Certification Practice Statement
certSIGN Web CA
for DV SSL Certificates

Version 2.1

Date: 15 January, 2026

Important
Notice

Address: 29 A Tudor Vladimirescu Avenue,

AFI Tech Park 1, Bucharest, Romania

Phone: 004-021-31.19.901

Web: www.certsign.ro

Document History

Version	Effective Date	Reason	The person who made the change
1.0	6 October 2022	First version publishing	PKI Policies Manager
1.1	31 January 2023	Annual review	PKI Policies Manager
1.2	31 July 2023	Updates according to CABF BR	PKI Policies Manager
1.3	31 January 2024	Annual review	PKI Policies Manager
1.4	31 March 2024	Add 3k and 4k key length	PKI Policies Manager
1.5	18 April 2024	Add cross certificate	PKI Policies Manager
1.6	15 August 2024	Updates acc. CABF BR	PKI Policies Manager
1.7	26 November 2024	Add ACME method	PKI Policies Manager
1.8	15 January 2025	Annual review	PKI Policies Manager
1.9	30 April 2025	Add Policy in the schema	PKI Policies Manager
2.0	30 November 2025	Add Mass revocation	PKI Policies Manager
2.1	15 January 2026	Annual review	PKI Policies Manager

This document was created and is the property of:

Owner	Author	Date created
certSIGN	PKI Policies Manager	October 2022

Distribution List

Destination	Date distributed
Public-Internet	October 2022
Public-Internet	January 2023
Public-Internet	July 2023
Public-Internet	January 2024
Public-Internet	March 2024
Public-Internet	April 2024
Public-Internet	August 2024
Public-Internet	November 2024
Public-Internet	January 2025
Public-Internet	April 2025
Public-Internet	November 2025
Public-Internet	January 2026

This document was approved by:

Version	Name	Date
1.0	Policies and Procedures Management Body	October 2022
1.1	Policies and Procedures Management Body	January 2023
1.2	Policies and Procedures Management Body	July 2023
1.3	Policies and Procedures Management Body	January 2024
1.4	Policies and Procedures Management Body	March 2024
1.5	Policies and Procedures Management Body	April 2024
1.6	Policies and Procedures Management Body	August 2024

Version	Name	Date
1.7	Policies and Procedures Management Body	November 2024
1.8	Policies and Procedures Management Body	January 2025
1.9	Policies and Procedures Management Body	April 2025
2.0	Policies and Procedures Management Body	November 2025
2.1	Policies and Procedures Management Body	January 2026

Content

1 Introduction

The Certification Practice Statement certSIGN Web CA for DV SSL certificates – (further referred as **CPS**) describes in detail the certification policy and practices applied by certSIGN for issuance of **DV (Domain Validation) SSL certificates**.

The structure and content of the CPS are in compliance with RFC 3647 recommendations and latest published version of:

- ETSI EN 319 411-1 (DVCP policy 0.4.0.2042.1.6)
- CA/B Forum Baseline Requirements (DV policy 2.23.140.1.2.1)
- CA/Browser Forum Network and Certificate System Security Requirements
- WebTrust Principles and Criteria for Certification Authorities
- Webtrust Principles and Criteria for Certification Authorities - TLS Baseline
- Webtrust Principles and Criteria for Certification Authorities – Network Security
- Mozilla Root Store Policy,
- Apple Root Certificate Program,
- Microsoft Trusted Root Program,
- Chrome Root Program Policy.

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

1.1 Overview

certSIGN, Subscribers, Subjects and associated Relying Parties' operation depend on the **CPS** for the issuance of DV SSL certificates. Also, this document describes the general rules for providing certification services delivery such as Subject's registration, public key certification, certificates rekey and certificate revocation.

1.2 Document name and identification

This document is called **Certification Practice Statement for certSIGN Web CA for DV SSL Certificates,** further referred as **CPS**.

The following Certificate Policy identifiers are reserved for use by certSIGN Web CA for asserting compliance with this document as follows:

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) certSIGN (25017) id-policy(3) id-cp (1) certSIGN Web CA (4) domain validated website authentication certificate (2)} (1.3.6.1.4.1.25017.3.1.4.5)

The document is available in electronic format within the Repository at address https://www.certsign.ro/en/document/certsign-web-ca-dv-certification-practice-statement/

1.3 PKI Participants

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

- certSIGN Web CA
- Registration Authority,
- Repository,
- Online certificate status protocol (OCSP Authority),
- Subjects,

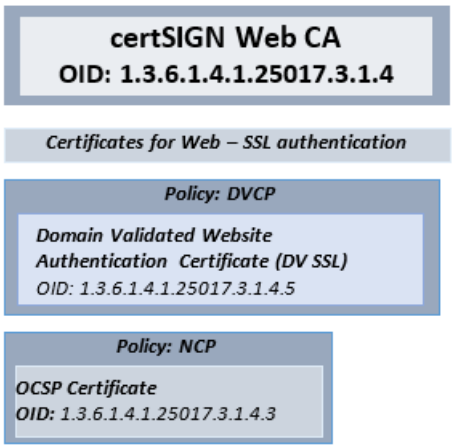
- Subscribers,
- Relying Parties,
- Relevant suppliers for certSIGN regarding issuance and management of digital certificates.
- Policies and Procedures Management Body
- Auditors

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

1.3.1 Certification authorities

certSIGN Web CA is a Subordinate Certification Authority for the certSIGN domain, subordinated to the certSIGN ROOT CA G2.

certSIGN Web CA is identified by the following OID: 1.3.6.1.4.1.25017.3.1.4.



1.3.2 Registration authorities

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

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

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

1.3.3 Subscribers

Subscriber

Subscriber is the Legal Entity to whom a certificate is issued and who is legally bound by a Subscriber Agreement. Subscribers may request issuance, revocation or rekey of end-entity certificates for Subjects under their care.

The subscriber is responsible for:

- Immediately notifying certSIGN upon (suspicion of) private key compromise;
- Submitting requests for certificates rekey to certSIGN in due time;
- Ensuring that the confidentiality of their private key is protected in a manner that is consistent with this document;
- Ensuring that access to use of their private key is controlled in a manner that is consistent with this document.

Subject

The Subject is a device under the control and operation of the Subscriber.

1.3.4 Relying parties

A Relying Party, using certSIGN's services, can be any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

A Relying Party is responsible for how it verifies the current status of a Subject's certificate. A Relying Party shall use the information in a certificate (for example, identifiers and qualifiers of certification policy) to decide whether a certificate was used according to the stated purpose.

1.3.5 Other participants

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

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

1.4 Certificate usage

The certificate applicability area settles the scope in which a certificate may be used. This scope is defined by two elements:

- The first defines the certificate applicability
- The other 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 used for a certain purpose. Taking into consideration the significant risk factors the Relying Party shall decide what type of certificate issued by certSIGN meets the formulated requests.

1.4.1 Appropriate certificate uses

Certificates issued by certSIGN Web CA can be used for TLS server authentication.

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

- Manage properly the public and private keys,
- Certificates and associated public keys are used in compliance with their declared purpose, confirmed by certSIGN,

- Have built-in mechanisms of certificate status verification, certification path creation and validation control (signature availability, expiration date etc.),
- Provides relevant information regarding certificates and their status for users.

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

It is the responsibility of the Relying Party to decide for which purpose the certificates are considered trustworthy. A Relying Party must always take into account the level of assurance and other information in the CPS before deciding on the applicability of the certificate.

1.4.2 Prohibited certificate uses

Certificates must only be used to the extent consistent with applicable law and for the purposes specified in chapter 1.4.1

1.5 Policy administration

1.5.1 Organization administering the document

The present document is administered by the certSIGN TSP Policies and Procedures Management Body (PPMB). The PPMB includes senior members of management as well as staff responsible for the operational management of the certSIGN TSP PKI environment.

Name	S.C. certSIGN S.A. Office: 29 A Tudor Vladimirescu Avenue, AFI Tech Park 1, Bucharest, Romania Register Number: J2006000484402 Tax registration code: RO 18288250 Registered office: 107A Oltenitei Street. building C1, ground floor, District 4, Bucharest, Romania, PC 041303
Phone	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Table: 1.5.1 Organization administering the document

1.5.2 Contact person

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

Table: 1.5.2 Contact person

Procedure for certificate problem reporting

Due to some errors, technical or procedural limitations or form other reasons, certificates may be misissued by certSIGN (e.g the issued certificate contains wrong information about the subject). Also, there may be cases when a certificate is used inappropriately (e.g. for criminal activities). If subscribers, relying parties or other third parties come across such situations, if they suspect private key compromise, or other kind of fraudulent activities, misuse of a certificate or inappropriate conduct or any other similar matters related to certificates issued

by certSIGN, they can report those problems at the address revokecsgn@certsign.ro, informing the issuing CA of reasonable cause to revoke the certificate. certSIGN CA will begin investigation of a Certificate Problem Report within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

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

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

1.5.3 Person determining CPS suitability for the policy

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

Table: 1.5.3 Person determining CPS suitability for the policy

1.5.4 CPS approval procedures

Policies and Procedures Management Body is responsible for the approval of the CPS.
The approval procedure is described in an internal instruction document.
Subscribers shall adhere to the CPS published at:
https://www.certsign.ro/en/document/certsign-web-ca-dv-certification-practice-statement/
Subscribers who do not accept new, modified terms and regulations of CPS shall make a suitable statement within 15 days of the date of the new version of CPS approval. This will lead to termination of the contract related to certification services providing and the revocation of the certificated issued on its ground.

1.6 Definitions and acronyms

1.6.1 Definitions

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Beneficiary/Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the **Beneficiary** /Applicant is referred to as the Subscriber. For Certificates issued to devices, the **Beneficiary** /Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Beneficiary/Applicant Representative: A natural person or human sponsor who is either the **Beneficiary**, employed by the **Beneficiary**, or an authorized agent who has express authority to represent the **Beneficiary**: (i) who signs and submits, or approves a certificate request on behalf of the **Beneficiary**, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the **Beneficiary**, and/or (iii) who acknowledges the Terms of Use on behalf of the **Beneficiary** when the **Beneficiary** is an Affiliate of the CA or is the CA.

Application Software Supplier: A supplier of Internet browser software or other relying party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on site at the CA.) The coverage rules and maximum length of audit periods are defined in section 8.1.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

Authorized Ports: One of the following ports: 80 (http), 443 (http), 25 (smtp), 22 (ssh).

Base Domain Name: The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

CAA: From RFC 8659 (http:tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate misissue."

CA Key Pair: A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7, e.g. a Section in a CA's CPS or a certificate template file used by CA software.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements, and describes the boundaries and acceptable uses of certificates from a given PKI.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Intermediate CAs.

