Certification Practice Statement
certSIGN ROOT CA G3

Version 1.4

Date: January 15, 2026

Important
Note

This document is the property of certSIGN SA

Address: 29A Tudor Vladimirescu Av.
AFI Tech Park 1, Bucharest 050881, Romania

Telephone: 004-021-31.19.901

Web: www.certsign.ro

Document history

Version	Date effective	Reason	Person who made the change
1.0	30 November 2022	Release of first version	PKI Policy Manager
1.1	31 January 2023	Annual review	PKI Policy Manager
1.2	31 January 2024	Annual review	PKI Policy Manager
1.3	15 January 2025	Annual review	PKI Policy Manager
1.4	15 January 2026	Annual review	PKI Policy Manager

This document was created by and is the property of:

Owner	Author	Date created
certSIGN	PKI Policy Manager	November 2022

Distribution list

Destination	Date distributed
Public-Internet	Noiembrie 2022
Public-Internet	January 2023
Public-Internet	January 2024
Public-Internet	January 2025
Public-Internet	January 2026

This document was approved by:

Version	Name	Date
1.0	Policies and Procedures Management Body (PPMB)	November 2022
1.1	Policies and Procedures Management Body (PPMB)	January 2023
1.2	Policies and Procedures Management Body (PPMB)	January 2024
1.3	Policies and Procedures Management Body (PPMB)	January 2025
1.4	Policies and Procedures Management Body (PPMB)	January 2026

Content

1 Introduction

The Certification Practice Statement of **certSIGN ROOT CA G3** (hereinafter referred to as the **CPS ROOT CA G3 or the CPS**) details the certification policy and practices that certSIGN applies for the issuance of digital certificates by CA ROOT G3 for subordinate certification authorities.
The structure and content of CPS ROOT CA G3 are compliant to RFC 3647, ETSI EN 319 411-1 and ETSI EN 319 411-2 recommendations.

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

1.1 Overview

The operation of certSIGN, of Certification Authorities and of Affiliated Parties rely on the **CPS ROOT CA G3** when issuing digital certificates to subordinate certification authorities. This document also describes the rules for the provision of certification services such as the registration of Subscribers, the certification of public keys, rekeying and certificate revocation.

1.2 Document name and identification

This document is titled the Certification Practice Statement of certSIGN ROOT CA G3, hereinafter referred to as the **CPS ROOT CA G3 or the CPS**.
The electronic document is available in the Repository, at: https://www.certsign.ro/en/document/certsign-root-ca-g3-certification-practice-statement/

1.3 PKI Participants

CPS ROOT CA G3 governs 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 G3
  - CADef CA
  - *certSIGN FOR BNR SIMPLE SSL PRODUCTION CA – on end-of-life*
  - *certSIGN FOR BNR QUALIFIED DS TEST CA – on end-of-life*
  - *certSIGN FOR BNR SIMPLE SSL TEST CA – on end-of-life*
  - *certSIGN FOR BNR QUALIFIED DS PRODUCTION CA – on end-of-life*
- Registration Authority,
- Repository,
- Policies and Procedures Management Body
- Authorities issuing electronic non-repudiation confirmation,
- Subjects,
- Subscribers,
- Relying Parties,
- Relevant suppliers of certSIGN regarding the 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 this CPS (that includes key generation procedures, certificate issuing procedure and information system security) is to ensure the

users of the certSIGN services that the declared levels of credibility related to issued certificates comply with the Certification Authorities' practices.

1.3.1 Certification authorities

certSIGN ROOT CA G3 is a Primary Certification Authority for the certSIGN domain.

Currently, the following Certification Authorities are certSIGN ROOT CA G3 subordinated:

- certSIGN CADef CA identified with the following OID: 1.3.6.1.4.1.25017.6.1
- *certSIGN FOR BNR SIMPLE SSL PRODUCTION CA identified with the following OID: 1.3.6.1.4.1.25017.1.1.2.1.1– on end-of-life: not issuing end-user certificates*
- *certSIGN FOR BNR QUALIFIED DS TEST CA identified with the following OID: 1.3.6.1.4.1.25017.1.1.2.1.2– on end-of-life: not issuing end-user certificates*
- *certSIGN FOR BNR SIMPLE SSL TEST CA identified with the following OID: 1.3.6.1.4.1.25017.1.1.2.1.3– on end-of-life: not issuing end-user certificates*
- *certSIGN FOR BNR QUALIFIED DS PRODUCTION CA identified with the following OID: 1.3.6.1.4.1.25017.1.1.3.1.1– on end-of-life: not issuing end-user certificates*

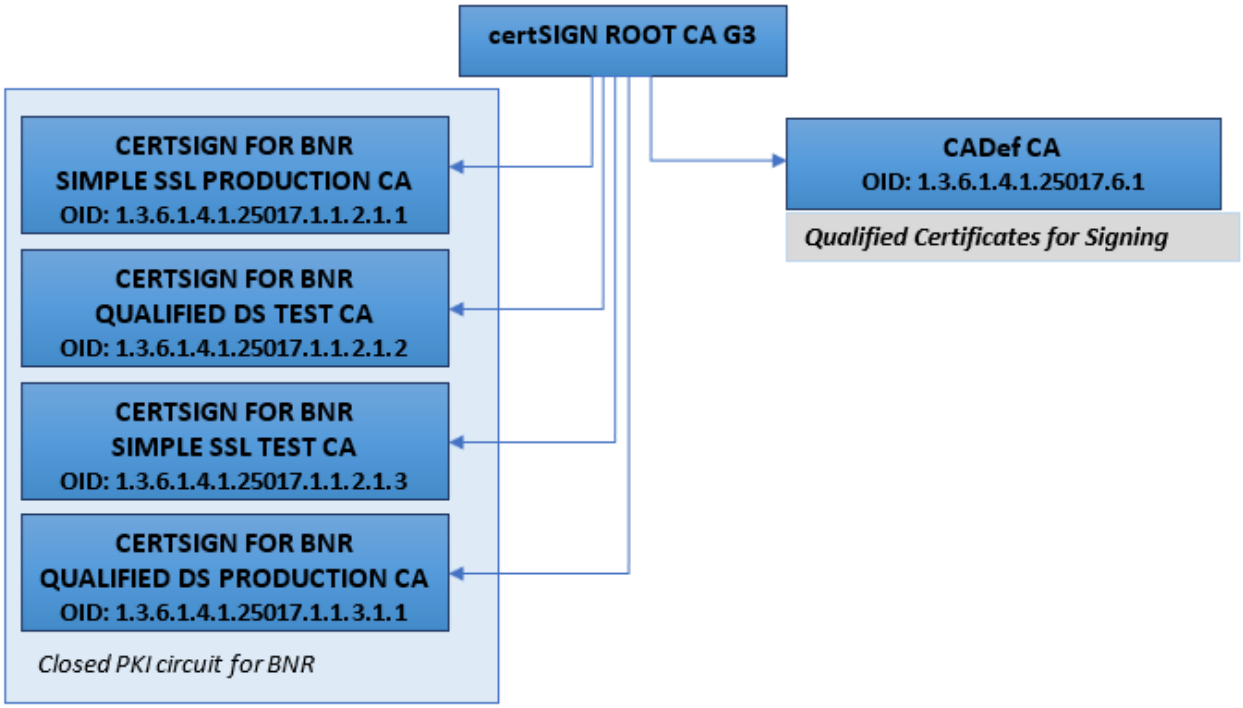

Figure 1: Structure of the certification certSIGN ROOT CA G3 domain

The primary certification authority, **certSIGN ROOT CA G3**, may register and issue certificates only to Certification Authorities and authorities issuing electronic non-repudiation confirmations belonging to the certSIGN domain. Prior to starting off the activity, all subordinate Certification Authorities shall send a request to the Primary Certification Authority**, certSIGN ROOT CA G3** for registration and issuance of the public key. (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 applications for registration and issuance of certificates, rekey or revocation of certificates. Verification of applications is intended to authenticate (based on the documents included in the applications) both the applicant and the data included in the application. The Registration Authority may send requests to the appropriate Certification Authority to cancel an application for registration and to revoke a certificate.

The Registration authority for certSIGN ROOT CA G3 is operated by certSIGN.

1.3.3 Beneficiaries

The Beneficiary is certSIGN, as an operator of the certSIGN ROOT CA G3 subordinate certification authorities.

Subjects may be either Certification Authorities or authorities issuing electronic non-repudiation confirmation of the certSIGN domain.

1.3.4 Relying parties

A Relying Party, using certSIGN services, can be any entity that makes decisions based on the correctness of the connection between the identity of a Subject and his/her public key.

A Relying Entity is responsible for how it verifies the current status of a Subject's certificate. Such a decision must be made whenever a Relying Party wishes to use a certificate to verify an electronic signature, verify the identity of the source or author of a message, or to create a secret communication channel with the Certificate Subject. A Relying Party will use the information in a certificate to decide whether a certificate has been used in accordance with the stated purpose.

1.3.5 Other participants

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

certSIGN service providers: external prviders supporting certSIGN business under a signed contractual agreement.

Qualified Electronic Signature Creation Device Providers (QSCD the external providers supporting certSIGN business under a signed contractual agreement that ensure the supply of physical cryptographic devices utilized by Subjects.

1.4 Certificate usage

The scope of certificates sets the purpose in 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 is 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 factors, 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 G3 may register and issue certificates only to Certification Authorities and Authorities issuing electronic confirmations of repudiation belonging to the certSIGN domain.

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

- Manage properly 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 to 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 (including key usage) of the Certificate, including any applicable limitation as written in the Certificate.

1.4.2 Prohibited certificate uses

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

1.5 Policy Management

1.5.1 Organization managing 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 Sediu social: 107A Oltenitei Street. building C1, ground floor, Sector 4, Bucharest, Romania, PO Box 041303
Telephone	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Table 1.5.1 Organization managing the document

1.5.2 Contact person

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

Table 1.5.2 Contact person

Procedure for reporting compromised certificates

Due to errors, technical or procedural limitations, or other reasons, there may be certificates issued incorrectly by certSIGN (e.g. the certificate issued contains erroneous information about the subject or organization). There may also be cases where a certificate is misused (e.g. for criminal activities). If beneficiaries, entities or other third parties encounter such situations, where they suspect compromise of the private key, or other fraudulent activity, misuse of the certificate or misconduct or any other issues related to certificates issued by certSIGN, they may report these issues to **revokecsgn@certsign.ro**, informing the issuing Certificate Authority of reasonable grounds for revocation of the certificate.

certSIGN CA will start investigating a report of problem certificates within 24 hours of receipt, and will decide whether revocation or other appropriate action is justified by at least the following reasons:

1. Nature of the alleged problem;
2. Number of reports with compromised certificates received on a particular Certificate or Beneficiary.
3. The reporting entity (for example, a complaint by an employee of a law enforcement authority that a website is engaged in illegal activities should have more weight than a complaint by a consumer claiming not to have received the ordered goods); and
4. Relevant legislation.

certSIGN CA maintains a 24x7 capacity to respond internally to a report with high priority certificate issues (Certificate Problem Report), and, where applicable, submit a complaint to law enforcement authorities and/or revoke a certificate subject to such a complaint. Reports of certificate issues shall be sent to: **revokecsgn@certsign.ro**.

1.5.3 Person determining CPS compliance with the policy

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

Table 1.5.3 Person determining CPS compliance with the policy

1.5.4 CPS approval procedures

Policies and Procedures Management Body (PPMB) is in charge of the CPS approval.

The Beneficiaries will adhere to the CPS in place and published at: https://www.certsign.ro/en/document/certsign-root-ca-g3-certification-practice-statement/Beneficiaries who do not accept the new CPS, containing the amended terms and regulations, are obliged to submit, within 15 days from the date on which the new version of the CPS was approved, a statement to this effect. This leads to the termination of the certification service agreement and the revocation of the certificate issued on its basis.

1.6 Definitions and acronyms

Definitions

Auditor – the person certifying compliance with the requirements specified in the relevant documents

Authentication – electronic processes enabling the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form.

Certificate – public key of a user, together with other information that is protected from forgery by encryption with the private key of the certification authority that issued it.

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

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 issuer of the certificate.

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

Cross-certification – certificates issued to establish a relationship of trust between two certification authorities.

