B Forum Baseline Requirements, we follow the requirements from the ETSI EN 319 401 standard and ESTI EN 319 411-1 and comply with:

- The requirements from the latest version of "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates"
- The audit requirements from #8 of the latest versions of "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates"
- The requirements from the Romanian Supervisory Body (ADR) as we are licensed as a CA in Romania

8.1 Frequency or circumstances of assessment

certSIGN activities supporting the delivery of the services presented by CPS ROOT 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, the technical standards ETSI 319 401, ETSI 319 411 technical standards and CA/B Forum Baseline/Extended 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 and CA/B Forum Baseline/EV Requirements specifications.

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 this CPS and in accordance with ETSI EN 319 411-1, which includes normative references to ETSI EN 319 401.
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 analyze 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. The audit report will comply with ETSI EN 319 403, chapter 7.4.4, and CABF Baseline Requirements, chapter 8.6.
An authoritative English language version of the publicly available audit information will be provided by the Qualified Auditor and the CA will ensure it is publicly available.
The Audit Report will be available as a PDF, and will be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report will be uppercase letters and will not contain colons, spaces, or line feeds.

8.7 Self-Audits

certSIGN CA monitors the adherence to its Certification Practice Statement and CA/B Forum Baseline Requirements and strictly control its service quality by performing self audits on a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9 Other business and legal matter

9.1 Fees

Certification services fees and the types of services charged 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 set 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 set according to the internal price policy.

9.1.4 Fees for other services

Prices are set 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

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

All information related to the Subjects/Subscribers/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 Beneficiary, 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 fulfill 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/Subscribers 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/Subscribers, 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 / Beneficiary;

- in any other circumstances warranted by prior notification of the Subject/Subscribers.

9.5 Intellectual Property Rights

All trademarks, patents, brand marks, licenses, 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, 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, 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.

The Root CA G2 is responsible for the performance and warranties of the Subordinate CAs, for the Subordinate CA's compliance with the CAB Requirements, and for all liabilities and indemnification obligations of the Subordinate CA, within the limits of current CPS, under the CAB Requirements, as if the Root CA G2 were the Subordinate CA issuing the Certificates.

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 willful 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.

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

The 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, served or sent pursuant to the CPS shall be in writing and shall be sent, except provided explicitly in the CPS, either by

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

9.12 Amendments

9.12.1 Procedure for amendment

certSIGN is responsible via its Policies and Procedures Management Body 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.

The 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 settled according to the Romanian laws.

9.14 Governing law

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

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

No stipulation.

9.17 Other provisions

No stipulation.