Certification Practice Statement (CPS) is a statement of the practices which a Certification Authority employs in issuing and managing certificates**.**

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

Cross-Certified Subordinate CA Certificate: A certificate that is used to establish a trust relationship between two CAs.

CSPRNG: A random number generator intended for use in cryptographic system.

Delegated Third Party: A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits, but is authorized by the CA

to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

DNS CAA Email Contact: The email address defined in CABF BR Appendix A.1.1.

DNS CAA Phone Contact: The phone number defined in CABF BR Appendix A.1.2.

DNS TXT Record Email Contact: The email address defined in CABF BR Appendix A.2.1.

DNS TXT Record Phone Contact: The phone number defined in CABF BR Appendix A.2.2.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Label: From RFC 8499 (http://tools.ietf.org/html/rfc8499): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names".

Domain Name: An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinated to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with:

(i) the Internet Corporation for Assigned Names and Numbers (ICANN),
(ii) a national Domain Name authority/registry, or
(iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names

at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

Intermediate CA: is a CA that falls below the Root CA in a given PKI and is normally managed by the same entity as the Root CA.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or an Intermediate/Subordinate CA.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it.

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair.

Key Pair: The Private Key and its associated Public Key.

LDH Label: From RFC 5890 (http://tools.ietf.org/html/rfc5890): "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets."

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Non-Reserved LDH Label: From RFC 5890 (http://tools.ietf.org/html/rfc5890): "The set of valid LDH labels that do not have '--' in the third and fourth positions."

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Onion Domain Name: A Fully Qualified Domain Name ending with the RFC 7686 ".onion" Special-Use Domain Name. For example, gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion is an Onion Domain Name, whereas torproject.org is not an Onion Domain Name.

Online Certificate Status Protocol: An online Certificate-checking protocol (OCSP) that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Parent Company: A company that Controls a Subsidiary Company.

Primary Network Perspective: The Network Perspective used by the CA to make the determination of
1) the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and
2) the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es).

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

P-Label: A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2.

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and

governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Request Token: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request.
The Request Token SHALL incorporate the key used in the certificate request.
A Request Token MAY include a timestamp to indicate when it was created.
A Request Token MAY include other information to ensure its uniqueness.
A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.
A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.
A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation.
The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

Requirements: The Baseline Requirements found in the CABF BR document.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved:
http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Root CA: The top level Certification Authority, whose Root Certificate is distributed by Application Software Suppliers, that represents the 'trust anchor' for the chain of trust, and that issues Intermediate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Intermediate CAs.

Short-lived Subscriber Certificate: For Certificates issued on or after 15 March 2024 and prior to 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).

Sovereign State: A state or country that administers its own government, and is not dependent upon, or subject to, another power.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Subsidiary Company: A company that is controlled by a Parent Company.

Technically Constrained Intermediate/Subordinate CA Certificate: An Intermediate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Intermediate CA Certificate may issue Subscriber or additional Intermediate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialists: Someone who performs the information verification duties specified by these Requirements.

Validity Period: From RFC 5280, (http://tools.ietf.org/html/rfc5280):the period of time from notBefore through notAfter, inclusive.

WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

Wildcard Domain Name: A Domain Name consisting of a single asterisk character followed by a single full stop character ("*.") followed by a Fully-Qualified Domain Name.

XN-Label: From RFC 5890 (http://tools.ietf.org/html/rfc5890): "The class of labels that begin with the prefix "xn--" (case independent), but otherwise conform to the rules for LDH labels."

1.6.2 Acronyms

Acronym	Meaning
ADN	Authorization Domain Name
AICPA	American Institute of Certified Public Accountants
BIPM	International Bureau of Weights and Measures
BIS	(US Government) Bureau of Industry and Security
CA	Certification Authority
CAA	Certification Authority Authorization
CARL	Certification Authority Revocation List
ccTLD	Country Code Top-Level Domain
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CICA	Canadian Institute of Chartered Accountants
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CP	Certificate Policy
CPA	Chartered Professional Accountant
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSO	Chief Security Officer
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
DV	Domain Validated
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
gTLD	Generic Top-Level Domain
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IFAC	International Federation of Accountants
IM	Instant Messaging
IRS	Internal Revenue Service
ISO	International Organization for Standardization
ISP	Internet Service Provider
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier

OV	Organization Validated
PKI	Public Key Infrastructure
PPMB	Policies and Procedures Management Body
QEVCP-w	Certificate Policy for EU qualified Website Authentication based on EVCP
QGIS	Qualified Government Information Source
QIIS	Qualified Independent Information Source
QNCP-w	Certificate policy for EU qualified website authentication certificates based on NCP and PTC
QSCD	Qualified Electronic Signature Creation Device
QTIS	Qualified Government Tax Information Source
QWAC	Qualified Certificate for Website Authentication
RA	Registration Authority
RSA	Rivest, Shamir, Adleman asymmetric cryptographic algorithm
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SEC	(US Government) Securities and Exchange Commission
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TSP	Trust Services Provider
UTC	Coordinated Universal Time
UTC(k)	National realization of Coordinated Universal Tim
VoIP	Voice Over Internet Protocol

2 Publication and repository responsibilities

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

2.1 Repositories

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

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

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

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

2.2 Publication of certification information

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

Certificates are available for retrieval in only those cases for which the Subscriber's consent has been obtained, and will be used as described in the Terms and Conditions document. All our web server certificates can be found in the Certificate Transparency logs. For all issued certificates, the certificate status information is available through CRLs and OCSP service provided by certSIGN 24*7*365.

certSIGN conforms to the latest published version of the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.
certSIGN hosts on https://testssl.certsign.ro/ 3 web pages that allow Application Software Suppliers to test software with Subscriber Certificates issued by certSIGN Web CA:
https://testssl-valid-evcp.certsign.ro
https://testssl-revoked-evcp.certsign.ro
https://testssl-expired-evcp.certsign.ro

Availability

Availability of the repository and the combined CRL repository is designed to exceed 99.8% of business hours - defined as 24 hours per day, seven days per week, excluding planned maintenance periods.

Planned maintenance periods will be announced on https://www.certsign.ro at least 24 hours in advance.

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

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

2.3 Time or frequency of publication

The information published by certSIGN (Certification Practice Statement) is updated annually or following specific events as specified here:

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

2.4 Access control on repositories

All information published by certSIGN in the Repository on the address https://www.certsign.ro/en/repository/ is available for the public. The repository is publicly and internationally available 24*7*365.

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

Subscribers, 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 and prevent against abusive usage of repository, the OCSP, and CRL download services.

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

3 Identification and authentication

3.1 Naming

The structure and use of names in certificates comply with X.500, RFC5280, and CABF Baseline Requirements.
CERTSIGN does NOT allow the use of internationalized domain names (IDNs) in certificates.

The Subject names in a DV certificate comply with the X.500 Distinguished Name (DN) form. certSIGN Web CA use a single naming convention as set forth in the Baseline Requirements published by the CA/Browser Forum.

The certificates issued pursuant to this CPS are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the website to which they are assigned in a meaningful way.

The Distinguished Name attribute is unique to the Subject to which it is issued. For each DV certificate, a unique serial number within the name space of the certSIGN Web CA is issued.

3.1.1 Types of names

Certificates issued by certSIGN are in compliance with X.509 v3 standard. This means that the certificate issuer and the Registration Authority that acts on behalf of the issuer approve the Subject's name in compliance with X.509 standard (with referring to X.500 series' recommendations). Basic names of the Subjects and of the certificate issuers placed in certSIGN's certificates are in compliance with the Distinctive Names – DN – (also known as directory names), created following X.500 and X.520 recommendations.

3.1.2 Need for Names to be Meaningful

SSL certificates, except wildcard and type Unified Communications certificates, are issued with a Fully Qualified Domain Name (FQDN) or with an IP address.

Wildcard SSL certificates contain an asterisk. Before issuing such a certificate, it needs to be determined whether the asterisk appears on the first position, to the left of the suffix of a domain controlled by the domain registration organization (i.e. *.com.ro) or of the public suffix (i.e. *.ro, *.edu, "*.com", "*.co.uk"; for details, see RFC 6454 Section 8.2) and if this happens, the CA ran by certSIGN will refuse the request, because the domain needs to be owned or controlled by the subscriber.

For SSL certificates, while FQDN or an authenticated domain name can be placed in the Common Name (CN) attribute of the Subject field, it is present in the Subject Alternative Name extension, in DNS Name. Subject Alternative Name are marked as non-critical, in accordance with RFC5280.

CertSIGN does not issue SSL certificates that contain "underscore character" ("_") in the domain name/dNSName, in compliancy with the CA/Browser Forum BR recommendations current version. FQDN consists solely of P - Labels and Non-Reserved LDH Labels.

Type Unified Communications SSL certificates (multi domain) must not include non-routable domains (i.e..local) or private IPs (in accordance with RFC 1918) within the Subject Alternative Name extension. Domain .int is treated as routable domain.

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

certSIGN does not issue SSL DV certificates for natural persons.

For legal entities, DN consists of the following mandatory fields (the description of the field is followed by its abbreviation that complies with X.520 recommendations):

- Field CN – Fully-Qualified Domain Name,
- Field C – international abbreviation for country name.

3.1.3 Anonymity or pseudonymity of subscribers

certSIGN does not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

The interpretation of the fields within the certificates issued by certSIGN is done in accordance with the certificate profiles described in Certificates and CRL-s Profiles (Chapter 7). In creating and interpreting the DN it goes to recommendations mentioned in Chapter 3.1.2.

3.1.5 Uniqueness of names

Name uniqueness is ensured through the use of the Fully Qualified Domain Name in Subject Alternative Name. The uniqueness of a domain name is guaranteed by Internet Corporation for Assigned Names and Numbers (ICANN).

3.1.6 Recognition, authentication and role of trademarks

No Stipulation.

3.2 Initial identity validation

3.2.1 Method to prove Possession of Private Key

The possession of the private key, corresponding to the public key for which it is requested the generation of the certificate, will be proven by sending the Certificate Signing Request (CSR), per the RSA PKCS#10 standard, in which it will be included the public key signed by the associated private key.

3.2.2 Authentication of organization identity

It is necessary to prove that the entity that requests the DV SSL certificate has control over the domain the certificate request is referring to.

The procedure for validating the Applicant's ownership or control of the domain is based on ETSI EN 319 411-1 and latest published version of CA/Browser Forum - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates.

3.2.2.1 Identity

The representative of the organization is bind to present upon the request of the Registration Authority a Purchasing request.