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

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

Private key – one of the asymmetric keys belonging to a Subject and which is used only by that Subject. In the case of systems with asymmetric keys, a private key describes the transformation of a signature. In the case of the asymmetric encryption system, a private key describes the transformation that takes place when decrypting. The private key is (1) the key whose purpose is decryption or signature creation for the exclusive use of the owner; (2) that key in a pair of keys that is known only by the owner.

Public key – one of the keys of the asymmetric key pair of a Subject, which may be publicly available. In the case of asymmetric encryption systems, the public key defines the signature verification transformation. In the case of asymmetric encryption, the public key defines the transformation of messages to encryption.

Public Key Infrastructure (PKI) – architecture, techniques, practices and procedures that collectively support the implementation and operation of certificate-based public key cryptography systems; PKI consists of hardware, software, databases, network resources, security procedures and legal obligation joined together, which collaborate to provide and implement certificate services, as well as other services, associated with the infrastructure (e.g. time stamp).

Qualified Electronic Signature Creation Device an electronic signature creation device that meets the requirements set out in Annex II of Regulation (EU) 910/2014.

Regulamentul (UE) nr. 910/2014 – REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and the repealing Directive 1999/93/EC.

Root CA – certification authority that has the highest level within the field of TSP and which is used for the signing of subordinated CAs.

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

Subordinate CA – certification authority whose certificates are signed by root CA, or other subordinate authority.

Beneficiary – natural or legal person, bound by a contract with a trusted service provider

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

Acronyms

CA Certification Authority
CPP 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 CPSs at least annually, even if there are no changes.

2.1 Repository

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

- 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
- Templates for contracts with Subjects and Beneficiaries

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

- • To make every effort to ensure that all certificates published in the Repository belong to the Subjects listed in the certificates and that the Subjects consented to these certificates,
- - Make sure that certificates of Certification Authorities, Registration Authorities belonging to the certSIGN domain as well as Subject certificates are published and archived in a timely manner,
- - Ensure publication and archiving of the Certification Practice Statement, CPS, list of applications and recommended devices,
- - Allow access to certificate status information through the publication of Certificate Revocation Lists (CRLs), via OCSP servers or HTTP queries,
- - Ensure permanent access to information in the Repository for Certification Authorities, Registration Authority, Subjects and Relying Parties,
- - Publish CRLs or other information in a timely manner and in accordance with the deadlines specified in the Certification Policy,
- - Ensure secure and controlled access to information in the Repository.

2.2 Publication of certification information

When issued, a digital certificate is published in the Repository.

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

Avaulability

The combined availability of the document repository and CRL repository is designed to exceed 99.8% of the working hours - defined as 24 hours a day, seven days a week, excluding planned maintenance periods.

Scheduled 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 will use its best endeavours to restore service within 24 hours.

Expired certificates that have been revoked before their expiry are not removed from the certificate revocation lists.

2.3 Time and frequency of publication

nformation published by certSIGN are updated annually or upon the following events:

- CPS updates ;
- Certificate of the Certification Authorities – after issuing a new certificate;
- The list of revoked certificates is created either every 12 months or when a certificate is revoked;
- Addressing non-conformities found following an audit;
- Additional information - after each update

2.4 Access control to the Repository

All information published by certSIGN in the Repository at https://www.certsign.ro/en/repository/ is publicly accessible. The Repository is publicly, and internationally, available 24x7x365.

certSIGN implemented logical and physical safeguards against adding, deleting and modifying information published in the Repository.

Beneficiaries, 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 misuse of repositories, OCSP or CRL download services.

Upon discovery of breaches affecting the integrity of information in the Repository, certSIGN will take appropriate measures to restore the integrity of the information, hold the culprits accountable and notify the affected entities.

3 Identification and authentication

3.1 Naming

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

certSIGN does not allow the use of internationalized domain names in certificates (IDN).

3.1.1 Types of names

Certificates issued by certSIGN follow the X.509 v3 standard. This means that the certificate issuer and the Registration Authority that act on behalf of the issuer approve the Subject's name in compliance with theX.509 standard (with reference to X.500 recommendations). Subject and certificate issuer names in certSIGN certificates are in accordance with the Distinctive Name (DN) name structure (also known as Directory Name structures) created according to X.500 and X.520 recommendations. Within the DN structure, specific Domain Name Service (DNS) attributes can be defined. This allows subjects to use two types of names simultaneously: DN and DNS. This is a very important option when issuing certificates for servers managed by the Subject.

3.1.2 Need for the Names to have a logical meaning

The names used in the certificates shall be chosen in such a way as to:

- Be clear that it is a CA certificate,
- Be clear on the purpose of the CA,
- Include a precise identification of the Beneficiary as a legal entity.

The names of the CA certificates issued shall contain the following information:

OrganizationIdentifier = VATRO-18288250

O= certSIGN SA

C= RO

Many software applications use the commonName field to present a selection of certificates to the end user. To help the end user choose the right certificate, the commonName field may also contain clear words describing the purpose of the certificate (e.g. "CA qualified").

commonName	Intuitive name of a subordinate CA
organizationName	Official registered name of the Beneficiary CA as a corporation or organization
countryName	Two-letter country code according to ISO 3166-1 for the country in which the CA business is located
OrganizationIdentifier	An official unique identifier of the beneficiary as a corporation or organization (as formatted in ETSI EN 319 412-1)

The Subject name will be confirmed by the PPMB and approved by the Root CA. certSIGN ensures (within its domain) the uniqueness of all DNs.

3.1.3 Anonymity or pseudonymity of Subscribers

certSIGN does not issue anonymous certificates but can issue certificates with pseudonyms for end-users with specific OIDs.

3.1.4 Rules for interpreting various name formats

The fields in the certificate issued by certSIGN are interpreted in accordance with the profile of the certificate described in the Certificates and in the CRL profiles presented in Chapter 7 of this document. The creation and interpretation of the DN shall be carried out in accordance with the recommendations of chapter 3.1.2 of this document.

3.1.5 Uniqueness of names

Name uniqueness is ensured by using the SerialNumber of the subject assigned by the CA. The semantics of SerialNumber is: first letter of name + first letter of first name + Index number. The index number is the sequential number of the prefix (as code + initials) in the database.

3.1.6 Recognition, authentication and role of trademarks

Not stipulated.

3.2 Initial validation of identity

3.2.1 Proof of Private Key Ownership

Ownership of the private key, corresponding to the public key for which a certificate is requested to be generated, will be proven by submitting the Certificate Signing Request (CSR), as per RSA PKCS #10, which will include the public key signed by the associated private key.

3.2.2 Authentication of company identity

certSIGN ROOT CA G3 is the Primary Certification Authority for the certSIGN domain. Any other Certification Authority in this domain will be subordinate to the certSIGN ROOT CA G3 and is operated by the same legal entity.

Thus, Legal Entity Authentication is not required.

Requests for certificates are made by certSIGN Root CA G3 associated Trusted Roles under the supervision of the Policy and Procedure Management Body (PPMB).

3.2.3 Authenticating the Identity of Natural Persons

Not applicable.

3.2.4 Unverified beneficiary 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

Chapters 4.7 and 4.8 of this document describe this process.

3.3.2 Identification and authentication for re-key after revocation

The same process as for initial identity validation is used.

3.4 Identification and authentication for revocation requests

certSIGN ROOT CA G3 is the Primary Certification Authority for the certSIGN domain. Any other certification authority in this field will be subordinated to certSIGN ROOT CA G3 and is operated by the same legal entity.

Thus, Requests for Revocation are made through trust roles associated with certSIGN root CA G3, under the supervision of the Policy and Procedures Management Body (CMPB).

4 Operational requirements for the lifecycle of the certificate

This chapter describes the basic procedures that are common to all types of certificates issued directly by certSIGN Root CA G3.

4.1 Scope of certificates

4.1.1 Who may submit an application for a certificate

Revocation requests are performed by certSIGN Root CA G3 associated trusted roles, under the supervision of the Policy and Procedure Management Body (PPMB).

4.1.2 Registration process and responsibilities

The registration process is carried out by certSIGN Root CA G3 associated trust roles under the supervision of the Policy and Procedure Management Body (PPMB).

certSIGN provides the infrastructure and resources to operate the certSIGN Root CA G3. certSIGN also provides oversight, support and auditing for all certSIGN Root CA G3 processes and services.

certSIGN provides segregation of delivery processes for a QSCD and associated activation data.
The OCSP certificate applicant for a certSIGN CA, certSIGN manager, submits the following documents to the Registration Authority:

- OCSP Certificate Request (CSR) signed by the applicant, i.e. certSIGN manager.

- Approval of the issuance of the OCSP certificate by the CIO, CTO, CEO or CISO of certSIGN

4.2 Processing certificate requests

4.2.1 Performing identification and authentication functions

certSIGN ROOT CA G3 is the Prrimary Certification Authority for the certSIGN domain. Any other Certification Authority in this domain will be subordinated to the certSIGN ROOT CA G3 and is operated by the same legal entity.

Thus, authentication and identification functions are performed by certSIGN Root CA G3 associated trust roles, under the supervision of the Policy and Procedure Management Committee (PPMB).

4.2.2 Approval or rejection of certificate requests

Approval or rejection of certificate requests is done by certSIGN Root CA G3 associated trust roles, under the supervision of the Policy and Procedure Management Body (PPMB).

4.2.3 Processing time of certificate requests

Processing time for certificates can take several hours, depending on the implementation of the Key Ceremony procedures.

4.3 Certificate issuing

4.3.1 CA actions during issuance of certificates

After receiving and processing a request, the Certification Authority issues a certificate. After the certificate is issued, certSIGN will publish it in the corresponding repository. The availability period of the issued certificate depends on the type of certificate and the category of the Subject, and is in accordance with the times described in table 6.3.2.1.
Issuance of certificates by the ROOT CA G3 requires that a person authorized by the CA (e.g. CA System Operator, System Officer or PKI Administrator) to deliberately transmit a disposition so that the Root CA executes the certificate signing operation.

4.3.2 Notification of the Subject by the CA regarding the issuance of the Certificate

Notification of certificate issuance by certSIGN ROOT CA G3 for an internal PKI component is default and is specified in the internal documentation.

4.4 Certificate acceptance

4.4.1 Conduct constituting acceptance of the certificate

Acceptance of a certificate is done by associated certSIGN Root CA G3 trusted roles, under the supervision of the Policy and Procedure Management Body (PPMB).

4.4.2 Publication of the certificate by CA

See chapter 2 of this document.

4.4.3 Notification by the CA of other entities about the issuance of the certificate

Each certificate issued is published in the certSIGN repository. Publication of the certificate is equivalent to notification to other entities (e.g. Relying Parties) of the issuance of a certificate to a subordinate CA.

4.5 Key pair and certificate usage

4.5.1 Beneficiary's private key and certificate usage

certSIGN protects the private key from unauthorized access by unauthorized personnel and third parties.
certSIGN uses the private key only in accordance with the uses specified in the key usage extension.
See sections 1.4.1, 6.1.7 and 7.1.

4.5.2 Use of the private key and the certificate by Relying Parties

certSIGN assumes that all software applications are compliant with X.509, SSL/TLS, and other applicable standards that enforce the requirements and requirement sets referenced in this

CPS. certSIGN does not guarantee that the software of any relying party will support or impose such controls and requirements, and all relying parties are advised to identify appropriate technical and legal support.

Rellying Entities will use private keys and certificates:

- In accordance with the stated purpose of this CPP and in accordance with the contents of the certificate (keyUsage and extendedKeyUsage fields),
- In accordance with the provisions of the agreement concluded between the Beneficiary/Subject and certSIGN,
- Only after the status and signature of the issuing Certification Authority have been verified.

Trust in an unverifiable digital signature or an SSL / TLS session may generate risks that the relying party undertakes but which certSIGN will not undertake in any way.

4.6 Certificate renewal

Not applicable.

4.7 Certificate Re-key

Not applicable.

4.8 Certificate modification

Not applicable.

4.9 Certificate revocation and suspension

Certificates issued by certSIGN ROOT CA G3 can be revoked but never suspended. Certificate revocation is an irreversible process.
Revocation of the certificate also includes the withdrawal of the certificate-issuing rights of the holder and the revocation of all certificates issued by the holder.

Revocation shall not affect either the transactions made prior to revocation or the obligations arising from adherence to this CPS.

This chapter sets out the conditions required for a Certification Authority to revoke a certificate.