The procedure performed by RA to verify the domain consists of:

- Verify the documents presented by the Subscriber,

- Verify the request, that consists of:
  - Verifying the compliance of the data mentioned in the request with those from the documents presented,
  - Verifying the proof of private key possession and the fact that the Distinctive Name is the right one,
- Verify that the domain mentioned in the certificate is registered by the entity submitting the certificate application or by the one that authorized the use of the domain by the requesting entity according to CA/Browser Forum– –#3.2.2.4.4 *(Constructed Email to Domain Contact),* or #3.2.2.4.7 (*DNS Change*) or #3.2.2.4.19 (*Agreed-Upon Change to Website - ACME).*
- Verifying in the regional Internet domain registry (the RIPE database for European subscribers) whether the person requesting the SSL certificate is the owner of or has the right to use the routable IP address for which the certificate is requested.

The Registration Authority is committed to verify the correctness and the authenticity of all data rendered in a request.

If the verification is successfully concluded an authorized operator of the Registration Authority issues a confirmation that certifies the compliance of the data from the processing request with the data provided and sends this confirmation to the Certification Authority. The Certification Authority verifies if this was issued by an authorized Registration Authority.

3.2.2.2 DBA (Doing Business As)/Trade Name

Not applicable.

3.2.2.3 Verification of country

The RA verifes the country associated with the Subscriber using one of the following:

(a) The IP Address range assignment by country for either

(i) the web site's IP address, as indicated by the DNS record for the web site or

(ii) the Subject/Subscriber's IP address;

(b) The ccTLD (Country Code Top-Level Domain) of the requested Domain Name;

(c) Information provided by the Domain Name Registrar; or

(d) As mention in Section 3.2.2.1.

The CA has implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

3.2.2.4 Validation of Domain Authorization or Control

This section defines the permitted processes and procedures for validating the Subscriber's ownership or control of the domain.

certSIGN confirms that prior to issuance has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below.

certSIGN will perform the domain check for all SANs included in the application. Therefore, multiple Administrative Contacts may be accessed or multiple actions may be required to demonstrate domain verification for all requested SANs.

certSIGN does not issue certificates for FQDNs that contain "onion" as the rightmost label.

Completed validations of Applicant authority may be valid for the issuance of multiple certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

certSIGN maintains records of which domain validation method, including relevant BR version number, they used to validate every domain.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method of domain validation is not used.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

This method of domain validation is not used.

3.2.2.4.3 Phone Contact with Domain Contact

This method of domain validation is not used.

3.2.2.4.4 Constructed Email to Domain Contact

certSIGN will send a Constructed Email to Domain Contact to confirm that the Applicant is aware of such ownership or control of the domain name. The e-mail will be sent to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by Authorization Domain Name and it will include a Random Value (generated through technical means, unique in each email).

The Random Value remain valid for use in a confirming response for 30 days from its creation. The response e-mail must be sent using the e-mail account used for initial sending, and certSIGN verifies if Random Value is the same. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.5 Domain Authorization Document

This method of domain validation is not used.

3.2.2.4.6 Agreed - Upon Change to Website

This method of domain validation is not used.

3.2.2.4.7 DNS Change

certSIGN will send an Email to the contact person who submitted the request to confirm that the Applicant has the control of the domain name. The e-mail will include a Random Value (generated through technical means, unique in each email) to be added in the DNS entry in one of DNS CNAME, TXT or CAA record of the domain to be checked.
The Random Value remain valid for use for 30 days from its creation.
certSIGN verifies if the value in the DNS entry is the same as the one sent.
Once the FQDN has been validated using this method, CERTSIGN MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN.
certSIGN implemented Multi-Perspective Issuance Corroboration as specified in #3.2.2.9.
This method is suitable for validating Wildcard Domain Names.

3.2.2.4.8 IP Address
This method of domain validation is not used.

3.2.2.4.9 Test Certificate
This method of domain validation is not used.

3.2.2.4.10 TLS Using a Random Number
This method of domain validation is not used.

3.2.2.4.11 Any Other Method
This method of domain validation is not used.

3.2.2.4.12 Validating Applicant as a Domain Contact
This method of domain validation is not used.

3.2.2.4.13 Email to DNS CAA Contact
This method of domain validation is not used.

3.2.2.4.14 Email to DNS TXT Contact
This method of domain validation is not used.

3.2.2.4.15 Phone Contact with Domain Contac
This method of domain validation is not used.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact
This method of domain validation is not used.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact
This method of domain validation is not used.

3.2.2.4.18 Agreed-Upon Change to Website v2
This method of domain validation is not used.

3.2.2.4.19 Agreed-Upon Change to Website – ACME
certSIGN confirms the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555. This is accomplished by receiving a successful HTTP response from the request. The token is not used for more than 30 days from its creation.

When certSIGN Web CA follows redirects, they are initiated at the HTTP protocol layer and are the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects are the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.

certSIGN implemented Multi-Perspective Issuance Corroboration as specified in #3.2.2.9.

This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.20 TLS using ALPN
This method of domain validation is not used.

3.2.2.4.21 DNS Labeled with Account ID – ACME

This method of domain validation is not used.

3.2.2.4.22 DNS TXT Record with Persistent Value

This method of domain validation is not used.

3.2.2.5 Authentication for an IP Address

No IP address certificates are issued under this CPS.

3.2.2.6 Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, the RA establishes and follow a documented procedure that determines if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation). If a wildcard would fall within the label immediately to the left of a registry-controlled or public suffix, RA refuses issuance unless the applicant proves its rightful control of the entire Domain Namespace.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, RA evaluates the source for its reliability, accuracy, and resistance to alteration or falsification. The RA considers the following during its evaluation:

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,
4. The public accessibility and the data availability, and
5. The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA Records

RA checks for CAA records and follow the processing instructions found, for each dNSName in the subjectAltName extension of the certificate to be issued, as specified in RFC 8659.

When processing CAA records, certSIGN process the issue, issuewild, and iodef property tags as specified in RFC 8659. certSIGN respect the critical flag and not issue a certificate if they encounter an unrecognized property tag with this flag set. certSIGN treat a non-empty CAA Resource Record Set that does not contain any issue property tags (and also does not contain any issuewild property tags when performing CAA processing for a Wildcard Domain Name) as permission to issue, provided that no records in the CAA Resource Record Set otherwise prohibit issuance. certSIGN will NOT issue a certificate unless the certificate request is consistent with the applicable CAA Resource Record set.

If a CAA record exists then it must list certSIGN as an authorized CA. The record allowed is certsign.ro. If the CA issues, the CA does so within the TTL of the CAA record, or 8 hours, whichever is greater.

certSIGN will document potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances, and will dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present.

certSIGN implemented Multi-Perspective Issuance Corroboration as specified in #3.2.2.9.

3.2.2.9 Multi-Perspective Issuance Corroboration

Multi-Perspective Issuance Corroboration attempts to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before Certificate issuance.
The set of responses from the relied upon Network Perspectives provides the CA with the necessary information to allow it to affirmatively assess:
- a. the presence of the expected Random Value, Request Token, or Contact Address, as required by the relied upon validation method specified in Sections 3.2.2.4 and
- b. the CA's authority to issue to the requested domain(s), as specified in Section 3.2.2.8.
Details on the MPIC requirements are in CA/B Forum Baseline Requirements #3.2.2.9.
certSIGN implemented Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives.

3.2.3 Authentication of individual identity

certSIGN does not issue SSL certificates to natural persons.

3.2.4 Non-verified subscriber information

No Stipulation.

3.2.5 Validation of authority

The authentication of authorizations is part of the procedure performed by the Registration Authority or by the Certification Authorities to process the certificate request for a device that belongs to a legal person. certSIGN use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request as listed in section 3.2.2.

The issuing of the certificate is a confirmation of the fact that a legal entity or a device has the right to use the private key on behalf of the legal entity.

3.2.6 Criteria for interoperation

certSIGN will disclose all Cross Certificates that identify the CA as the Subject, provided that the certSIGN arranged for or accepted the establishment of the trust relationship.
certSIGN ROOT CA issued a cross-certificate for certSIGN Web CA, initially issued by certSIGN ROOT CA G2, both PKI systems operated by certSIGN.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The same process as for initial identity validation is used (Chapter 3.2).

3.3.2 Identification and authentication for re-key after revocation

The same process as for initial identity validation is used (Chapter 3.2).

3.4 Identification and authentication for revocation request

Revocation requests can be sent via e-mail directly to the certificate issuer or indirectly to the Registration Authority. As well, the requests can be sent in other format than electronic.

- In first case, the Subscriber shall submit an authenticated request for certificate revocation. The Subscriber authenticates the request by applying an electronic signature.
- In the second case, the Subscriber is unable to send and electronic revocation. The revocation request shall be certified by the Registration Authority.

In both cases, there shall be a univocal identification of the Subscriber's identity. The revocation request may aim more certificates. The Subscriber's authentication and identification at the Registration Authority is realized as in the initial registration (see Chapter 3.2). The Subscriber's authentication to the Certification Authority consists of verifying the authenticity of the request. The detailed revocation procedure is described in Chapter 4.9.
The following entities can send certificate revocation requests:

- The Subscriber who enters into a contractual agreement with certSIGN for certificate issuance
- The Registration Authority that can request the revocation either on behalf of a Subscriber or if it has information that justifies the certificate revocation, by creating an authenticated request using the security mechanisms of the Registration Authority software
- Trusted roles associated to CertSIGN Web CA, under the supervision of the Policies and Procedures Management Body (PPMB), by creating an authenticated request using the security mechanisms of the Certification Authority software

4 Certificate life-cycle operational requirements

This chapter describes the basic procedures that are common to DV certificates issued by certSIGN Web CA.

4.1 Certificate Application

4.1.1 Who can submit a certificate application

certSIGN maintains an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. certSIGN uses this information to identify subsequent suspicious certificate requests.

Certificate Application by Natural Persons

certSIGN does not issues SSL certificates to natural persons.

Certificate Application by Legal Persons (Organizations)

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

The Certification Authority only issues certificates as a response to an authenticated request from the Registration Authority operated by certSIGN.

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

4.1.2 Enrollment process and responsibilities

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

certSIGN provides supervision, support and auditing for all the processes and services of the RA. The RA is responsible for the verification of the following items:

- The Subscriber's entitlement to the requested certificate(s)

The enrolment process is performed in compliance with the rules and methods described in the present CPS and in the internal guidelines and procedures of the RA & the applicable law. Prior to the issuance of a certificate, certSIGN obtains the following documentation from the Subscriber:

1. A certificate request, which may be electronic; and
2. An executed Subscriber Agreement or Terms of Use, which may be electronic.

The Subscriber is provided the following information which forms the Subscriber Agreement:

- The registration form
- The Certificate Terms and Conditions
- Reference online address of the CPS
- Bylaws, notices or other documents provided by the Subscriber (to be defined in the Subscriber Agreement)

The signed registration form is considered the formal acceptance by the Subscriber of the Subscriber Agreement whereby the Subscriber accepts the following:

- His responsibility that the information provided by the Subscriber to the RA is correct, complete, valid and up to date,

- That certSIGN maintains a retention period of 10 years counting from the date of the issued certificate of all the information pertaining to the registration and enrolment, the certificate request, revocation of the certificate
- That in case certSIGN (as CA and RA) ceases its activities, this data may be transferred to a third party, respecting the same terms and conditions as defined in the Subscriber Agreement,
- Acknowledges the rights, obligations and responsibilities of certSIGN and the other PKI Participants, as defined in the Subscriber Agreement and by national law,
- That the Subscriber has the obligation to inform certSIGN of any changes or events that may affect the validity or the content of the certificate

Enrollment Process

The enrolment process begins at the RA.

The RA operator does the certificate request verification.

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

4.2 Certificate application processing

certSIGN accepts requests individually or collectively submitted. The requests may be sent *on-line* or *off-line*.

The certificate request is filled in electronic format:

- The certificate request is filled-in via pages on the certSIGN's website using the following address: https://www.certsign.ro. A Subscriber that visits the respective site fills in (in compliance with the instructions on the web site) a request form, and
  - Proceed with the online payment, identification and registration following the site instructions, or
  - Personally hand it to a RA or directly to the Certification Authority, or
  - Submits it using courier/ postal services to the CA, together with letter that shall contain copies of all original documents
- The request form filled in (received via e-mail or from the web site www.certsign.ro) is electronically signed with a valid (not revoked or expired) qualified digital certificate issued by CERTSIGN and sent to the Certification Authority via e-mail or an authenticated channel
- The certificate request may be filled in and posted on site: https://shop.certsign.ro/

The certificate request is filled in off-line:

- By Subscriber's personal attendance at the Registration Authority or at the Certification Authority, case when the request is filled in and hand signed. The Subscriber signs the agreement concerning certification services provided, or
- The Subscriber submits the filled in request, hand signed, using courier/ postal services to the CA, together with letter that shall contain copies of all original documents.

RA checks for CAA records and follow the processing instructions found, for each dNSName in the subjectAltName extension of the certificate to be issued, as specified in RFC 8659. certSIGN will NOT issue a certificate unless the certificate request is consistent with the applicable CAA Resource Record set.

If a CAA record exists, then it must list certSIGN as an authorized CA. The record allowed is certsign.ro and CAA "issue" or "issuewild" records are permitted.

4.2.1 Performing identification and authentication functions

The Registration Authority Officers performs identification and authentication according to the procedure defined in chapter 3.2, and within internal confidential documentation.
High Risk Certificate Request is a Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

CA uses the documents and data provided in Section 3.2 to verify certificate information, provided that the CA obtained the data or document from a source specified under Section 3.2 no more than twelve (12) months prior to issuing the Certificate.

The CA develops, maintains, and implements documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified.

To prevent High Risk Certificates issuance, prior to the Certificate's approval, the internal verification procedure require one or more the following actions:

- Careful examination of the FQDN to confirm whether the intent of Applicant is to imitate or mislead customers;
- Manual cross check and review of all information provided by the Subscriber;
- Request further documentation confirming control of the domain from the Applicant

and/or other verifiable proof as deemed necessary by the PPMB.
If a Delegated Third Party fulfills any of the CA's obligations under this section, the CA verifies that the process used by the Delegated Third Party to identify and further verify High Risk Certificate Requests provides at least the same level of assurance as the CA's own processes.

4.2.2 Approval or rejection of certificate applications

Approval or rejection of certificate applications is undertaken by the RA. The RA validates each request and may reject a certificate request if the request cannot be authenticated or if the request does not comply with the rules and standards governing CertSIGN Web CA or for other reasons, at the discretion of and under the responsibility of the RA.
Certificate requests are ultimately processed by the certSIGN CA system which validates each request and may reject a certificate request if the request cannot be authenticated or if the request does not comply with the rules and standards as defined for the type of certificate, at the discretion of and under the responsibility of certSIGN.
certSIGN does not issue certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name.
Entries in the dNSName is in the "preferred name syntax", as specified in RFC 5280, and thus MUST NOT contain underscore characters ("_").

4.2.3 Time to process certificate applications

certSIGN does not issue certificate immediately upon registration. Certificates have to be issued by the Certification Authority by approving the certificate request after it has been validated by RA, therefore the certificates are not immediately available to the Subscriber when the certificates are issued by the CA.

4.3 Certificate Issuance

After receiving and processing a request (see Chapters 4.1 and 4.2) the Certification Authority issues a certificate. After the certificate is issued, certSIGN publishes it in the corresponding repositories. The issued certificates' availability period depends on the certificate's type and the Subject's category and is compliant with the periods presented in Table 6.3.2.2.
certSIGN informs the Subscriber about the certificate issuance by sending an e-mail (at the address rendered by the Subscriber) information that allows the Subscriber to obtain the certificate.
Every certificate issued is published in certSIGN's Repository. The certificate publication is equivalent with the notification of other Relying Parties about the fact that a certificate was issued for a Subscriber.

4.3.1 CA actions during certificate issuance

The certificate is issued as part of the certificate enrolment process. The CA will only receive certificate requests from the RA. The CA, the RA and the personalization process are integrated systems and communicate over closed network connections. The CA only process requests that are originated from a trusted RA/DRA of certSIGN.
certSIGN implemented its own certificate Linting tool, that uses also external Linting tools, to test the technical conformity of each to-be-signed artifact prior to signing it.
For every certificate request, the CA will perform the following verifies and actions:

- Does the request originate from the RA?
- The CA verifies the requester's authorization for the type of request and refuse requests that pertain to certificate profiles for which the requester is not authorized.
- The CA also matches the certificate request against a pre-defined certificate profile. The variable information in the request shall match with the template and rule set of the certificate profile.
- The CA adds non-variable and variable information to the certificate, as defined in the specified certificate profile.
- The CA ensure the uniqueness of each certificate it issues using the certificate SerialNumber field of each certificate.

certSIGN Web CA implemented a Linting process to test the technical conformity of each to‐be‐signed artifact prior to signing it. The method used to produce a certificate containing the to‐be‐signed Certificate content is to sign the tbsCertificate with a "dummy" Private Key whose Public Key component is not certified by a Certificate that chains to a publicly‐trusted CA Certificate.

certSIGN Web CA uses a Linting process to test each issued Certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The certificate is issued as part of the certificate enrollment process. The Subscriber receives a notification of certificate issuance.

One month before the certificate expiration, the Subscriber is informed that the certificate is about to expire.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

When receiving a certificate the Subscriber is committed to verify its content, especially the data correctness and the complementariness of the public key with the private key he owns. If the certificate has any faults or mistakes that cannot be accepted by the Subscriber, the Subscriber will immediately inform the Certification Authority concerning the certification revocation.
The certificate is considered accepted in case of occurrence of the following events in term of maximum 3 calendar days from the date of the certificate receiving by the Subscriber:

- The explicit acceptance of the issued certificate at the moment of obtaining the certificate from certSIGN's site

If a certificate is not rejected in 3 calendar days from its receiving then the certificate is considered accepted.
Certificate acceptance is solely by the Subscriber, prior to its usage and its applying to any cryptographic operation through which it is considered that he accepted the terms and conditions specified in the present CPS, Certification Policy and Service providing agreement.
In case of electronic submission of the request, the solicitor automatically accepts the certificate at the moment of applying for this certificate.
By accepting the certificate, the Subscriber accepts the rules of the CPS and of the Certification Policy and agrees to follow the provisions of the agreement concluded with certSIGN.
The RA and the Subscriber have the right to reject the certificate provided at least one of the following objections applies:

- The information in the certificate is incorrect,
- The information in the certificate became invalid since the date of registration,
- Loss of entitlement of the Subscriber.

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

- The RA requests revocation of the certificates
- The RA executes the revocation of the certificate

4.4.2 Publication of the certificate by the CA

See chapter 2 -"PUBLICATION AND REPOSITORY RESPONSIBILITIES"

4.4.3 Notification of certificate issuance by the CA to other entities

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

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

certSIGN issues certificates for keys provided by the Subscribers in the certificate requests.

Subscribers shall protect their private keys from access by unauthorized personnel or other third parties.

Subscribers shall use private keys only in accordance with the usages specified in the key usage extension.

See Sections 1.4.1, 6.1.7 and 7.1.

4.5.2 Relying party public key and certificate usage

certSIGN assumes that all user software will be compliant with X.509, the SSL/TLS protocol, and other applicable standards that enforce the requirements and requirements set forth in this CPS. certSIGN does not warrant that any third party's software will support or enforce such controls or requirements, and all relying parties are advised to seek appropriate technical or legal advice.

Relying Parties shall use the public keys and certificates:

- In compliance with their stated purpose in the present CPS and in compliance with the certificate content (fields *keyUsage* and *extendedKeyUsage*),
- In compliance with the provisions of the agreement between the Subscriber and certSIGN,
- Only after verification of their status and verification of the Certification Authority's signature that issued the respective certificate.

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

4.6 Certificate Renewal

certSIGN allows CA certificates renewal only in special conditions, with PPMB approval.
certSIGN does not perform end-user SSL certificate renewal.

4.6.1 Circumstance for certificate renewal

Not stipulated.

4.6.2 Who may request renewal

Not stipulated.

4.6.3 Processing certificate renewal requests

Not stipulated.

4.6.4 Notification of new certificate issuance to subscriber

Not stipulated.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not stipulated.

4.6.6 Publication of the renewal certificate by the CA
Not stipulated.

4.6.7 Notification of certificate issuance by the CA to other entities
Not stipulated.

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

4.7.1 Circumstance for certificate re-key
certSIGN performs certificate rekey for the valid (not expired and not revoked) digital certificates Certsign issued, that require no changes of certificate data or extensions. The rekey process consists of re-issuing a certificate with a new key pair to extend its expiry date without changing the identity or other certificate extensions.

4.7.2 Who may request certification of a new public key
certSIGN allows the re-key process to be initiated by both the Subscriber of the certificate, or the CA / RA managing that appropriate certificate.

4.7.3 Processing certificate re-keying requests
The RA uses the same processes as for a newly requested certificate.

4.7.4 Notification of new certificate issuance to subscriber
The RA uses the same notification processes as for a newly requested certificate.

4.7.5 Conduct constituting acceptance of a re-keyed certificate
The RA uses the same processes as for a newly requested certificate.

4.7.6 Publication of the re-keyed certificate by the CA
The RA uses the same processes as for a newly requested certificate.

4.7.7 Notification of certificate issuance by the CA to other entities
The RA uses the same processes as for a newly requested certificate.

4.8 Certificate Modification
certSIGN allows CA certificates modification only in special conditions, with PPMB approval. certSIGN does not allow modification of end-user certificate details during the lifetime of the certificate. If any information on the certificate changes, the Subscriber must request revocation of the original certificate and request that a new certificate be issued.