4.9.1 Circumstances for certificate revocation

4.9.1.1 Reasons for revocation of a ROOT Certificate

certSIGN shall revoke a certificate within 24 hours if one or more of the following occurs:

1. The beneficiary requests in writing the revocation of the certificate by the CA;
2. The Beneficiary notifies the CA that the initial certification request has not been authorized and will not grant the retroactive authorization;
3. CA obtains evidence that the Beneficiary's Private Key corresponding to the Public Key in the certificate has been compromised; or

4. CA obtains evidence that the validation of domain authorization or control for any Fully Qualified Domain Name (FullyQualified Domain Name) or IP address in the certificate cannot be trusted.

certSIGN will revoke a certificate within 5 days in the following situations:

1. Certificate no longer meets the requirements under Sections 6.1.5 and 6.1.6;
2. CA obtains evidence of certificate misuse;
3. CA is informed that the Beneficiary has breached one or more material obligations of the contractual agreement or the Terms and Conditions.;
4. CA is informed of any situation in which the fully qualified Domain Name or IP address in the Certificate is no longer legal (e.g. a court or arbitrator has revoked the Domain Registrar's right to use the Domain Name, a license agreement or relevant services between the Domain Applicant and the Domain Registrar has ceased, or the Domain Registrar has not renewed the Domain Name);
5. CA is informed of material changes to the information in the certificate;
6. CA is informed that the certificate has not been issued in accordance with the requirements of certSIGN CPS;
7. CA determines or is informed of any erroneous information contained in the certificate;
8. The CA's right to issue certificates expires or is revoked or terminated, unless the CA has taken steps to continue to hold the CRL/OCSP Repository;
9. CA is informed of a demonstrated or proven method that exposes the Beneficiary's private key to compromise. Methods have been developed that can easily calculate it based on the Private Key (such as a weak Debian key, see http://wiki.debian.org/SSLkeys), or there is clear evidence that a particular method used to generate the Private Key has been flawed.
10. In other cases, at the decision of the PPMB.

4.9.1.2 Reasons for revocation of a Subordinate CA certificate

The issuing CA, certSIGN ROOT CA G3, will revoke a Subordinate CA's certificate within seven (7) days if one or more of the following reasons occur:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the issuing CA that the original request for the issuance of the certificate has not been authorised, and no retroactive authorisation is granted;
3. The issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the public key in the certificate has been compromised and no longer complies with the requirements of sections 6.1.5 and 6.1.6;
4. The issuing CA obtains evidence that the certificate has been misused;
5. The Issuing CA has discovered that the Certificate has not been issued, or the Subordinate CA has not complied with the requirements of this document or applicable policy or procedure documents;
6. The issuing CA discovers that information appearing in the certificate is incorrect or inadequate;
7. The issuing CA or subordinate CA ceases operations for whatever reason, and does not have arrangements with other CAs to provide certificate revocation support;
8. The right to issue certificates by the issuing CA or subordinate CAs, expires, is revoked or terminated, unless the issuing CA has arrangements to continue the Repository for the OCSP/CRL;
9. Revocation is required by the issuing CA's policy or the CPS.

In any other instance where the Beneficiary fails to comply with this CPS, the Contractual Agreement, the Terms and Conditions, or other agreements between the parties relating to the services provided by CertSIGN Web CA.

A compromised private key means:
(1) unauthorised access to the private key or a reasonable suspicion thereof,
(2) loss of the private key or the appearance of a reason to suspect such loss,
(3) theft of the private key or the appearance of a reason to suspect such theft,
(4) accidental deletion of the private key.
The revocation request is made by certSIGN Root CA G3 associated trusted roles, under the supervision of the PPMB.

4.9.2 Who may request revocation of certificates

The Policy and Procedure Management Body (PPMB) is the only entity that can request the revocation of a certificate issued by certSIGN Root CA G3.

In addition, beneficiaries, partner entities, software vendors and other stakeholders may file certificate problem reports, informing the issuing CA of reasonable causes to revoke the certificate.

4.9.3 Procedure for revoking certificates

Revocation of certificates is done by associated certSIGN Root CA G3 trusted roles, under PPMB supervision.

Prior to revocation of a subordinate CA's certificate, all valid certificates signed by this authority shall be revoked.

Information about revoked certificates is placed in the Certificate Revocation List issued by the appropriate Certificate Authority.

The CA maintains continuous, 24x7, capability to accept and respond to revocation requests and certificate problem reports.
The CA provides beneficiaries, relying parties, software vendors and other stakeholders with clear guidelines for reporting suspected private key compromise, certificate misuse, and other types of fraud, compromise, misuse, improper maintenance, or any other certificate-related issues. The CA presents the instructions on the web site as well as in section 1.5.2 of this document.

4.9.4 Grace period for the revocation request

certSIGN performs the revocation in a time limit of 24 h, to ensure that the time needed to process the revocation request and to publish the revocation notification (updated CRL) is as short as possible.

4.9.5 Timeframe for the CA to process the revocation request

Within 24 hours of the receipt of a Certificate Problem Report, certSIGN will investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report of its findings to both the beneficiary and the entity that submitted the Certificate Problem Report.

After reviewing the facts and circumstances, certSIGN works with the Beneficiary and any entity reporting the Certificate Issue or other revocation-related notice to determine whether

the Certificate will be revoked and, if so, to set a date by which the CA will revoke the Certificate. The period from receipt of the Certificate Problem Report or revocation related notice to the published revocation shall not exceed the time frame specified in section 4.9.1.1. certSIGN shall consider the following:

1. Nature of the alleged problem (scope, context, severity, extent, risk of harm);
2. Consequences of revocation (direct and collateral impacts for beneficiaries and related parties);
3. Number of certificate problem reports received on a particular certificate or beneficiary;
4. The entity making the complaint (e.g., a complaint from a law enforcement official that a website is engaging in illegal activity should carry more weight than a complaint from a consumer who claims they did not 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 Verification of revocation requirements for Relying Parties

Relying Parties shall use all the resources provided by certSIGN through its repository, to verify the certificate status at any time, before relying on.

4.9.7 Frequency of CRLs issuance

The Certificate Revocation List (CRL) of the certSIGN ROOT CA G3 Authority is issued at least once a year, provided that no certificates of one of the authorities subordinated to the certSIGN CA Authority are revoked.

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

4.9.8 Maximum latency for CRLs

The CRL of this CA and of all subordinated issuing CAs is issued in accordance with Chapter 4.9.7 and published without delay.

4.9.9 Availability of online revocation/status check

The availability of online revocation/status verification 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 verified.

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

4.9.10 On-line verification of revocation requirements

The CA supports an OCSP capability using the GET method for certificates issued according to the current version of the CA/B Forum Baseline Requirements.

For the status of certSIGN ROOT CA certificates, the CA updates the information provided via the OCSP protocol at least:

- Every 12 months or

- Within 24 hours after revocation of the certificate of a subordinate CA.

If an OCSP responder receives a status request for a certificate that has not been issued, then the responder does not respond with "good" status for such certificates.

certSIGN monitors the OCSP responder for "unused" serial number requests as part of its security response procedures.
The OCSP responder provides definitive answers for certificates with "reserved" serial numbers, as if there is a corresponding certificate that matches the Precertificate [RFC6962].

In an OCSp request for a certificate serial number, there are the following options:

1. "assigned" whether a certificate with that serial number was issued by the issuing CA using any current or previous key associated with that subject;
2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by:
   a. The issuing CA;
   b. A Precertificate of a Signing Certificate [RFC6962] has been associated with the issuing CA;
3. "unused" if none of the above conditions apply.

See chapter 4.9.6 of this document.

4.9.11 Other forms available for the announcement of revocation

Not applicable.

4.9.12 Special requirements re key compromise

Nu se aplică.

4.9.13 Circumstances for suspension

Not applicable

4.9.14 Who can request the suspension

Not applicable

4.9.15 Procedure for requesting the suspension

Not applicable

4.9.16 Limitations of the suspension period

Not applicable

4.10 Certificate status services

4.10.1 Operational characteristics

certSIGN's certificate status verification services are CRL and OCSP. Access to these services is via the "certsign.ro" website and the LDAP online directory "ldap.certsign.ro". The Certificate Status Check Services provide information on the status of valid certificates. The integrity and authenticity of their status information is protected by the electronic signature of the respective CA.

Revocation entries for a CRL or OCSP response are not deleted until after the expiry date of the revoked certificate.

4.10.2 Service availability

The CA operates and maintains OCSP and CRL capabilities with sufficient resources to provide a response time of two seconds or less under normal operating conditions.

The CA maintains a 24x7 online repository that software applications can use to automatically check the status of unexpired certificates issued by the CA.

The CA maintains an ongoing 24x7 capability to respond inhouse to high priority certificate reports, and where appropriate, forwards this report to law enforcement authorities, and/or revokes the certificate that is the subject of such a request.

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 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, Security policy and requirements for Trusted Service Providers issuing timestamps.

5.1 Physical Controls

certSIGN's network of computer systems, operator terminals and information resources are located in a dedicated area, physically protected against unauthorised access, destruction or disruption. These locations are monitored. Every entry and exit are recorded in the event log (system logs); the stability of the power supply as well as temperature and humidity are also 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 to certSIGN is controlled and monitored by an integrated alarm system. certSIGN has fire prevention systems, intruder detection systems and emergency power supply systems.

certSIGN headquarter is accessible to the public every working day between 09:00 and 18:00. During the rest of the time (including non-working days), access is only allowed to people authorized by the certSIGN management.

Visitors to sites belonging to certSIGN must be permanently accompanied by authorized personnel.

certSIGN premises are divided into:

- Office areas,
- IT areas,
- CA operators' area
- RA and administrator areas,
- Development and testing area.

IT areas are equipped with a monitored security system consisting of motion, intrusion and fire sensors. Access to this area is restricted to authorized personnel only. The monitoring of access rights is done using identity cards and readers, mounted near the access point. Each entry and exit to and from the area are automatically recorded in the event log.

Access to **operators' area** is based on an electronic card and a card reader. As all sensitive information is protected by the use of safes and access to operators' and administrators' terminals requires their prior authorisation, physical security in this area is considered adequate. Access keys may only be picked up by authorized personnel. The area is only accessible to certSIGN staff and authorized persons; the latter are only allowed to be present in the area if they are accompanied by an employee of certSIGN.

Unattended individuals are not allowed in this area. Programmers and developers do not have access to sensitive 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 supply and air conditioning

All areas are air-conditioned. In the server area, the air conditioning units are redundant, and temperature is monitored both automatically (with an alert when a certain level is reached) and manually. From the moment of power failure, emergency power supplies (UPS) allow uninterrupted continuation of activity until the automatic intervention of the building's generator set. The power infrastructure is designed so that after a power outage in the building all activities are available for at least 24 hours with the help of the diesel generator. Each server, network equipment, and all employee computers performing important CA and RA activities are connected to the UPSs. The main components of physical security are also connected to the UPSs and the diesel generator.

5.1.4 Water exposure

The flood risk in the server area is controlled by racks. All equipment is placed in the rack at a minimum distance of 15 cm from the ground. In addition, all server rooms are monitored with humidity sensors.

5.1.5 Fire prevention and protection

certSIGN facility has a fire prevention and protection system in accordance with the standards and regulations in the field. The doors of the server rooms are certified as fireproof, and all accesses are protected with fire-resistant substances.

5.1.6 Media storage

In accordance with the requirements of the information classification policy, media containing back-up data or information are handled and stored securely within the primary facility. Backup media is securely stored in a location separate from the primary location with the same level of security as the primary location. Media containing sensitive data are securely destroyed when no longer needed.

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, HSMs will be factory reset to prevent any possibility of reusing CA private keys and will be 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 the Information Security policy of certSIGN.

5.1.8 Offsite backup

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

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 disaster recovery facility.

5.2 Procedural controls

5.2.1 Trusted roles

All roles involved in the provision of certSIGN certification services are assigned to employees of certSIGN.

All certSIGN 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 being detected.

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 recording, generating certificates, providing devices to subjects and managing certificate revocations. Installs hardware and operating systems; installs and configures network equipment.
- **System operator** – In charge 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**: In charge for verifying the information needed for certificate issuance and approval of certification requests;
- **Revocation officers:** In charge with the operation of certificate status changes;
- **System auditor** – Authorized to access archives and audit logs of the Certification Authority's trustworthy systems. Responsible for performance of internal audit, compliance of a Certification Authority with this CPS; this responsibility extends also to the Registration Authority, operating within certSIGN.