4.8.1 Circumstance for certificate modification
Not stipulated.

4.8.2 Who may request modification
Not stipulated.

4.8.3 Processing certificate modification requests
Not stipulated.

4.8.4 Notification of new certificate issuance to subscriber
Not stipulated.

4.8.5 Conduct constituting acceptance of a modified certificate
Not stipulated.

4.8.6 Publication of the modified certificate by the CA
Not stipulated.

4.8.7 Notification of certificate issuance by the CA to other entities
Not stipulated.

4.9 Certificate revocation and suspension
Certificates issued by CertSIGN Web CA can be revoked but they are never suspended. Certificate revocation is irreversible.

The revocation affects neither the transactions made before the revocation, nor the obligations resulting from the following of the present CPS.
This chapter states the conditions necessary for a Certification Authority to have reasons to revoke the certificate.
If a private key corresponding to a public key contained in a revoked certificate stays under Subscriber's control, after revocation it should be safely stored until it is destroyed.
Short-lived certificates are not revoked. In case of short-lived certificates, the mechanism to notify problems is the same mechanism described in #1.5 at "Procedure for certificate problem reporting".

4.9.1 Circumstances for revocation
certSIGN will revoke a certificate within 24 hours and use the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

1. The Subscriber requests in writing, without specifying a CRLreason, that the CA revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL)
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization(CRLReason #9, privilegeWithdrawn);
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) (CRLReason #1, keyCompromise);
5. The CA obtains evidence that the validation of domain authorization or control for any FullyQualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).

certSIGN will revoke a certificate within 5 days and use the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

6. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 from BR (CRLReason #4, superseded);

7. The CA obtains evidence that the certificate was misused (CRLReason #9, privilegeWithdrawn);
8. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms and conditions (CRLReason #9, privilegeWithdrawn);
9. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);
10. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);
11. The CA is made aware of a material change in the information contained in the certificate (CRLReason #9, privilegeWithdrawn);
12. The CA is made aware that the certificate was not issued in accordance with CA/Browser Forum Baseline Requirements or certSIGN CPS (CRLReason #4, superseded);
13. The CA determines or is made aware that any of the information appearing in the certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
14. The CA's right to issue certificates under CA/Browser Forum Baseline Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
15. Revocation is required by the certSIGN Certification Practice Statement for a reason that is not otherwise required to be specified by this section (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);;
16. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

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

4.9.2 Who can request revocation

The following entities can send certificate revocation requests:

- The Subscriber who is the holder of the private key associated with the public key from the certificate
- The Subscriber who enters into a subscriber agreement with certSIGN for issuing certificates

- The Registration Authority that can request the revocation either on behalf of a Subscriber or if it has information that justifies the certificate revocation
- Trusted roles associated to CertSIGN Web CA, under the supervision of the Policies and Procedures Management Body (PPMB)

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

The revocation request may aim more certificates.

4.9.3 Procedure for revocation request

The CA maintains a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

The submission of the revocation request is described in chapter 3.4. The certificate revocation request shall precisely identify each certificate, shall contain the reason(s) for which the revocation is requested and shall be authenticated. The information about the revoked certificates is placed on the Certificate Revocation List issued by certSIGN Web CA. A certificate revocation request takes place as it follows:

- certSIGN verifies the revocation request, including that it is submitted by a legitimate entity. If the request is successfully verified, certSIGN Web CA places the information concerning the certificate revocation on the Certificate Revocation List (CRL);
- certSIGN notifies the Subscriber about the revocation or about the decision of request cancellation along with the reasons for this cancellation.
- If certSIGN determines that revocation is appropriate, certSIGN personnel revoke the Certificate and update the CRL.

4.9.4 Revocation request grace period

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

4.9.5 Time within which CA must process the revocation request

Within 24 hours after receiving a Certificate Problem Report, certSIGN will investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, certSIGN work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation will not exceed the time frame set forth in Section 4.9.1.1. certSIGN will consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);

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

certSIGN will revoke certificates after validating the revocation request following the guidelines of this section and Section 4.9.1.
As an exception, if the revocation request cannot be confirmed or validated within 24 hours, certSIGN will not revoke the certificate and the justification will be recorded.

4.9.6 Revocation checking requirements for relying parties

Relying Parties shall use all the resources that the certSIGN makes available through its repository to verify the status of a Certificate any time before relying on it. certSIGN updates OCSP, CRLs accordingly.

4.9.7 CRL issuance frequency

Every Certification Authority part of certSIGN issues different Certificate Revocation Lists. A new CRL is published in the Repository immediately after every certificate revocation, or within maximum one day. The CRL's availability period is of 48 hours and it is updated daily. The Certificate Revocation List (CRL) for certSIGN ROOT CA G2 Authority is issued at least yearly under the condition that there are no certificate revocations of one of the subordinate CA authorities.
In case of certificate revocation of an authority affiliated to certSIGN this certificate is immediately published in the Certificate Revocation List.

4.9.8 Maximum latency for CRLs

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

4.9.9 On-line revocation/status checking availability

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

OCSP responders operated by certSIGN support the HTTP GET method, as described in RFC 6960, process the Nonce extension (1.3.6.1.5.5.7.48.1.2) in accordance with RFC 8954, and provide an authoritative response no more than 15 minutes after the Certificate or Precertificate is first published.

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

For the status of Subscriber Certificates, the CA updates information provided via an Online Certificate Status Protocol at least every hour. OCSP responses from this service have a default maximum expiration time 24h.

For the status of Subordinate CA Certificates:

The CA updates information provided via an Online Certificate Status Protocol at least

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

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

certSIGN monitors the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.

The OCSP responder provides definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC6962]. A certificate serial number within an OCSP request is one of the following three options:

1. "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or

2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by (a) the Issuing CA; or (b) a Precertificate Signing Certificate [RFC6962] associated with the Issuing CA;

3. "unused" if neither of the previous conditions are met.

4.9.10 On-line revocation checking requirements
No Stipulation.

4.9.11 Other forms of revocation advertisements available
No Stipulation.

4.9.12 Special requirements related to key compromise
If a Subscriber knows or suspects that the integrity of his certificate's private key has been compromised, the Subscriber shall:

- Immediately cease using the certificate,
- Immediately initiate revocation of the certificate,
- Delete the certificate from all devices and systems,
- Inform all Relying Parties that may depend on this certificate.

The compromise of the private key may have implications on the information protected with this key. The Subscriber shall decide how to deal with the affected information before deleting the compromised key.
Acceptable methods that third parties may use to demonstrate private key compromise:
1. Perform the procedure described in Section 7.6 of RFC 8555 and sign the revocation request with the compromised private key.
2. Sign a challenge provided by certSIGN using the compromised private key.
3. Submit the private key itself.

4.9.13 Circumstances for suspension
Not stipulated

4.9.14 Who can request suspension
Not stipulated

4.9.15 Procedure for suspension request
Not stipulated

4.9.16 Limits on suspension period
Not stipulated.

4.10 Certificate status services

4.10.1 Operational characteristics
certSIGN's certificate status services are CRL and OCSP. Access to these services is made through the web site "www.certsign.ro" and "ocsp.certsign.ro". The certificate status services provide information on the status of valid certificates. The integrity and authenticity of the status information is protected by a digital signature of the respective CA. Revocation entries on a CRL or OCSP Response are not removed until after the Expiry Date of the Revoked Certificate.

4.10.2 Service availability
certSIGN operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of two seconds or less under normal operating conditions.

certSIGN maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

certSIGN maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

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

4.11 End of subscription
End of subscription occurs after:

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

For reasons of legal compliance, certSIGN and all registration authorities keep all Subscribers data and documentation for a period of 10 years after termination of a subscription.

4.12 Key escrow and recovery
certSIGN does not perform escrow or recovery of the subscriber private keys.

4.12.1 Key escrow and recovery policy and practices
Not stipulated.

4.12.2 Session key encapsulation and recovery policy and practices
Not stipulated.

5 Facility, Management and Operational Controls

This chapter describes general requirements concerning control, physical and organizational security, as well as personnel activity, used in certSIGN for example in the time of key generation, entity authenticity verification, certificate issuance and publication, certificate revocation, audit and backup copy creation.

As a certificate service provider, certSIGN places security at the core of its activities. In order to ensure that all of its assets, activities and services are secure, certSIGN has implemented, maintains and continuously improves an ISO 27001:2013 certified information security management system. In accordance with the requirements of this security framework, all security activities start with a risk assessment to identify and classify all the information assets, to evaluate the risks they are exposed to and to determine the required technical, managerial, organizational and procedural controls. certSIGN maintains an inventory of all information assets and assigns them a classification consistent with the risk assessment.

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

- ETSI EN 319 401, General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1, Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates
- CA/Browser Forum Network and Certificate System Security Requirements

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

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

The Certificate Management Process includes:

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

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

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes;
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

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

5.1 Physical Controls

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

5.1.1 Site location and construction

certSIGN CA is located in Bucharest, Romania, at the following address: 29 Tudor Vladimirescu Avenue, AFI Tech Park 1, Bucharest, Romania.

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;Equipment is correctly maintained to ensure its continuous availability and integrity.

5.1.2 Physical access

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

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

Visitors are permanently escorted by the authorized personnel.

certSIGN premises are divided into:

- Office areas,
- IT areas,
- CA operators area
- RA operators and administrators area,
- Developing and testing area.

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

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

The *developing and testing area* is protected in a manner similar to the protection of the operators and administrators area. Unattended individuals are not allowed in this area. Programmers and developers do not have access to sensible information. If such access is necessary, the presence of the security administrator is required. Projects being implemented and their software are tested on the development environment of certSIGN.

5.1.3 Power and air conditioning

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

5.1.4 Water exposure

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

After the retention period expires, paper and electronic media containing information significant for certSIGN security are destroyed. Security hardware modules are destroyed in compliance with the manufacturer's recommendations.

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

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

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

5.1.8 Off-site backup

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

Offsite storage comprises also archives, current copies of information processed by the system and installation kits of certSIGN applications. It enables emergency recovery of every certSIGN function within 48 hours in certSIGN's disaster recovery location.

5.2 Procedural controls

5.2.1 Trusted roles

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

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

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

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

security administration and operation functions, are provided. Particularly, the use of system utility programs is restricted and controlled.