*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 PPMB. The "least privilege" principle is applied when configuring access privileges to trust roles.

5.2.2 Number of people 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.

Each 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 viewpoint of roles fulfilled. Segregation of duties and the principle of least privilege are applicable. Sensitivity of the position based on duties determines the level of access, background screening and employee training.

Procedures are established and implemented for all fiduciary and administrative roles that impact service delivery.

5.3 Personnel control

certSIGN makes sure that the person performing his / her job responsibilities, arising from the assigned role in a Certification Authority or a Registration Authority:

- Has graduated at least the high school,
- Has understood and signed a contract describing his role and responsibilities within the system,
- Has received an advanced traineeship in accordance with the obligations and tasks associated with his/her position,
- Has been trained in the protection of personal data and confidential or private information,
- Has signed a contract containing clauses regarding the protection of the sensitive information of certSIGN and of the confidential and private data of the Beneficiaries,
- Fails to perform tasks that may give rise to conflicts of interest between the Certification Authority and the Registration Authority acting on its behalf.

Security roles and responsibilities, as specified in certSIGN 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 makes sure that all employees acting to provide certification services are screened prior to employment for the identity, trust, qualifications, expertise, experience and authorisation required and, where appropriate, to perform trusted roles and perform the position specific to the position held. Senior management has expertise and experience in PKI technology and sufficient experience in information security management and risk management to perform their senior management functions.

5.3.2 Background check procedures

certSIGN ensures the performance of relevant controls to potential personnel by means of status reports issued by a competent authority, third party declarations or signed declarations.

5.3.3 Staff training requirements

Personnel performing roles and tasks arising from the employment in certSIGN must complete the following trainings on:

- basic knowledge of Public Key Infrastructure (PKI),
- CPS requirements,
- Procedures and security controls used by the Certification Authority and the Registration Authority
- Responsibilities arising from the roles and tasks performed in the system,

Upon completion of the training, participants sign a document confirming their familiarity with the Certification Practice Statement, the Certification Policy and accept the restrictions and obligations imposed.

5.3.4 Frequency and requirements of traineeships

The training described in Chapter 5.3.3 must be repeated or supplemented whenever significant changes occur in the operation of certSIGN or the Registration Authority.

All staff with trusted roles maintain their skills consistent with the training and performance programs of the CA.

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

certSIGN will act against those responsible of policies or procedures violations, unauthorized actions, unauthorized use of authority and unauthorized use of systems. This may include among others revocation of privileges, disciplinary actions, sanctions regulated by the Romanian labour laws, civil or criminal proceedings.

5.3.7 Requirements for independent contractors

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). In addition, the personnel employed on a contract basis, while working in the certSIGN premises, must be permanently accompanied by a certSIGN employee, except for those who have received approval from the security administrator and who can access classified information internally or in accordance with the legal norms in force.

5.3.8 Documentation provided to the personnel

certSIGN staff has access to the following documents:

- CPS,
- List of responsibilities and obligations associated with the role held 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 certification services is distributed during the initial training, annual trainings and whenever otherwise appropriate.

5.4 Audit logging procedures

For the efficient management of the systems and applications used by certSIGN in its activity as a certification service provider, but also to allow the auditing of the actions of employees and customers, all information regarding important events generated by the systems and applications are logged. This information, collectively known as logs, must be kept in such a way that it can be accessed by Relying Parties, auditors and state authorities whenever they need it, in order to provide evidence of the proper functioning of the services for the purposes of legal proceedings or to detect attempts to compromise the security of certSIGN. Logged events are archived and stored in a secondary facility.

Whenever possible, logs are created automatically. If logs cannot be created automatically, paper event logs will be used. Each log, electronic or on paper shall be kept and disclosed when an audit is conducted, if necessary. Time accuracy of logs is ensured by a time server that is synchronized with at least two-time sources that can be GPS or UTC satellites (NIMB).

5.4.1 Logged events

Each critical activity in terms of certSIGN security is logged in event logs and is archived. Archives are stored on storage media that cannot be easily overwritten or destroyed (unless they are transferred to a long-term storage medium) during the time frame in which they are required to be kept. certSIGN event logs contain logs of all activities generated by software components within the system. These logs are divided into three distinct categories:

- **System logs** – contain information about customer's requests and server responses (or vice versa) at the level of the network protocol (for example http, https); hard data being recorded are: the IP address of the station or server, the executed operations (for example: search, edit, write, etc.) and their results (for example, the successful entry of a record in the database),
- **Errors** – contain information about errors at network protocol level and at the software modules level;
- **Audit logs** – contain information specific to the certification services, for example: application for registration and certification, application for rekey, acceptance of the certificate, issuance of the certificate and CRL etc.

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

Every automatic or manual log contains the following information:

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

All events related to the life cycle of the CA keys are recorded, including:

- Generating, backing up, storing, recovering, archiving and destroying keys;
- Lifecycle management events for cryptographic devices.

All events related to the life cycle of certificates are recorded:

- Requests for certificates, renewals, re-key and revocation;
- All checks stipulated in this CPS;
- Date, time, phone numbers used, people spoken to, and results of phone checks;
- Acceptance or rejection of certificate requests;
- Certificate issuing;
- Generating inputs for CRL and OCSP.

All events about the life cycle of keys managed by the CA, including any subject keys generated by the CA are logged.

All requests and reports referring to revocation, as well as the resulting action are logged.

All events related to registration requests, including requests for the certificate re-key are logged.

All registration information, including the following, is recorded:

- The type of document(s) submitted by the applicant upon registration;
- Registration 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 agreement signed by the Subject/Subscriber;
- Any specific option within the agreement (i.e., consent to the certificate publication)
- Identity of the entity accepting the application;
- Method employed to validate identification documents,

In addition, certSIGN keeps internal logs of all security and relevant operational events throughout the entire infrastructure, whichever the technical item, yet not limited to:

- Security policy amendments;
- System startup and shutdown;
- Outages;
- System crashes and hardware failures;
- Firewall and router activities;
- PKI system access attempts;
- Physical access of personnel and other people to sensitive parts of any secured site or area;
- Back-up and restore;
- Report of disaster recovery tests;
- Audit inspections;
- Upgrades and changes to systems, software and infrastructure;
- Security intrusions and attempts at intrusion.

Access to logs is exclusively allowed for the security officer and administrators of Certification Authorities and auditors.

Confidentiality of Subject Information is maintained.

5.4.2 Frequency of processing event logs

Audit logs are processed continuously and/or as a result of an alarm or abnormal event. Audit logs are archived and backups are made continuously.

5.4.3 Retention period of audit logs

Event logs are stored in files on the system disk until they reach the maximum allowed capacity. During this time they are available online, at the request of each authorized person or process. Once the allotted space is exceeded, the logs are kept in archives and can only be accessed offline from a given workstation.

Archived logs are kept for at least 10 years.

5.4.4 Protection of event logs

Log files are properly protected by an access control mechanism. A system of adequate protection against alteration and deletion of audit logs is implemented so that no one can alter or delete audit records except for transfer to a long-term storage medium for archiving purposes. Only the security officer, administrators or an auditor may review an event log. Access to the event log shall be configured so that:

- Only the above entities have the right to read the log records,
- The central log platform automatically archives or deletes files (after archiving) containing recorded events,
- It is possible to detect any integrity violations; this ensures that records contain no gaps or falsifications,
- No entity has the right to modify the content of a log.

In addition, log protection procedures are implemented in such a way that, even after log archiving, it is impossible to delete records, or to delete the log before the log retention period expires.

5.4.5 Backup Procedure for Audit Logs

certSIGN security policies require that the event log be periodically backed up. These backup copies are kept in the auxiliary facilities of certSIGN. Backups of log files and audit paths are saved in accordance with internal procedures.

5.4.6 Audit Data Collection System (internal vs external)

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

- Collect
- Store
- Analyse
- Correlate
- Archive
- Generate long-term backups

5.4.7 Notification of the generating source

Not applicable.

5.4.8 Vulnerability assessments

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

In order to ensure that all of its assets, activities and services are secure, certSIGN has implemented, maintains and continuously improves an ISO 27001:2013 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. Assess the likelihood and potential for damage from these threats, taking into account the sensitivity of Certificate Data and Certificate Management Processes; and
3. Verifies that the CA's policies, procedures, IT systems, technology and other arrangements are sufficient to counter such threats.

5.5 Log archiving

It is necessary that all data and files relating to the recording of information related to system security, requests sent by Subjects/Beneficiaries, information about Subjects/Beneficiaries, certificates issued and CRLs, keys used by the Certification and Registration Authorities, and all correspondence between certSIGN and Subjects/Beneficiaries be archived.

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. The archive of revoked certificates contains information about the certificate, the reason for revocation, at the time when the certificate was placed in CRL. The archive is used to settle any disputes, regarding old documents, electronically signed by a Subject.

Backup copies are created and retained outside certSIGN location.

5.5.1 Types of archived data

The following data are included in a trustworthy archive:

- All certificates for a period of at least 10 years after their expiration
- Archived logs are kept for at least 10 years.
- Logs for issuing and revoking certificates for a period of at least 10 years from the date of issue / revocation
- CRLs are retained for at least 10 years from publication
- • The following, for at least 10 years after the expiration of all certificates based on these records:
    - 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 Archive retention timeframe

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

5.5.3 Archive protection

certSIGN provides:

- Implementation of controls for preventing the loss of archived data
- Confidentiality of archived data and maintaining integrity during its retention period.

Archives are accessible only to authorized personnel.

5.5.4 Archive back-up procedures

Backup of archived data is done in accordance with the internal policies and procedures on back up.

5.5.5 Requirements for timestamping of logs

certSIGN warrants that the exact archiving time of all events, records and documents mentioned above is logged. This is achieved by synchronizing all systems with the time servers. Time accuracy is provided by a time server that is synchronized with at least two time sources that can be GPS or UTC satellites (NIMB).

5.5.6 Archive collection system (internal or external)

Archive collection systems of certSIGN are internal.

5.5.7 Procedures to obtain and verify archived information

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

The Beneficiary/Subject may receive access to records and other information relating to the Subject of the Certificate.

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 life, certSIGN ceases to use the expiring CA Private Key to sign Certificates (at least three years before the expiration) and uses the old Private Key only to sign CRLs. A new pair of CA signing keys is ordered and all certificates issued subsequently and CRLs are signed with the new private signing key. Both old and new key pairs can be active simultaneously. This key exchange process helps minimize any negative effects of the expiration of the CA certificate. The new CA certificate is provided to customers and Partner Entities by the methods of transmission specified in point 6.1.4.

5.7 Compromise and disaster recovery

This chapter describes the procedures used by certSIGN in abnormal situations (including natural disasters) to restore services to the guaranteed level. These procedures are executed in accordance with the 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 in a coordinated manner to incidents

and to limit the impact of security breaches. Employees are assigned trusted roles to track alerts of potential critical security events and to ensure that relevant incidents are reported in accordance with the procedure. In the case of critical failures, the same procedure shall be used.

The procedure for managing security incidents also specifies how the notification of the appropriate parties is made in accordance with the regulatory rules applicable to any security breach or loss of integrity that has a significant impact on the trust service provided and the personal data retained by it 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.

If the security breach or loss of integrity may adversely affect a natural or legal person to whom the certification service has been provided, we will also notify the natural or legal person immediately.

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

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

certSIGN has an Incident Response Plan and a Disaster Recovery Plan, that include the Crisis Management Plan, as well as documented business continuity and disaster recovery procedures designed to reasonably notify and protect software vendors, beneficiaries and relying parties in the event of a disaster, security compromise or business failure. certSIGN makes business continuity and security plans available to auditors upon request. All procedures are annually tested, reviewed and updated.

5.7.2 Procedures upon compromise of computing resources, software and/or data

certSIGN 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, user applications and execution of malicious software, for example viruses, worms, Trojan horses,
- Loss of network services, important for certSIGN business. Its main site power failure and damages to the network connections.
- Corruption of part of the Intranet used by certSIGN to provide services – this can lead to customer obstruction and (unintentional) denial of services.

To prevent or limit the results of the above threats:

- The Security Policy of certSIGN includes a Business continuity and Disaster Recovery Plan,
- If there is an event that blocks the operation of certSIGN, in maximum 48 hours, the auxiliary facility will be activated, which can substitute all the important functions of a Certification Authority until the restoration of the primary facility. The distance

between the primary facility and the secondary location is large enough for the potential disaster affecting the primary facility not to affect the secondary location.

- Installation of new versions of software applications in production can only be done after their intensive testing in a test environment, in accordance with the procedures described. Any changes to the system require the approval of the Security Administrator of certSIGN.
- certSIGN systems use applications for data backup based on which the system can be restored and audited at any time. Backups include all security relevant data.

All systems of which the IT infrastructure is composed for the provision of certification and timestamp services are continuously monitored and all security events are recorded and analysed. Abnormal system activities indicating a potential security breach, including intrusion into network systems, are detected and reported as alarms to enable certSIGN to detect, record and react in a timely manner to any unauthorized and/or unusual attempt to access its resources.

The sensitivity of any information collected or analysed is taken into account, protecting it against unauthorized access.

In order to detect any discontinuity in the monitoring operations, the start and stop of the logging functions is also monitored.

The availability of all important components of the ICT infrastructure used for the provision of certification services as well as the availability of critical services are also monitored.

certSIGN address any previously unaddressed critical vulnerability within 48 hours of its discovery. If this is cost-effective, given the impact, a plan to reduce vulnerability will be created and implemented or the decision that vulnerability does not require remediation will be documented.

5.7.3 Procedures upon compromise of an entity's private key

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 compromise of the private keys of a Certification Authority (affiliated to certSIGN) or if there is a suspicion that they have been compromised, the following measures must also be taken:

- Notification of compromise of all Subjects / Subscribers and other entities with which certSIGN has agreements or other forms of established relationships, among which Affiliated Entities and other Trust Service Providers. In addition, this information will be made available to other Affiliated Entities via the media system and by electronic mail.
- Notification of the general public through several channels, including a message on the certSIGN 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 disaste

certSIGN has established in a Business Continuity (BCP) and Disaster Recovery Plan (DRP) 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 system data required to resume CA operations are saved and stored in a remote and safe place to enable certification and time stamping services to resume their activities in a timely manner in the event of an incident / disaster.

Backups of essential information and software are performed on a regular basis. Adequate back-up facilities shall be provided to ensure that all essential information and software can be retrieved following a disaster or media failure. Back-up activities are regularly tested to ensure they meet the requirements of business continuity plans.

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

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

Following a disaster, where possible, steps will be taken to avoid a repeat of a disaster.

5.8 Termination of CA or RA activities

certSIGN has an up-to-date termination to minimize disruptions to Subjects/ Subscribers and Relying Parties which might arise from a decision of a Certification Authority to cease operation. The plan includes the obligation 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 with the transfer of responsibility

Before a Certification Authority ceases its activity, it will:

- Inform (at least 30 days in advance) about the decision to terminate the services the following: all Subjects/Subscribers holding active certificates (not expired and not revoked) issued by this authority and other entities with which CertSIGN has agreements or other forms of collaboration, including 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 trusted party to maintain all information necessary to provide evidence of the operation of the certification and timestamp services for a reasonable period of time, unless it can be demonstrated that certSIGN does not hold any such information; the information refers to registration information, to the revocation status of the unexpired certificates that were issued and to the archives of the event log for the respective period of time, as mentioned to the Subjects /Beneficiary and the Relying Party;

- Destroy or withdraw from use the CA's private keys, including backups, in a manner that makes it impossible to retrieve the private keys;
- If possible, certain arrangements will be made to transfer the provision of certification services to existing customers to another certification service provider.

certSIGN keep or transfer to a trusted party its obligations so as to ensure the availability of its public key for a reasonable period of time.

If certSIGN ceases its activity, without transferring some or all of its activities, it shall revoke the affected certificates after one month from the notification of the Subscribers and / or Subjects and shall initiate the procedure for terminating the contracts concluded with the partners and/or suppliers involved.

certSIGN has an arrangement to cover the costs of meeting these minimum requirements if it goes bankrupt or if for any other reason cannot cover these costs on its own, to the extent possible, within the limits of applicable bankruptcy law.

Issuance of certificates by the successor of the ceasing Certification Authority

In order to ensure the continuity of the services of issuing the certificates for the Subjects, the Certification Authority that ceases its activity may sign a contract with another Certification Authority that provides similar services, in order to issue certificates to replace the certificates remaining in use, issued by the Certification Authority that ends its activity.

By issuing a certificate to replace the old one, the successor of the Certification Authority ceasing its activity takes over the rights and obligations of this authority regarding the management of the certificates that remain in use.

The archive of the ceasing Certification Authority must be handed over to the successor Certification Authority (in case of termination of certSIGN ROOT CA G3).

5.1 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 related 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 CAs, and other PKI Participants, and other critical security parameters.

Key management procedures refer to the safe storage and use by the owner of his keys. Particular attention is paid to the generation and protection of the certSIGN private key, which influences the safe operation of the entire public key certification system.

certSIGN **ROOT CA G3 Certification Authority** holds at least one self-signed certificate. The private key corresponding to the public key contained in the self-signed certificate shall be used exclusively for the purpose of signing the public keys of **certSIGN CADef CA Certification Authorities**, by signing the operational certificates and the Certificate Revocation List required for the operation of those authorities. The private keys held by the following authorities operating in a PKI closed circuit have a similar role: **certSIGN FOR BNR SIMPLE SSL PRODUCTION CA, certSIGN FOR BNR QUALIFIED DS TEST CA, certSIGN FOR BNR SIMPLE SSL TEST CA, certSIGN FOR BNR QUALIFIED DS PRODUCTION CA** corresponding to the public keys included in the certificates issued by **certSIGN ROOT CA G3** for each authority.

The key pairs held by each Certification Authority must allow the signing of certificates and CRLs - - a public key associated with a private key authenticated with a self-signed certificate (for **certSIGN ROOT CA G3**) or a certificate (for **certSIGN CADef CA,** respectively in the case of the authorities in the closed circuit of the BNR).

An electronic signature is created using the RSA algorithm in combination with the SHA-2 hash algorithm.

6.1.1 Key pair generation

certSIGN has a documented procedure (key ceremony) for generating CA keys for all certificate authorities, whether root CAs or subordinate CAs, including CAs that issue certificates to users. This procedure indicates the following:

- The roles attending the ceremony (internal and external to the company);
- Function to be performed by every role and in which phase;
- Responsibilities during and after the ceremony;
- Requirements of evidence to be collected during the ceremony.

After the key ceremony, certSIGN will produce a key ceremony report which will prove that the key ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. This report will be signed:

- For ROOT CA G3: the trusted role responsible for certSIGN's key management ceremony security (security officer) and a trusted person independent of certSIGN

management (auditor) as a witness attesting that the report includes accurate key management ceremony data.
- For subordinated CAs: By the trusted role responsible for the security of the certSIGN key management ceremony (e.g. security officer), as witness that the report correctly records the key management ceremony as it was performed.

In all cases, CA:

- Generates CA keys within cryptographic modules that meet applicable technical and business requirements as described in the CPS;
- Records its CA key generation activities; and
- Maintains effective controls to provide reasonable assurance that the private key has been generated and protected in accordance with the procedures described in the CPS and, where applicable, the Key Ceremony Script.

certSIGN CADef CA keys**,** of the authorities in the closed circuit of the BNR as well as the keys of other subordinate authorities and the subsequent certification of the public keys are carried out in a secure physical environment by staff in trusted roles under at least dual control:

- At least three employees in trusted roles,
- Security officer,
- At least one representative of the Policy and Procedure Management Body (PPMB),
- A Key Ceremonial Coordinator,
- At least one independent or external auditor,

Certification Authority key pairs operating within certSIGN are generated on designated workstations, authenticated and connected to security hardware modules, compliant with FIPS 140-2 Level 3 or ISO/IEC 15408 EAL 4 requirements. They are kept permanently encrypted on these devices.

The process for generating CA key pairs is similar to the accepted procedure for generating keys in certSIGN as described above. The actions performed during key pair generation are recorded, dated and signed by each person present during generation. The records are kept for the needs of common system audits and reviews.

Registration Authority operators only hold keys to authenticate all their actions. These keys are generated by the operator (in the presence of the security officer) via authentication software provided by a Certification Authority and on a QSCD device.

Key pair generation is done on a secure cryptographic device that conforms 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 key length of 4096 bits.

Prior to the expiry of its CA certificate, which is used for signing Subjects' keys, the CA will generate a new certificate for signing Subjects' key pairs and will apply all necessary measures to avoid disrupting the operations of any entity relying on the CA certificate. The new CA certificate will also be generated and distributed in accordance with this CPS. These operations must be performed at an appropriate time interval between the expiry date of the certificate and the last signed certificate in order to allow all parties dealing with certSIGN (subjects, beneficiaries, relying parties, CAs higher in the CA hierarchy, etc.) to be aware of this key change and to implement the necessary operations to avoid creating inconveniences and

failures. This does not apply if we cease our operations before the expiry date of our own signing certificate.

6.1.2 Delivering the private key to the Beneficiary

Not applicable.

6.1.3 Delivering the public key to the certificate issuer

Not applicable.

6.1.4 Delivering the public key of the Certification Authority to Relying Parties

The (public) CA signature verification keys are made available to Relying Parties in a way that ensures the integrity of the CA public key and authenticates its origin.

Public Keys of a Certification Authority issuing Certificates to Subjects are distributed exclusively in the form of certificates conforming to ITU T X.509 v.3 recommendations. In case of certSIGN ROOT CA G3, the certificates are self-signed.

certSIGN certification Authorities publish their certificates in the repository publicly available at: https://www.certsign.ro/en/repository/Certificates of certSIGN Certification Authorities are delivered to relying parties along with the software (operation systems, web browsers, e-mail clients etc.), which enables the use of certSIGN services.

Certificate repository requires access control after adding, deleting certificates or modifying related information.

6.1.5 Key size

The key sizes used by Web CA, Registration Authority operators and Subjects are shown in Table 6.1.

Key owner	Main usage of the key		
	RSA for certificates and CRL signing	**RSA for message signing**	**RSA for key changeover**
certSIGN ROOT CA G3	4096 bit	-	-
certSIGN CADef CA	4096 bit	-	-
certSIGN FOR BNR SIMPLE SSL PRODUCTION CA	4096 bit	-	-
certSIGN FOR BNR QUALIFIED DS TEST CA	4096 bit	-	-
certSIGN FOR BNR SIMPLE SSL TEST CA	4096 bit	-	-
certSIGN FOR BNR QUALIFIED DS PRODUCTION CA	4096 bit	-	-

Table 6.1. Size of used keys

6.1.6 Public Key Generation Parameters and Quality Check

certSIGN has a documented procedure for performing key pair generation for CAs. The verification procedures include steps to verify that the value of the public exponent is an odd

number equal to 3 or above. The module must have the following characteristics: an odd number, not the exponent of a prime number, and not have factors less than 752.

În plus, exponentul public este în intervalul recomandat, între $2^{16}+1$ și $2^{256}-1$.

6.1.7 Purposes for which the keys may be used (according to the scope of the X.509 v3 keys)

The purposes for which keys can be used are described in the KeyUsage field (see Chapter 7.1.1.2) of the standard X.509 v3 certificate extensions. This field must be checked by the Beneficiary's application doing the certificate management.

Private keys corresponding to ROOT CA G3 certificates can be used to sign:

1. Self-signed certificates representing the Root CA itself;
2. Certificates for subordinate CAs;
3. Certificates for verification of OCSP responses.

The use of bits in the KeyUsage field must respect the following rules:

a) **digitalSignature**: certificates for the electronic signature verification,

b) **nonRepudiation**: certificates for the provision of the non-repudiation service by natural persons, as well as for purposes other than those described in points f) and g). The Non-repudiation bit can only be set in a public key certificate with which it is intended to verify electronic signatures and should not be combined with those described in points c) - e) and related to ensuring confidentiality,

c) **keyEncipherment**: used to encrypt keys of symmetric algorithms, providing data privacy,

d) **dataEncipherment**: used to encrypt Subject data other than those described in paragraphs c) and e),

e) **keyAgreement**: used for key exchange protocols,

f) **keyCertSign**: the public key is used for the verification of the electronic signature in certificates issued by entities providing certification services,

g) **cRLSign**: the public key is used for the verification of electronic signatures on the lists of revoked and suspended certificates issued by entities providing certification services,

h) **encipherOnly**: can only be used with the keyAgreement bit to indicate the purpose of encrypting data within key exchange protocols,

i) **decipherOnly**: can only be used with the keyAgreement bit to indicate the purpose of decrypting data within key exchange protocols.