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

- **Security officer** – Overall responsibility for the implementation of the security practices and policies.
- **System administrator** – Authorized to install, configure and maintain the Certification Authority's trustworthy systems for registration, certificate generation, subject device provision and revocation management. Installs hardware and operating systems; installs and configures the network equipment.
- **System operator** – Responsible for operating the Certification Authority's trustworthy systems on a day to day basis. Authorized to perform system backup and recovery. Has access to Subjects' certificates; revokes Subjects' certificates; provides continuity of backup copies and archives of database and system logs creation; manages databases; has access to confidential information about Subjects/ Subscribers but is not allowed to physically access any other system resources; transfers archive copies and current backup copies to the designated premises.
- **Registration Officers**: Responsible for verifying information that is necessary for certificate issuance and approval of certification requests;
- **Revocation Officers:** Responsible for operating certificate status changes;
- **System Auditor** – Authorized to access archives and audit logs of the Certification Authority's trustworthy systems. Responsible for performance of internal audit, compliance of a Certification Authority with this CPS; this responsibility extends also to the Registration Authority, operating within certSIGN.

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

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

5.2.2 Number of persons required per task

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

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

5.2.3 Identification and authentication for each role

certSIGN personnel are subject to identification and authentication procedure in the following situations:

- Placement on the list of persons allowed to access certSIGN locations,
- Placement on the list of persons allowed to physically access system and network resources of certSIGN,
- Issuance of confirmation authorizing to perform the assigned role,
- Assignation of an account and a password in certSIGN information system.

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

Every assigned account:

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

Operations performed in certSIGN that require access through shared network resources are protected with implemented mechanisms of strong authentication and encryption of transmitted information.

All certSIGN personnel involved in providing the certification services are identified and authenticated before using critical applications related to those services. Particularly, HSM administrators and operators and CA and RA operators are issued a credential (digital certificates on tokens or HSM smartcards) in order to ensure strong identification and authentication (two-factor) prior to being allowed to perform any trusted action. All cryptographic credentials are stored securely in individual boxes.

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

5.2.4 Roles requiring separation of duties

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

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

5.3 Personnel controls

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

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

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

5.3.1 Qualifications, experience and clearance requirements

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

5.3.2 Background check procedures

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

5.3.3 Training requirements

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

- Requirements of Certification Practice Statement,
- Procedures and security controls employed by the Certification Authority and the Registration Authority
- basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures
- Common threats to the information verification process (including phishing and other social engineering tactics), and CA/B Forum Baseline Requirements
- Responsibilities arising from roles and tasks performed in the system,

Upon completion of the training, participants sign a document confirming their familiarization with Certification Practice Statement, other relevant documentation and acceptance of associated restrictions and obligations.

The CA ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. CA documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the CPS and the CA/B Forum Baseline Requirements.

5.3.4 Retraining frequency and requirements

Trainings described in Chapter 5.3.3 have to be repeated or supplemented always in situations when significant modification to certSIGN or its Registration Authority operation is executed.

All personnel in Trusted Roles maintains skill levels consistent with the certSIGN training and performance programs.

5.3.5 Job rotation frequency and sequence

No Stipulation.

5.3.6 Sanctions for unauthorized actions

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

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

5.3.7 Independent contractor requirements

Contract personnel (external service, developers of subsystems or applications, etc.) are subjected to the same verification procedure as employees of certSIGN (see Chapters 5.3.1, 5.3.2, 5.3.3 and 5.4.1). Additionally, when performing their task at certSIGN premises, contract personnel have to be escorted by a certSIGN employee, except those who have been cleared by the security officer and who can access internal classified information or in compliance with the laws in force.

5.3.8 Documentation supplied to personnel

certSIGN provides to personnel access to the following documents:

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

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

5.4 Audit logging procedures

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

Whenever possible the logs are created automatically. If this is not possible logs on paper will be used. Each record in a log created either automatically or by hand is preserved or disclosed during an audit, if required. The time accuracy of logs is ensured by three time servers. Two of them use as a reference time source GPS satellites and one is synchronized with the system that provides the official time of Romania (NIMB). The time used to record events as required in the audit log are synchronized with UTC at least once a day.

5.4.1 Types of events recorded

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

- **System logs** – contain information about customer's requests and server's responses (or vice versa) at the level of the network protocol (for example http, https); the recorded data is: IP address of the station or server, performed

operations (for example: searching, editing, writing etc.) and their results (for example the successful entry of a record in the database),
- **Errors** – contain information about errors at the network protocols level and at the applications' modules level;
- **Audit logs**– contain information specific for the certification services, for example: registration and certification request, rekey request, certificate acceptance, certificate issuing and CRL etc.

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

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

The CA record at least the following events:

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

Every automatic or manual recording contains the following information:

- Event type,

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

Logging of router and firewall activities at a minimum include:

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

All registration information, including the following, is recorded:

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

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

The privacy of subject information is maintained.

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

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

The archived journals of logs are kept at least 10 years.

The CA and each Delegated Third Party retain:

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

5.4.4 Protection of audit log

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

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

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

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

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

5.4.7 Notification to event-causing subject

Not stipulated.

5.4.8 Vulnerability assessments

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

In order to ensure that all of its assets, activities and services are secure, certSIGN has implemented, maintains and continuously improves an ISO 27001:2013 certified information security management system. In accordance with the requirements of this security framework, all security activities start with a risk assessment to identify and classify all the information assets, to evaluate the risks they are exposed to and to determine the required technical, managerial, organizational and procedural controls. certSIGN maintains an inventory of all information assets and assigns them a classification consistent with the risk assessment.

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

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

5.5 Records archival

It is required that all data and files related to registration of information associated with the system security, requests submitted by Subscribers, information about Subjects/ Subscribers, issued certificates and CRL's, keys used by Certification and Registration Authorities, and whole correspondence between certSIGN and the Subscribers should be subjected to archive.

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

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

Backup copies are created and retained outside certSIGN location.

5.5.1 Types of data archived

The following data are subjected to a trustworthy archive:

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

5.5.2 Retention period for archive

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

5.5.3 Protection of archive

certSIGN ensures:

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

Archives are accessible only to the authorized personnel.

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

certSIGN ensures that the precise time of archiving all events, records and documents mentioned above is recorded. This is accomplished through synchronization of all systems with the time servers. The time accuracy of logs is ensured by a time server that is synchronized with at least two time sources that can be GPS satellites or UTC (NIMB).

5.5.6 Archive collection system (internal or external)

certSIGN archive collection systems are internal.

5.5.7 Procedures to obtain and verify archive information

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

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

5.6 Key Changeover

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

5.7 Compromise and Disaster Recovery

This Chapter describes procedures carried out by certSIGN in abnormal situations (including natural disasters) to restore a guaranteed service level. Such procedures are executed in accordance with the accepted Business continuity and disaster recovery plan.

5.7.1 Incident and compromise handling procedures

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

The security incident management procedure also specifies how to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity

that has a significant impact on the trust service provided and/or on the personal data maintained therein within 24 hours of the breach being identified.

In case of security incident, internal procedures are used. The procedures include the notification of Application Software Suppliers, certSIGN's auditors, and the Supervisory body, the National CSIRT or other competent authorities.

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

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

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

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

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

certSIGN CA maintains a comprehensive and actionable plan for mass revocation events, performs annual testing of its procedures, and incorporates lessons learned to improve preparedness over time.

5.7.2 Computing resources, software and/or data are corrupted

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

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

To prevent or limit results of the above threats:

- The Security Policy of certSIGN includes a Business continuity and Disaster Recovery Plan,
- In the case of corruption restraining certSIGN functionality, within 48 hours an emergency facility will be activated, which should substitute all significant function of a Certification Authority until the services of the primary facility are restored. The

distance between the primary and the emergency facilities is large enough to avoid that the potential disasters occurring at the primary site could also affect the emergency site.

- Installation of updated software version in production is possible only after carrying out intensive tests on a testing environment, performed in strict accordance with disclosed procedures. Every modification in the system requires certSIGN security administrator's acceptance.
- certSIGN systems use applications for creating backup copies of data, allowing system recovery at any moment and audit to be performed. Backup copies include all the relevant data from security point of view.

All the systems from the IT infrastructure used to provide certification and timestamp services are continuously monitored and all the security events are logged and analyzed. Abnormal system activities that indicate a potential security violation, including intrusion into the systems and network are detected and reported as alarms to enable certSIGN to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

The sensitivity of any information collected or analyzed is taken into account by protecting it from unauthorized access.

In order to detect any discontinuity in the monitoring operations, the start-up and shutdown of the logging functions is also monitored

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

certSIGN addresses any critical vulnerability not previously addressed, within a period of 48 hours after its discovery. certSIGN prepares and implements a mitigation plan for the new vulnerabilities, if this is cost effective compared to their impact, or documents the decision that the vulnerability does not require remediation.

5.7.3 Entity private key compromise procedures

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

In case of CA private key compromise or suspicion of such compromise the following actions will also be taken:

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

- If a Certificate is revoked because of CA key compromise, certSIGN Root CA G2 will issue a new CRL within 24 hours after receiving notice of the compromise and publish online CRLs immediately.

When a private key associated to a public key from the certificate was compromised or there is a serious reason to suspect it was compromised, the Subscriber shall request Certsign to revoke the certificate.

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

5.7.4 Business continuity capabilities after a disaster

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

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

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

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

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

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

5.8 CA or RA termination

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

Requirements associated to duty transition

Before Certification Authority ceases its activity, it will:

- Inform (at least 30 days in advance) the following about the decision to terminate its services: all Subjects/ Subscribers who hold active (unexpired and unrevoked) certificates issued by this authority and other entities with which certSIGN has

agreements or other form of established relations, among which relying parties, other trust service providers and relevant authorities such as supervisory bodies. In addition, this information will be made available to other relying parties;
- Revoke the unexpired certificates that have been issued.
- Transfer its obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the certification services for a reasonable period, unless it can be demonstrated that certSIGN does not hold any such information. The information refers to registration information, revocation status for unexpired certificates that have been issued and event log archives for their respective period of time as indicated to the Subscriber and relying party;
- Destroy CA private keys, including backup copies, or withdraw them from use, in such a manner that the private keys cannot be retrieved;
- Where possible, make arrangements to transfer provision of certification services for the existing customers to another certification service provider.

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

In case certSIGN will terminate its activities without a partially or full transfer of its activities, it will revoke the impacted certificates one month after having notified Subscribers and will initiate the termination procedure for the contracts signed with the implied partners and/or supliers.

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

Certificate issuance by the successor of terminated Certification Authority

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

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

The archive of the Certification Authority ceasing its service has to be turned over to the primary Certification Authority – certSIGN ROOT CA G2 (in the case of termination of services of the certSIGN Web CA) or to the institution that the contract was signed with (in the case of termination of services of certSIGN ROOT CA G2).

5.9 Supply chain

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

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

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

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

6 Technical security controls

6.1 Key pair generation and installation

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

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

certSIGN Web CA owns at least one certificate signed by certSIGN ROOT CA G2. The private key corresponding to the public key contained in the certificate is used exclusively to sign the public keys of the Subjects and the Certificate Revocation List necessary for the functioning of the CA.