6.2 Private Key protection and Cryptographic Module Controls

Each Subject, operator of the Certification Authority and Certification Authority generates and stores his/her private key using a trusted system that prevents loss, disclosure, modification or unauthorized access to the private key. If a Certification Authority generates a pair of keys at the authorized request of the Subject/Benefciary, it must deliver it safely to the Subject and require the Subject to protect his/her private key.

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

The hardware and software mechanisms that protect the CA's private keys are adequately documented. HSMs are prepared, distributed and managed in accordance 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 premises of certSIGN.

HSMs shall not leave the secure premises of the CA. If HSMs require maintenance or repairs which cannot be carried out in the secured enclosure of the AC (under the dual control of more than one trusted employee), they are transported safely to their manufacturer.

Between use sessions, HSMs are kept securely within the CA's secure premise.

The CA's private keys remain under the multiple control of n of m employees. CA Custodians have the function to activate and deactivate the CA's private keys. The keys of the CAs are then active for defined periods of time.

CA private signing keys stored on secure cryptographic device are destroyed after device withdrawal.

6.2.1 Cryptographic module standards and controls

The subject uses hardware key protection that meets at least FIPS 140-2 level 3 or Common Criteria EAL 4. CA key pair generation will be performed in a secure cryptographic device that is a trusted system that meets at least FIPS 140-2 level 3 or Common Criteria EAL 4.

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

Multi-person control of a private key applies to private keys of **certSIGN ROOT CA G3 CA** used for signing certificates and CRLs.

Dual access control is achieved by distributing secrets to authorized operators. Secrets are stored on cryptographic cards or tokens, protected by a PIN code and transferred through an authenticated manner to their holders.

The common secrecy transfer procedure must include: the key generation and distribution process, the acceptance of the related secrecy and the responsibilities resulting from its retention.

Accepting the shared secret by its holders

Each holder of shared secrets, before receiving his share of the secret, must personally witness the sharing of the secret, verify the correctness of the secret created and its distribution. Each part of the shared secret must be transferred to its holder on a cryptographic card protected by a PIN code, chosen by the holder and known only to him. The receipt of the shared secret and its creation shall be confirmed by a handwritten signature on a form, a copy of which shall be kept in the archives of the Certification Authority and by the holder of the secret.

Protecting of the shared secret

The keepers of the shared secret must protect their part against disclosure. The holder declares that:

- Will not disclose, copy or share the secret shared with anyone and not use his part of the secret in an unauthorized manner,
- Will not disclose (directly or indirectly) that it is the holder of the secret.

Availability and deletion (transfer) of the shared secret

The holder of the shared secret must allow access to his part of the secret to authorised legal persons (by means of an appropriate form signed by the holder prior to the offer of his part of the secret) only after authorization of the transmission of the secret. This situation should be properly recorded in the security logs.

In the event of natural disasters, the holder of the secret shall report to the certSIGN emergency recovery site as directed by the issuer of the shared secret. The shared secret must be delivered personally by the holder to the emergency recovery facility, in a way that allows it to be used for certSIGN business recovery to its normal state.

Responsibilities of the shared secret holder

The holder of the shared secret must also carry out his duties and obligations as required by this Certification Practice Statement, deliberately and responsibly in every possible situation. A holder of a shared secret must notify the issuer of the secret in case of theft, loss, unauthorized disclosure or compromise of the secret's security immediately after the incident. A Shared Secret Holder is not responsible for the failure to perform his duties/obligations due to reasons that are impossible to control by him, but is responsible for the inopportune disclosure of the secret or for neglecting the obligations to notify the secret issuer about the inopportune disclosure or violation of the secret's security as a result of the owner's mistakes, negligence or irresponsibility.

6.2.3 Private key escrow

Private keys of Certification Authorities are not placed in escrow.

6.2.4 Private key back-up

Certification Authorities operating within certSIGN create a backup of their private key. The backups are used in case of implementation of standard, or emergency (e.g. after disaster) key recovery procedures. When found outside the secure cryptographic device, the CA's private keys are protected in a way that provides the same level of protection provided by the secure cryptographic device. Copies of private keys are protected by shared secrets.

certSIGN does not retain copies of the private keys pertaining to the operators of the Certification Authority.

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

The copies of the CA’s signing private keys are subject to the same (or higher) level of security controls as the keys in use.

6.2.5 Private key archival

Private keys of Certification Authorities that are used for electronic signature creation are not archived – are destroyed right after the completion of the cryptographic operation requiring these keys or at the expiration/revocation of the certificate associated to the public key.

6.2.6 Transfer of the private key into or from a cryptographic module

The operation of inserting the private key in a cryptographic module is performed in the following cases:

- When creating backup copies of private keys stored in a cryptographic module, it may be necessary occasionally (e.g. in case of compromise or failure of the module) to insert a key pair in a different security module,
- It is necessary for the entity to transfer a private key from the operational module used for standard operations to another module; the situation may arise when the module breaks down or needs to be destroyed.

Inserting a private key in a security module is a critical operation and therefore during the execution of the operation, measures and procedures must be implemented to prevent the disclosure, modification or falsification of the private key.

Inserting a private key in a security hardware module of the **certSIGN ROOT CA G3 Certification Authority** requires restoration of the key on the cards in the presence of an appropriate number of shared secret holders protecting the module containing the private keys. Since each Certification Authority can hold an encrypted copy of its private key, keys can also be transferred between modules.

6.2.7 Storage of private keys 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 the premises of certSIGN.

certSIGN protect their private keys in hardware security modules (HSMs) that have been validated to at least FIPS 140 level 3.

Access control is enabled to ensure that keys are not accessible outside the dedicated secure cryptographic devices on which the CA signing keys and any copies thereof are stored.

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

Between usage sessions, HSMs are kept safe in the secure CA premises.

The private keys of the CA remain under the multiple control of n out of m employees. CA custodians are in charge of activating and deactivating CA private keys. CA keys are then active for defined periods of time.

Operators use qualified electronic signature generating devices (tokens/cards). Keys are always generated on the devices and never leave them. Secure devices are protected during transport from supplier to certSIGN, during storage and distribution.

6.2.8 Private key activating method

All **certSIGN ROOT CA G3** private keys private keys are inserted in a module after their generation, imported in an encrypted form from another module or restored from a shared secret. Activation of private keys is always proceeded by the operator's authentication.

Authentication is based on a cryptographic card held by the operator After inserting the card into the cryptographic module and using the PIN code, the private key remains in the active state until the card is removed from the module.

6.2.9 Private key deactivation method

Private key deactivation methods refer to the deactivation of the key after its use or following the end of a session during which the key was used.

Deactivation of a private key is performed when the card is taken out of the module.

6.2.10 Private key destruction method

At the end of their lifespan, CA private keys are destroyed by trusted roles within the CA, in the presence of more than one representative of the Policy and Procedures Management Body, to ensure that these private keys can never be recovered or used again.

The CA private key can be destroyed by deleting all HSM Cards (Operator and Administrator). Furthermore, the HSMs allow device factory reset 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 factory reset 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. PPMB authorizes the CA private key destruction and assigns the personnel for the task.

Each destruction of a private key is recorded in the event log.

6.2.11 Cryptographic module rating

See above (6.2.2).

6.3 Other Key Pair Management Aspects

certSIGN will use properly the CA's private signature keys and will not use them after the end of their life cycle.

The CA signing key(s) used for generating certificates and/or issuing revocation status information will not be used for any other purpose.

Certificate signing keys are only used in physically secure premises.

The use of the CA private key must be compatible with the hash algorithm, signature algorithm and signature key length used for certificate generation in accordance with current practice (the selected key length and algorithm for the CA signing key are RSA 4096 bits in accordance with the Requirements in ETSI TS 119 312 for CA signing purposes).

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

The attributes of the ROOT CA G3 certificate (self-signed certificate) shall be compatible with the defined use of keys as specified in ITU-T Recommendation X.

6.3.1 Public key archival

certSIGN archives its own public CA keys. See section 5.5 of the CPS for archiving conditions.

The purpose of archiving public keys is to create the possibility of verifying the electronic signature after the removal of a certificate from the repository. This is very important when providing non-repudiation services, such as a timestamp service or a certificate status verification service.

Archiving public keys involves archiving the certificates containing these keys.

Each issuing authority shall archive the public keys of the Subjects to whom certificates have been issued. The Certificate Authority's public keys are archived together with the private keys in the manner described in Chapter 6.2.5. Certificates may also be archived locally by the Subjects, in particular when required by the application used (e.g. electronic mail systems).

Public key archives must be protected in such a way as to prevent unauthorised addition, insertion, modification or deletion of keys from the archive. Protection is achieved by authenticating the entity doing the archiving and authorising its requests.

The Security Administrator checks the integrity of public key records twice a year. The purpose of this check is to ensure that there are no gaps in the archives and that the certificates in the archives have not been modified. The mechanisms for verifying the integrity of the archives consider that the retention period may be longer than the security mechanisms used to create the archives.

Public keys are kept in digital certificate archives for at least 10 years.

6.3.2 Operational timeframes of certificates and private key usage period

The period of use of public keys is defined by the validity field value of each public key certificate. There is also a private key validity period. The maximum period of use of Subject keys cannot exceed 2 times the lifetime of a certificate, which is specified below.

The standard values for the maximum period of use of Certification Authority certificates are described in Table 6.3.2.1 and of Subject certificates are described in Table 6.3.2.2.

The period of use of certificates and the corresponding private keys may be shorter if a certificate is revoked.

In general, the start date of the validity period of the certificate corresponds to the date of its issue. It is not allowed to set this date in the past or in the future.

Holder of the key	Main purpose of key usage
	RSA for signing certificates and CRLS
certSIGN ROOT CA G3	25 years
certSIGN CADef CA	10 years
certSIGN FOR BNR SIMPLE SSL PRODUCTION CA	10 years
certSIGN FOR BNR QUALIFIED DS TEST CA	10 years
certSIGN FOR BNR SIMPLE SSL TEST CA	10 years
certSIGN FOR BNR QUALIFIED DS PRODUCTION CA	10 years

Table 6.3.2.1 Maximum period of use of CA certificates

6.4 Activation data

6.4.1 Generating and Installing Activation Data

Activation data are used in two main situations:

- As an element of an authentication procedure based on one or more factors (the so-called authentication phrase, e.g. password, PIN code, etc.),
- As part of a shared secret.

Operators and administrators of Registration Authorities and Certification Authorities, as well as other persons performing the roles described in Chapter 5.2, must use strong passwords (tokens/cards) to authenticate to their roles. Their private keys that are generated on qualified electronic signature devices or smartcard-HSM by certSIGN are associated with the user's activation data (PIN) being personalized and securely distributed. certSIGN ensures that the activation data of RA and CA operators and administrators is managed and protected by such participants, through applicable internal procedures made available to such participants.

Shared secrets used to protect the Certificate Authority's private key are generated in accordance with the requirements outlined in Chapter 6.2 and stored on cryptographic cards. The cards are protected by a PIN code. Shared Secrets become activation data after their activation, e.g. by correctly entering the PIN code protecting the card. certSIGN ensures that key activation data and CA private key activation operations are generated, managed, stored and archived as described in the relevant subsection of sections 6.1 and 6.2. Installation and retrieval of CA key pairs in a secure cryptographic device requires simultaneous control of at least two employees in trusted roles.

6.4.2 Protecting the activation data

Protection of activation data includes methods of controlling activation data to prevent disclosure. The methods of controlling activation data depend on the nature of the activation data: whether it is an authentication phrase, or whether this control is based on the private key or on the sharing of activation information in shared secrets.

The activation data used to activate the private key must be protected by cryptographic controls and physical access control. The activation data must be stored (not written) by the authenticated entity. If the activation data is written, its level of protection should be the same as that of data protected by the use of a cryptographic card. Several unsuccessful attempts to access the cryptographic module should result in its blocking. Stored activation data must not be kept together with the cryptographic card.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

The tasks of Registration Authorities and Certification Authorities operating within certSIGN are performed by means of trusted hardware devices and software applications.

6.5.1 Specific technical requirements for computer security

Security measures that protect computer systems are applied at the operating system, application and physical levels.