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

6.1.1 Key pair generation

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

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

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

The CA:

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

The keys of certSIGN Web CA are undertaken in a physically secured environment by personnel in trusted roles under, at least, dual control and split knowledge:

- At least three employees in trusted roles
- The security officer

- At least one representative of Policies and Procedures Management Body (PPMB)
- A Master of Key Ceremony
- At least one independent and external Qualified Auditor

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

Actions executed while performing key pair generation are recorded, dated and signed by each person present during the generation. The records are retained for the needs of audits and common system reviews.

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

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

Before expiration of its CA certificate which is used for signing subject keys, the CA will generate a new certificate for signing subject key pairs and will apply all the necessary actions to avoid disruption to the operations of any entity that may rely on the CA certificate. The new CA certificate will also be generated and distributed in accordance with this CPS. These operations should be performed with a suitable time range between the certificate expiry date and the last certificate signed to allow all parties that have relationships with certSIGN (subjects, subscribers, relying parties, CAs higher in the CA hierarchy, etc.) to acknowledge this key changeover and to implement the required operations in order to avoid any inconvenience and malfunction. This does not apply to the case in which we would cease our operations before our own certificate-signing or certificate expiration date.

The Subscriber's keys are generated by the Subscriber, by means of software applications or cryptographic devices. The CA rejects a certificate request if one or more of the following conditions are met:

- the Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6
- There is clear evidence that the specific method used to generate the Private Key was flawed;
- The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
- The CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;
- The CA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

If the Subscriber Certificate contains an extKeyUsage extension containing either the values id-kp-serverAuth or anyExtendedKeyUsage, the CA will NOT generate a Key Pair on behalf of the Subscriber, and will NOT accept a certificate request using a Key Pair previously generated by the CA.

6.1.2 Private key delivery to subscriber

We do not perform private key delivery to subscriber due to fact that private key is generated only by Subscriber.

6.1.3 Public key delivery to certificate issuer

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

6.1.4 CA public key delivery to relying parties

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

The public keys of a Certification Authority issuing certificates to Subjects are distributed solely under the form of certificates complying with the ITU-T X.509 v.3 recommendations.

CA publishes its certificates by placing them in the publicly available repository of certSIGN: https://www.certsign.ro/resources/chain-of-trust-g2

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

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

6.1.5 Key sizes

CertSIGN Web CA uses a 4096 bit key for certificates and CRL signing.

The digital certificates issued by certSIGN Web CA use 2048, 3072 or 4096 bit RSA keys.

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

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

6.1.6 Public Keys parameters generation and quality checking

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

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

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

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

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

a. digitalSignature: certificate intended for electronic signature verification,
b. nonRepudiation: certificate intended to provide a non-repudiation service by private individuals, as well as for purposes other than those described under f) and g). NonRepudiation bit may be set only in a public key certificate intended to verify

electronic signatures and should not be combined with the purposes described at points c)-e) and connected with providing confidentiality,

c. keyEncipherment: intended to encrypt symmetric algorithm keys, providing data confidentiality,
d. dataEncipherment: intended to encryption of Subject's data, other than those described in c) and e),
e. keyAgreement: intended for protocols of key exchange,
f. keyCertSign: public key is used for electronic signature verification in certificates issued by entities providing certification services,
g. cRLSign: public key is used for verification of electronic signatures on revoked and suspended certificates lists issued by entities that provide certification services,
h. encipherOnly: may be used solely with keyAgreement bit to indicate its purpose of data encryption in key exchange protocols,
i. decipherOnly: may be used solely with keyAgreement bit to indicate its purpose of data decryption in key exchange protocols

The private key of certSIGN Web CA is used only in the following cases:

1. Certificates for end-users;
2. Certificates for infrastructure purposes (OCSP Response verification certificates);

6.2 Private Key protection and Cryptographic Module Engineering Controls

Every Subscriber, Certification Authority operator and Certification Authority generates and stores his/her/its private key employing a reliable system that prevents private key loss, disclosure, modification or unauthorized access.

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

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

- ETSI EN 319 401

- ETSI EN 319 411-1

- CA/B Forum Baseline Requirements

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

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

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

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

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

6.2.1 Cryptographic module standards and controls

CA key pair generation is carried out within a secure cryptographic device which is a trustworthy system complying at least with FIPS 140-2 level 3 or Common Criteria EAL 4 standards

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

Multi-person control of a private key applies to private keys of CA used for certificate and CRL signing.

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

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

Acceptance of secret shared by its holders

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

Protection of shared secret

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

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

Availability and erasure (transfer) of the shared secret

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

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

Responsibilities of shared secret holder

The shared secret holder should perform his/her duties and obligations according to the requirements of this Certification Practice Statement and in a deliberate and responsible manner in any possible situation. A shared secret holder should notify the issuer of the shared secret in case of theft, loss, unauthorized disclosure or security violation immediately after

the incident occurrence. A shared secret holder cannot be accused of neglecting his/her duties due to reasons that are beyond his/her control. On the other hand, he is responsible for inappropriate disclosure of the secret or for omitting to notify the issuer of the secret about the security violation of the secret, resulting from the holder's mistake, negligence or irresponsibility.

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

6.2.3 Private Key escrow

Private keys of Certification Authorities are not subject to custody.

Subscriber's private keys are not subject to custody.

6.2.4 Private Key backup

CA creates a backup copy of their private key. Copies are used in case of execution of standard or emergency key recovery procedure (e.g. after disaster). When outside the secure cryptographic device the CA private key is protected in a way that ensures the same level of protection as provided by the secure cryptographic device. The copies of the private keys are protected by shared secrets.

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

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

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

6.2.5 Private Key archival

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

6.2.6 Private Key transfer into or from a cryptographic module

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

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

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

Introducing a private key into a security hardware module of the CA requires the restoration of the key on HSM in the presence of a corresponding number of shared secret owners that

protect the module containing the private keys. Due to the fact that the CA can retain an encrypted copy of its private key, the keys may also be transferred between modules.

If CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the CA, then the certSIGN ROOT CA G2 revokes all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7 Private key storage on cryptographic module

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

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

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

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

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

Operators use qualified electronic signature creation devices (tokens/cards) that comply minimum with FIPS 140-2 level 3 or Common Criteria EAL 4. Keys are always generated on the devices and never leave them. The secure devices are protected from producers to certSIGN, on storage while at certSIGN and while distributed.

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

6.2.8 Method of activating the private key

All private keys of CA are entered into the module after their generation, import in an encrypted form from another module or after restoration from shared secrets. Activation of private keys is always preceded by the operator's authentication. The authentication is carried out on the basis of a cryptographic card held by the operator. After the card is inserted into the cryptographic module and after typing the PIN number, the private key remains active until the card is removed from the module.

6.2.9 Method of deactivating private key

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

6.2.10 Method of destroying private key

At the end of their lifetime, the CA private keys are destroyed by trusted CA roles in the presence of more than one representative of the Policies and Procedures Management Body (PPMB) in order to ensure that these private keys can never be retrieved or used again.

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

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

Every private key destruction is recorded in the event journal.

The Subscriber is responsible to destroy the private key.

6.2.11 Cryptographic Module Rating
See above.

6.3 Other aspects of key pair management
certSIGN uses appropriately the CA private signing keys and does not use them beyond the end of their life cycle.

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

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

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

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

6.3.1 Public key archival
certSIGN archives its own CA public keys and all the public keys certified by certSIGN Web CA in the form of X509 certificate containing the key.

See chapter 5.5 for archival conditions.

6.3.2 Certificate operational periods and key pair usage periods
Usage period of public keys is defined by the value of the field validity of every public key certificate. It is also a validity period of a private key. The maximal usage period of Subscriber's keys cannot exceed twice the life period of a certificate, which period is mentioned below.

Standard values of maximal usage period of Certification Authority certificates are described in Table 6.3.2.1, while Subscriber's certificates are presented in Table 6.3.2.2.

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

Generally, beginning date of the certificate validity period complies with the date of its issuance. It is not allowed to set this date in the future or in the past.

Key owner	Main purpose of key usage
	RSA for certificate and CRL signing
certSIGN Web CA	10 years

Table 6.3.2.1 Maximum usage period of CA certificates

Key owner	Certification Policy	Main key usage
Legal entities	certSIGN Web	397 days[1]

Table 6.3.2.2. Maximum usage periods of Subscriber's certificates

Re-use of validation information is limited to the lifetime of the issued certificate.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data are used in two basic cases:

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

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

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

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

[1] *From March 15, 2026 maximum duration is 200 days; From March 15, 2027 it is reduced to 100 days.*

6.4.2 Activation data protection

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

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

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

6.4.3 Other aspects of activation data

No Stipulation.

6.5 Computer security controls

This chapter describes certSIGN's computer security controls.

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

6.5.1 Specific computer security technical requirements

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

Computers are configured with the following security mechanisms:

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

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

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

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

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

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

6.5.2 Computer security rating

certSIGN computer system complies with requirements described in ETSI EN 319 411-1.

6.6 Life cycle technical controls

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

6.6.1 System development controls

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

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

Similar rules apply to hardware components replacement, as follows:

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

6.6.2 Security management controls

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

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

6.6.3 Life cycle security controls

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

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

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

certSIGN implements internal security procedures for ensuring that:

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

The reasons for not applying any security patches are documented.

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

6.7 Network security controls

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

a) our systems are segmented into networks or zones based considering functional, logical, and physical (including location) relationship between trustworthy systems and services. certSIGN applies the same security controls to all systems co-located in the same zone.
b) access and communications between zones are restricted to those necessary for the operation of certification services. Not needed connections and services are explicitly forbidden or deactivated. The established rule set is reviewed on a regular basis.
c) all systems that are critical to the certification services operation are kept in one or more secured zone(s)
d) Dedicated network for administration of IT systems and operational network are separated. Systems used for administration of the 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 only established through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.
f) If a high level of availability of external access to a specific certification service is required, the external network connection is redundant to ensure availability of the services in case of a single failure.
g) a regular vulnerability scan on public and private IP addresses identified by certSIGN is performed and evidence is recorded that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.
h) certSIGN certification services undergo a penetration test on the related systems at set up and after infrastructure or application upgrades or modifications that certSIGN determines are 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), devised in more sub-networks provided with controlled access. Access from the Internet to any segment is protected by means of intelligent firewall.

Security controls are developed on the basis of firewall and traffic filtering on the routers and Proxy services that protect certSIGN's internal network domains from unauthorized access including access by Subjects/ Subscribers and third parties. Firewalls are configured to prevent all protocols and accesses not required for the operation of certSIGN CA.