Computers are configured with the following security mechanisms:

- Mandatory authentication at operating system and app level,
- Discretionary access control,
- The possibility to conduct a security audit,
- The computer is accessible only to authorized personnel, with trusted roles in certSIGN,
- Separation of tasks, according to the role within the system,
- Identification and authentication of roles and personnel performing these roles,
- Prevent an object from being reused by another process after it has been released by an authorized process,
- Cryptographic protection of information exchanges and database protection,
- Archiving the history of the operations performed on a computer and the data necessary for the audit,
- A secure path that allows the identification and authentication of roles and personnel performing these roles,
- Key restoration methods (only for security hardware modules), applications and operating system,
- Means of monitoring and alerting in case of unauthorized access to computing resources.

The media used within the certSIGN systems are safely handled to protect the media against damage, theft, unauthorized access and obsolescence.

Procedures for managing environments are in place to protect against obsolescence and deterioration of media during the period of time it is mandatory to keep records.

Sensitive data shall be protected against disclosure by reused storage objects (e.g. deleted files) and shall be accessible to unauthorised users. For this purpose, special software must be used, with secure deletion algorithms for storage media, HSMs reset, secure cryptographic devices (tokens/ cards) must be formatted before reuse / or physically destroyed at the end of their life cycle.

For all accounts capable of directly producing the issuance of certificates, multi-factor authentication is implemented.

6.5.2 Assessing computer security

The certSIGN IT system meets the requirements described in the ETSI standards: 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).

6.6 Lifecycle specific security controls

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

6.6.1 System development specific controls

A security requirements analysis is performed at the design and requirements definition stage of any systems development project undertaken by certSIGN or on behalf of certSIGN, to ensure that security is built into the information systems.

Before being used in production in certSIGN, each application is installed so as to allow the control of the current version and to prevent the unauthorized installation of programs or the falsification of existing ones.

Similar rules apply when replacing hardware, such as:

- the physical devices are provided in such a way that each route to its place of installation can be traced and assessed,
- the delivery of a physical device for replacement is carried out in a manner similar to the delivery of the original device; the replacement is carried out by qualified and trusted personnel.

6.6.2 Security management specific controls

The purpose of the security management specific controls is to supervise the functionality of certSIGN systems, thus ensuring that they operate correctly and in accordance with the configuration accepted and implemented.

Controls applied to certSIGN systems allow continuous verification of the integrity of applications, version and authentication and verification of the origin of hardware devices.

6.6.3 Lifecycle security controls

Change control policies and procedures are applied to releases, changes and emergency fixes of any operational software, as well as configuration changes that apply to security policy of certSIGN.

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 Systems/Internal Support Systems are checked at least weekly to determine any changes that would violate the CA's security policies.

certSIGN implements internal security procedures to ensure that:

- security patches are applied within a reasonable time after they become available;
- security patches do not apply if they bring additional vulnerabilities or instabilities that outweigh the benefits of their application;
- the reasons why no security patch is applied are documented

certSIGN implements an internal capacity management procedure that ensures that for ITC infrastructure dedicated to certification services, capacity requests are monitored and projections of future capacity requirements are made to ensure that adequate processing power and storage is 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 taking into account the functional, logical and physical (including location) relationship between the systems and trusted services. certSIGN applies the same security controls to all co-located systems 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) 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 trustworthy 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 based on firewall and traffic filtering on the routers and Proxy services that protect certSIGN 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.

Network security protection supports only messages sent using HTTP, HTTPS, NTP, POP3 and SMTP protocols. The events (logs) are recorded in the system logs and allow the supervision of the correctness of the use of the services provided by certSIGN.

certSIGN maintains and protects all CA systems at least in a safe area and has in place a security procedure that protects systems and communications between systems in safe areas and those in high security areas.

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

certSIGN provides access to safe and high-security areas exclusively to trusted roles. The Root CA system is in a highly secured area and is in an offline state.

6.8 Timestamping

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

7 Certificate, CRL and OCSP profile

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

7.1 Certificate profile

The profile of basic fields for the certSIGN ROOT CA G3 certificate is described in Table 7.1.

Field name	Value or value constraints	
Version	3	
Serial Number	11504611F4CD06231E	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Department (OU)=	certSIGN ROOT CA G3
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Not before (start date of validity period)	11:01:04 21 Sep 2017	
Not after (end date of validity period)	11:01:04 22 Sep 2042	
Subject (Distinguished Name)	Department (OU)=	certSIGN ROOT CA G3
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Info about the Subject Public Key	4096 bits RSA key	
Info about the Subject Public Key	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	

Table 7.1. Profile of the basic fields for certSIGN ROOT CA G3

Profile of basic fields for certificates issued by certSIGN ROOT CA G3 is described in Table 7.2.

Field name	Value or value constraints sau restricțiile valorii	
Versione	Version 3	
Serial Number	Single value greater than zero (0) for all certificates issued by certSIGN Certification Authorities. The series is constructed using a unique icremental prefix constrained in the database that is concatenated with an 8-byte random sequence. A hardware cryptographic module is used to generate the random value	
Signature algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished	Department (OU)=	certSIGN ROOT CA G3

Field name	Value or value constraints sau restricțiile valorii	
Name)	Organization (O) =	certSIGN SA
	Country (C) =	RO
Not before (start date of validity period)	Universal Time Coordinated based.	
Not before (start date of validity period)	Universl Time Coordinated based.	
Subject (Distinguished Name) **Info about the Subject Public Key**	Name (CN) =	Common Name of the CA
	Organization (O) =	Organization name
	Country (C) =	CA country
	OrganizationIdentifier (OID: 2.5.4.97)	Organization Identifier
Signature	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and public key value); RSA key size is shown in chapter 6.1.5.	
Signature algorithm	Signature of the certificate, generated and coded in accordance with the requirements described in RFC 5280.	

Table 7.2. Profile of basic fields of certificates issued at ROOT CA level

7.1.1 Version numbers

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

7.1.2 Certificate extensions

Certificate extensions for certSIGN ROOT CA G3 are described in Table 7.3.

Extension	Value or value constraints	Extension status
Basic Constraints	Subject type=CA, Path length constraint=none	Critical
Key Usage	keyCertSign (bit 5), cRLSign (bit 6)	Critical
Beneficiary Key Identifier	2C:66:C5:03:D8:0D:4E:9C:FB:A3:D8:1E:05:D4:BA:88:E9:BF:1D:95	Non-Critical

Table 7.3. Extensions of certSIGN ROOT CA G3 certificate

Certificate extensions for subordinate CA are described in Table 7.4

Extension	Value or value constraints	Extension status
Authority Key Identifier	2C:66:C5:03:D8:0D:4E:9C:FB:A3:D8:1E:05:D4:BA:88:E9:BF:1D:95	Ne-Critic
Beneficiary Key Identifier	The KeyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the label, length and number of unused bits).	Non-Critical

Extension	Value or value constraints	Extension status
Basic constaints	Subject type=CA, Path length constraint=0	Critical
Key usage	keyCertSign (bit 5), cRLSign (bit 6)	Critical
CRL distribution points	http://crl.certsign.ro/certsign-rootg3.crl	Non-Critical
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-Critical
Authority access data	[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-rootg3.crt	Non-Critical

Table 7.4. Certificate extensions for Subordinate Authorities certificates

Certificate extensions for OCSP certificates are described in Table 7.5.

Extension	Value or value constraints	Extension status
Identifier of the Authority key	2C:66:C5:03:D8:0D:4E:9C:FB:A3:D8:1E:05:D4:BA:88:E9:BF:1D:95	Non-Critical
Identifier of the Beneficiary key	KeyIdentifier is composed of the 160-bit SHA-1 hash of the value of BIT STRING subjectPublicKey (except for the label, length and number of unused bits).	Non-Critical
Key usage	digitalSignature (bit 0nonRepudiation (bit 1)	Critical
Extended key usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	Non-Critical
OCSPNoCheck	-	Non-Critical

Table 7.5. Certificate extensions for OCSP certificates

7.1.3 Electronic signature algorithm identifier

The signature algorithm field contains a cryptographic algorithm identifier used for electronic signature created by a certificate authority on the certificate. For certSIGN, the algorithm used is sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

7.1.4 Name formats

The content of the name fields in certificates conforms to the requirements in section 3.1 of this document, and to the certificate policy requirements in the current version of the CAB Forum Baseline Requirements.

The Issuer Name, for all possible certification paths, must be byte-for-byte identical to the Subject Name in the Issuer's certificate. Subject attributes cannot contain only metadata such as '.', '-', and ' ' (i.e. space) to indicate that the value does not exist, is incomplete, or is not applicable.

7.1.5 Name constraints

Not applicable.

7.1.6 Object identifier for the identification policy

The policy object identification certificates used at CA Root level are described in Table 7.6.

Root CA level	Type	OID
certSIGN ROOT CA G3	**CA certificates**	**2.5.29.32.0**
	OCSP certificate	**1.3.6.1.4.1.25017.6.1.3**

Table 7.6 Object identifier for the certification policy

7.1.7 Use of Policy constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

certSIGN issues certificates containing a policy qualifier within the Certificate Policies extension. This extension contains a CPP qualifier that sends 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 and value restrictions	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer	Department (OU)=	certSIGN ROOT CA G3
	Organization (O) =	certSIGN SA
	Country (C) =	RO
ThisUpdate	Date emiterii CRL	

Field name	Value and value restrictions
NextUpdate	Data urmatorului update CRL
Revoked Certificates	Lista certificatelor revocate

Table 7.7 CRL profile for certSIGN ROOT CA G3

7.2.1 Version numbers

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

7.2.2 CRL and CRL input extensions

CRL extensions for certSIGN ROOT CA G3 are described in Table Tabelul 7.8.

Extension	Value and value constraint	Extension status
Authority Key Identifier	2C:66:C5:03:D8:0D:4E:9C:FB:A3:D8:1E:05:D4:BA:88:E9:BF:1D:95	Non-critical
CRL Number	monotonically increasing sequence number	Non-critical
crlEntryExtensions	ReasonCode for revocation	Non-critical

Table 7.8. Extensions of certSIGN ROOT CA G3 CRL

CRL input extensions (**crlEntryExtensions**) accepted by certSIGN - contain the following fields:

- **ReasonCode**: code of the reason for the certificate revocation. This field is not critical and allows to determine the reason for revocation of a certificate. The following revocation reasons are allowed:
  - **keyCompromise** – key compromise;
  - **cACompromise** – compromise of the CA key;
  - **affiliationChanged** – modification of the Subscriber's data;
  - **superseded** – certificate renewal;
  - **cessationOfOperation** – discontinuation of the certificate use;
  - **removeFromCRL** – removal of the certificate from the CRL.

The reason ReasonCode **unspecified** – unspecified, is NOT allowed.

7.3 OCSP profile

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

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

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

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

The OCSP server certificate also contains the OCSPNoCheck extension, described by RFC 6960. This extension must be declared as non-critical and means that an OCSP client who receives a signed response with the private key associated with this certificate can trust the status of the certificate of the OCSP server, no need to check its revocation status.

Entitatea care primeşte o confirmare emisă de serverul OCSP trebuie să suporte formatul standard de răspuns având identificatorul **id-pkix-ocsp-basic**.

Informaţiile despre starea certificatului sunt incluse în câmpul **certStatus** al structurii **SingleResponse**. Acesta poate avea una dintre următoarele trei valori principale:

- GOOD – indică faptul că certificatul este în stare validă
- REVOKED – indică faptul că certificatul a fost emis și a fost revocat sau certificatul nu a fost emis conform RFC 6960
- UNKNOWN – indică faptul că nu există suficiente informaţii pentru determinarea stării certificatului respectiv
- Când răspunsul OCSP conține un cod de eroare (mesaj), răspunsul nu este semnat digital (RCF 6960).

7.3.1 Version

OCSP server operating in 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

According to RFC 6960, certSIGN OCSP server accepts the following extension:

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

The **revocationReason** field in **RevokedInfo** and **CertStatus** is present, and has a value allowed for the CRLs, as per section 7.2.2 above.

8 Compliance audit and other assessments

Regarding the compliance audits and competence, the consistent functioning and impartiality of the conformity of the assessment bodies that assess and certify our compliance as a certification service provider and the compliance of our certification services for the criteria of Regulation 910/2014 and the implementing acts, we follow the requirements of the ETSI EN 319 403 and ESTI EN 319 411-1 standards.

8.1 Frequency or circumstances of assessment

certSIGN activities supporting the provision of services presented by the CPS ROOT CA are audited at least once every 12 months.

The audit verifies compliance with CPS technical standards and ETSI 319401 and ETSI 319411 technical standards and CA/B Forum Baseline requirements.

On-demand audits may be performed at the discretion of certSIGN, at the request of the supervisory body as defined in EU Regulation 910/2014, or to demonstrate compliance with specific industry, legal or business requirements.

8.2 Auditor's identity/qualifications

The assessment will be carried out by a conformity assessment body as defined in EU Regulation 910/2014 and the CA/B Forum Baseline specifications.

8.3 Relation of the auditor with the assessed entity

The conformity assessment body is and independent auditor, who is not directly or indirectly affiliated to certSIGN.

8.4 Topics covered by the audit

Planned audits include, but are not limited to, all aspects of certSIGN operations and services specified in this CPS and in accordance with ETSI EN 319 411-1, which includes normative references to ETSI EN 319 401.

8.5 Action taken as a result of the deficiency

The conformity assessment body shall report the detected deficiencies and non-conformities to the PPMB. certSIGN and the conformity assessment body shall analyse the results of the report at the same time and shall approve a corrective plan and a time-frame for its implementation.

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 PPM.

8.7 Internal audit

Not stipulated.

9 Other business and legal matters

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.

The services offered by certSIGN are established as follows:

- **Individual certification services** – the price is determined for each service, for example, for each certificate sold or for a small number of certificates,
- **Certification service packages** – the price is set for bundles of services supplied to a single entity,
- **Subscription services** – the price is set for services rendered on a periodic basis; the amount paid depends on the type and number of services accessed and is used in particular for time-stamping and certificate status checking services by means of OCPS protocols,
- **Indirect services –** the price is set for each service offered to its customers by a certSIGN partner, which bases its activity on the certSIGN infrastructure.

Payments will be made in cash, by payment order, and by credit cards, according to the legal regulations in force.

9.1.1 Rates for issuance and renewal of digital certificates

Rates are set according to the internal price policy.

9.1.2 Rates for certificate access

Fre of charge service.

9.1.3 Rates for revocation services or access to certificate status information

Fees are set according to the internal price policy.

9.1.4 Other rates

Fees are set according to the internal price policy.

9.1.5 Refunding

Payments may be reimbursed according to the applicable contractual conditions.

9.2 Financial liability

9.2.1 Warranty coverage

Not applicable.

9.2.2 Other assets

Not applicable.

9.2.3 Securing or covering the guarantee for the final entities

Not applicable.

9.3 Confidentiality of Business Information

9.3.1 Purpose of Confidential Information

All information regarding the Subject/Beneficiary/Relying Party processed by certSIGN is obtained, stored and processed in accordance with the provisions of Regulation (EU) no. 910/2014. Relationships between a Subject, the Beneficiary, a Relying Party and certSIGN are based on trust.

A third party may only have access to publicly available information in certificates. The other data provided to certSIGN shall not be disclosed under any circumstances to any third party, on a voluntary basis (except as provided by law).

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.

Disclosure of any information to the entities involved in the fulfilment of the obligations shall be confidential and shall extend only to the information necessary for the fulfilment of the obligations.

Types of information considered to be confidential or private

certSIGN, its employees as well as the entities performing certification activities are bound to keep the information secrecy, both during and after the termination of the employment contract, in the case of employees. The following is classified as private or confidential information:

- information provided by Subjects/Beneficiaries, in addition to the information appearing in the certificates and in the Repository; disclosure of such information shall be made only with the prior written consent of the owner of the information or under other conditions prescribed by law;
- contents of contracts with Subjects/Beneficiaries or Relying Parties, bank accounts, applications for registration, issuance, renewal, revocation of certificates; this information may only be disclosed with the approval and for the purpose stated by the owner of the information (e.g., the Subject), except for information contained in certificates or from the Repository, in accordance with this CPS;
- the corresponding transaction records in the system (all types of transactions as well as transaction control data, so-called transaction logs in the system);
- records of events (logs) related to certification services kept by certSIGN;
- the results of internal and external audits, if they pose a threat to certSIGN security;
- emergency plans;
- information on measures taken to protect hardware devices and software applications, information on the administration of certification services and planned registration rules.

Persons who have access to confidential information are subject to the rules on the management of confidential information and are liable according to the applicable law.

Disclosing the reason why a certificate has been revoked

If a certificate has been revoked at the request of an authorized party other than the Subject, the information on the revocation and the reasons for such revocation shall be communicated to both parties.

Disclosing Confidential Information to the Representatives of Legal Authorities

The confidential information may be disclosed to representatives of legal authorities only after the fulfilment of all the formalities required by the legislation in force in Romania.

9.3.2 Information not considered to be confidential

The information included in a certificate by the issuing Certification Authorities as specified in Chapter 7 is not confidential. A Subject /Beneficiary applying for a certificate knows what kind of information will be included in the certificate and agrees to its publication.

Except for the information provided in the previous paragraph, the information provided by / to the Subject / Beneficiary may be made available to other entities, only with the written consent of the Subject / Beneficiary and for the purpose stated in the contract concluded with the Subject / Beneficiary.

9.3.3 Responsibility to protect confidential information

certSIGN and its employees, maintain confidentiality of information both during the provision of certification services and after the end certificates validity.

9.4 Confidentiality of Personal Information

In the provision of trust services, certSIGN processes personal data of the Subject/Subscriber in accordance with the requirements of Regulation (EU) no. 910/2014 and in compliance with the national provisions, Regulation no. 679/2016 on the protection of individuals with regard to the processing of personal data and to the free movement of such data and other provisions of Union law on data protection.

The purpose of the processing of personal data is to provide certification services.

9.4.1 Plan to ensure the protection of personal data

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

The security measures required by Regulation (EU) No 910/2014, Regulation No 679/2016 and by the supervisory authority in the field of processing personal data are implemented by certSIGN to ensure that:

- adequate technical and organizational measures are taken to ensure the security of the processed data, to protect the rights of the Subjects and to comply with the principles provided by Regulation no. 679/2016 and the provisions of Regulation (EU) no. 910/2014.
- access to certSIGN services refers to the processing of only those identification data, which are adequate, relevant and not excessive to grant access to that service
- the confidentiality and integrity of the registration data are ensured: when they are exchanged with the subscriber / subject, when they are exchanged between the components of the certSIGN system, as well as when they are stored.

9.4.2 Information considered as personal data

All information about the Subject that leads to its identification is considered as personal data.

9.4.3 Information not considered as personal data

The content of the digital certificates and the information accessible through the Repository are public information.

9.4.4 Responsibility to protect confidential information

certSIGN undertakes to maintain the confidentiality of personal information both during the provision of certification services and after the end of certificate validity.

certSIGN shall not disclose personal information to any third party, for any reason, except when it shall be required to do so by law or by the competent authorities.

9.4.5 Notification of data subjects and their consent for the use of personal data

In the process of issuing a digital certificate, the subjects/beneficiaries are informed about the need to use the personal data belonging to them, in order to provide the service and the need to grant the consent. If data Subjects do not agree to certSIGN processing their data, they cannot benefit from certification services.

Also, the Subjects/Beneficiaries have the possibility to explicitly opt for the use of personal data for other purposes expressly communicated by certSIGN by contract or otherwise.

9.4.6 Disclosure as a result of an administrative or legal process

certSIGN is exonerated from liability for the disclosure of personal data of the Subjects/Beneficiaries in the following situations:

- disclosure of personal information to the Supervisory Body according to the applicable legislation;
- to the competent institutions and bodies, based on the public law obligations that certSIGN has, in accordance with the legal provisions;

9.4.7 Other circumstances for disclosure

The following situations also constitute exceptions to the obligation to maintain the confidentiality of personal data which relieves certSIGN of liability:

✓ Disclosing personal information to:

- auditors during the audits to which certSIGN is subject according to the provisions of Regulation (EU) no. 910/2014 under confidentiality conditions;
- the courier companies with which certSIGN has a contract, with the consent of the Subject/Beneficiary, if he has opted for sending the certificate to his home address or to another address communicated, in compliance with the same obligations regarding the security of personal data that certSIGN has;
- proxies to whom certSIGN outsourced certain services;
- companies affiliated to certSIGN

- ✓ personal information appearing in certificates or in Public Directories (Repository), with the consent of the Subject/Beneficiary;
- ✓ in any other justified situations with prior notification of the Subject/Subscriber.

9.5 Intellectual Property Rights

All trademarks, names, patents, logos, licenses, applications, software, graphic images, etc. used by certSIGN are and will remain the intellectual property of their legal holders. certSIGN undertakes to specify this according to the requirements imposed by the holders.

All trademarks, names, patents, logos, licenses, applications, software, graphic images, etc., belonging to certSIGN are and remain the property thereof, whether or not accompanied by patents, utility models, copyrights or the like, and may not be reproduced or supplied to any third party without the prior written consent of certSIGN.

9.6 Representations and Warranties

9.6.1 CA representations and warranties

certSIGN emite certificate compatibile X509 v3.

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 G3 is responsible for the performance and warranties of the subordinate CAs, and for all liabilities and indemnification obligations of the subordinate CAs, within the limits of current CPS, acting as if the ROOT CA G3 were the subordinate CA that issued the certificates.

9.6.2 RA representations and warranties

The RA has the obligation to strictly observe the CPS, the relevant section of the applicable CP, as well as the relevant internal procedures of certSIGN.

9.6.3 Subject's representations and warranties

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

The Subject agrees to the CPS and his relevant responsibilities, duties and obligations as set out in the relevant sections of the CPS and the applicable CP.

The Subject shall be liable in particular to the Relying Parties for any use of his or her QSCD, including keys or certificate (s).

9.6.4 Representations and warranties of Relying Parties

Examples of obligations and responsibilities pertaining to Relying Parties 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,
- Immediate cessation of any use of a certSIGN Certificate if it has been revoked or when it has 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

Not applicable.

9.7 Warranty waiver

Except as expressly provided elsewhere than in the CPS, in the applicable CP and in the applicable law, certSIGN disclaims all warranties and obligations of any kind, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of the information provided (except that it came from an authorized source) and undertakes no liability for the negligence and inattention of Subjects, Beneficiaries and Relying Parties.

9.8 Limitation of Liability

To the extent permitted by the Romania Law, in no event (except for fraud or willful misconduct by certSIGN) certSIGN will be liable for:

- Any loss of profit;
- Any loss of data;
- Any indirect, consequential or punitive damages arising out of or in connection with the use, delivery, license, and performance or non-performance of certificates or electronic signatures;
- Any other damages.

9.9 Indemnification

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

9.10 Terms and termination

9.10.1 Terms

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

CPS remains in force until replaced by a new version.

9.10.3 Effect of termination and survival

The conditions and effect resulting from the termination of this CPS will be communicated through the website of certSIGN. This communication will highlight the provisions that may

survive the termination of this CPS and will remain in force. The responsibilities for protecting Confidential Information and Personal Information must survive termination and the terms and conditions for all existing certificates will remain valid for the remainder of the validity periods of such certificates.

9.11 Individual notifications and communication with participants

All notifications and other communications which may or must be given or sent mandatorily under the CPS shall be in writing and shall be delivered, except as expressly provided in the CPS, either by (i) registered e-mail address, acknowledgement of receipt, prepaid mail, (ii) a "within 24 hours" courier service or internationally recognized express, (iii) hand delivery or (iv) in electronic format, signed with a qualified electronic signature and addressed to certSIGN, using the contact details provided in chapter 1.5.1 of this document.

9.12 Amendments

9.12.1 Procedure for amendment

certSIGN is responsible, through its Policies and Procedures Management Body (PPMB) for the approval and change of the present 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 the customers of certSIGN. Subjects/Beneficiaries shall comply only with the currently applicable CPS.

9.12.2 Notification mechanism and timeframe

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

9.12.3 Circumstances in which the OID must be changed

Not applicable.

9.13 Dispute settlement procedures

All disputes associated with this CPS shall be resolved in accordance with the laws of Romania.

9.14 Governing law

The Romanian law governs the applicability, construction, interpretation, and validity of this CPS (excluding any conflict of law which would determine the application of other national or international laws).

9.15 Compliance with applicable laws

This CPS and the provision of the certSIGN Services are in accordance with the relevant and applicable Romanian laws and regulations EU 910/2014.

9.16 Miscellaneous

Not applicable.

9.17 Other provisions

Not applicable.