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

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

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

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

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

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

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

6.8 Time-stamping

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

7 Certificate, CRL and OCSP profile

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

7.1 Certificate profile

certSIGN Web CA meets the technical requirements set forth in CABF BR Section 2.2 - Publication of Information, Section 6.1.5 - Key Sizes, and Section 6.1.6 - Public Key Parameters Generation and Quality Checking.
SerialNumber field is a non - sequential number greater than zero (0) and less than 2159 containing at least 64 bits of output from a CSPRNG.
All objects signed by a certSIGN CA Private Key conform to the CABF BR #7.1.3.2, RSA or ECDSA requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier - derived type in the context of signatures.
The SubjectPublicKeyInfo field indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier, with an explicit NULL parameter.
The AlgorithmIdentifier for RSA keys is byte - for - byte identical with the following hex - encoded bytes: 300d06092a864886f70d0101010500.
For ECDSA, the identifiers and encodings specified in #7.1.3.2 from CABF BR will be used.

TLS Subordinate CA Certificate Profile
All subject names are encoded as specified in Section 7.1.4 and contain the AttributeTypes following #7.1.2.10.2 "CA Certificate Naming" from CABF BR.
Profile of basic fields for certSIGN Web CA certificate is described in Table 7.1.

Field name	Value or value's constraint	
Version	3	
Serial Number	10034b8e66f50920f6c5	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Department (OU)=	certSIGN ROOT CA G2
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Not before (validity period beginning date)	Feb 6 10:18:16 2017 GMT	
Not after (validity period end date)	Feb 6 10:18:16 2027 GMT	
Subject (Distinguished Name)	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-18288250
	Common Name (CN) =	certSIGN Web CA
	Organization (O) =	certSIGN SA
	Country (C) =	RO

Subject Public Key Info	4096 bits RSA key
Signature	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)

Table 7.1. Profile of the basic fields for certSIGN Web CA

Subscriber (Server) Certificate Profile

The notBefore field has a value within 48 hours of the certificate signing operation.
All subject names are encoded as specified in Section 7.1.4 and contain the AttributeTypes following #7.1.2.7.2 "Domain Validated" from CABF BR.
Subscriber Certificate Common Name Attribute contain exactly one entry that is one of the values contained in the Certificate's subjectAltName extension, encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name will be encoded as LDH Labels, and P-Labels will NOT be converted to their Unicode representation.

Profile of basic fields for end-user DV certificates issued by certSIGN Web CA is described in Table 7.2.

Field name	Value or value's constraint	
Version	Version 3	
Serial Number	Unique value greater than zero (0) for all certificate issued by Certification Authorities within certSIGN. Serial numbers are constructed using a database constrained unique incremental prefix which is concatenated to a 8 bytes random sequence. A hardware cryptographic module is used for generating the random value.	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-18288250
	Common Name (CN) =	certSIGN Web CA
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Not before (validity period beginning date)	Universal Time Coordinated based.	
Not after (validity period end date)	Universal Time Coordinated based.	
Subject (Distinguished Name)	Encoded in accordance with RFC 5280, may contain fields presented in Chapter 7.1.4.	
Subject Public Key Info	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key).	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.	

Table 7.2. Profile of the basic fields of DV certificates issued by certSIGN Web CA

Precertificate Profile

A Precertificate appears structurally identical to a end-user DV Certificate, with the exception of a special critical poison extension in the extensions field, with the OID of 1.3.6.1.4.1.11129.2.4.3, and is created after a CA has decided to issue a Certificate, but prior to the actual signing of the Certificate.

The basic fields of the precertificate:

- **version** Encoded value is byte-for-byte identical to the version field of the Certificate
- **serialNumber** Encoded value is byte-for-byte identical to the serialNumber field of the Certificate (as an exception to RFC 5280, Section 4.1.2.2)
- **signature** Encoded value is byte-for-byte identical to the signature field of the Certificate
- **issuer** Encoded value is byte-for-byte identical to the issuer field of the Certificate
- **validity** Encoded value is byte-for-byte identical to the validity field of the Certificate
- **subject** Encoded value is byte-for-byte identical to the subject field of the Certificate
- **subjectPublicKeyInfo** Encoded value is byte-for-byte identical to the subjectPublicKeyInfo field of the Certificate
- **issuerUniqueID** Encoded value is byte-for-byte identical to the issuerUniqueID field of the Certificate, or omitted if omitted in the Certificate
- **subjectUniqueID** Encoded value is byte-for-byte identical to the subjectUniqueID field of the Certificate, or omitted if omitted in the Certificate

Field name	Value or value's constraint for Precertificates	
Version	Version 3	
Serial Number	Unique value greater than zero (0) for all certificate issued by Certification Authorities within CERTSIGN. It contains a random value of 8 bytes. A hardware cryptographic module is used for generating this value.	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Common Name (CN) =	certSIGN Web CA
	OrganizationIdentifier =	VATRO-18288250
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Not before	Universal Time Coordinated based.	
Not after	Universal Time Coordinated based.	
Subject (Distinguished Name)	Encoded in accordance with RFC 5280, contains countryName and commonName fields.	
Subject Public Key Info	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key).	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.	

OCSP Responder Certificate Profile

The Issuing CA of the Responder is the same as the Issuing CA for the Certificates it provides responses for.

Field name	Value or value's constraint for OCSP Responder	
Version	Version 3	
Serial Number	Unique value greater than zero (0) for all certificate issued by Certification Authorities within CERTSIGN. It contains a random value of 8 bytes. A hardware cryptographic module is used for generating this value.	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Common Name (CN) =	certSIGN Web CA
	OrganizationIdentifier =	VATRO-18288250
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Not before	Universal Time Coordinated based.	
Not after	Universal Time Coordinated based.	
Subject (Distinguished Name)	Encoded in accordance with RFC 5280, contains countryName and commonName fields.	
Subject Public Key Info	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key).	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.	

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

The certificates profiles extensions are according to CABF BR # 7.1.2 "Certificate Content and Extensions".

TLS Subordinate CA Certificate Profile Extensions

The ***AuthorityInfoAccess*** contain one or more AccessDescriptions. Each AccessDescription only contains a permitted accessMethod, and each accessLocation is encoded as the specified GeneralName type.

Authority Key Identifier extension have only the ***keyIdentifier*** field, identical to the subjectKeyIdentifier field of the Issuing CA.

CA Certificate ***Basic Constraints***: cA set TRUE; pathLenConstraint set to 0 or NULL.

Certificate Policies extension contains at least one PolicyInformation and it contain exactly one Reserved Certificate Policy Identifier – for CA certificates issued after 2023.

The ***CRL Distribution Points*** extension contains at least one DistributionPoint, of type uniformResourceIdentifier, and the scheme of each is "http". The first GeneralName contains the HTTP URL of the Issuing CA's CRL service for the CA certificate.

certSIGN CA generates a ***subjectKeyIdentifier*** that is unique within the scope of all Certificates it has issued for each unique public key.

For CA certificates issued after 2023 - the CA Certificate ***Extended Key Usage*** contains id-kp-serverAuth key, and optionally id-kp-clientAuth.

Certificate extensions for certSIGN Web CA are described in Table 7.3.

Extension	Value or Value constraint	Extension status
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.certsign.ro/certcrl/certsign-rootg2.crt	Non-critical
Basic Constraints	Subject type=CA, Path length constraint=0	Critical
Key Usage	keyCertSign (bit 5), cRLSign (bit 6)	Critical
Authority Key Identifier	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	Non-critical
Subject Key Identifier	65 29 2b 19 2b 5a 41 d3 01 62 9b 7b 47 00 e2 18 08 71 c3 41	Non-critical
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=All issuance policies[2] [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution Points	http://crl.certsign.ro/certsign-rootg2.crl	Non-critical
Extended Key Usage[3]	Server Authentication (1.3.6.1.5.5.7.3.1)	Non-critical

Table 7.3. Extensions of certSIGN Web CA certificate

Subscriber (Server) Certificate Profile Extensions

The ***AuthorityInfoAccess*** contain one or more AccessDescriptions. Each AccessDescription only contains a permitted accessMethod, and each accessLocation is encoded as the specified GeneralName type.

Authority Key Identifier extension have only the ***keyIdentifier*** field, identical to the subjectKeyIdentifier field of the Issuing CA.

Certificate Policies extension contains at least one PolicyInformation and it contain exactly one Reserved Certificate ***Policy Identifier***:

*{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)}(**2.23.140.1.2.1**)*

The permitted ***policyQualifiers,*** id-qt-cps (OID: 1.3.6.1.5.5.7.2.1), HTTP or HTTPS URL for the Issuing CA's Certification Practice Statement.

The end-user DV Certificate ***Extended Key Usage*** contains id-kp-serverAuth key, and optionally id-kp-clientAuth.

[2] *certSIGN will replace current Web CA certificate with a new one that may have Policy Identifier: 2.23.140.1.2.1.*

[3] *For new Intermediate CAs dedicated to issuing TLS certificates this extension will be added*

The ***Subject Alternative Name*** is present and contains at least one dNSName. dNSName contains either a Fully-Qualified Domain Name or Wildcard Domain Name that the CA has validated in accordance with CABF BR Section 3.2.2.4. Wildcard Domain Names are validated for consistency with CABF BR Section 3.2.2.6. The dNSName entry does not contain an Internal Name. The Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name contained in the entry is composed entirely of P-Labels or Non-Reserved LDH Labels joined together by a U+002E FULL STOP (".") character. The zero-length Domain Label representing the root zone of the Internet Domain Name System is NOT included.
Key Usage values: digitalSignature and keyEncipherment.
The ***CRL Distribution Points*** extension contains at least one DistributionPoint, of type uniformResourceIdentifier, and the scheme of each is "http". The first GeneralName contains the HTTP URL of the Issuing CA's CRL service for the CA certificate.

End User DV SSL certificate contains extensions described in Table 7.4.

Extension	Value or Value constraint	Extension status
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.certsign.ro/certcrl/certsign-webca.crt	Non-critical
Key Usage	digitalSignature (bit 0), Key Encipherment (bit 2)	Critical
Authority Key Identifier	65 29 2b 19 2b 5a 41 d3 01 62 9b 7b 47 00 e2 18 08 71 c3 41	Non-critical
Subject Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	Non-critical
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=2.23.140.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.6 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.3.1.4.5 [3,1]Policy Qualifier Info: Policy Qualifier Id=CPS	Non-critical

Extension	Value or Value constraint	Extension status
	Qualifier: http://www.certsign.ro/repository	
CRL Distribution Points	http://crl.certsign.ro/certsign-webca.crl	Non-critical
Subject Alternative Name	This extension MUST contain at least one entry. Each entry is either a DNS Name containing the Fully-Qualified Domain Name. Wildcard FQDNs are permitted.	Non-critical
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Non-critical

Table 7.4. DV SSL certificate extensions

Precertificate Profile Extensions

The Precertificate contains the Precertificate Poison extension (OID:1.3.6.1.4.1.11129.2.4.3). This extension has an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.

OCSP Responder Certificate Profile Extensions

Authority Key Identifier extension have only the ***keyIdentifier*** field, identical to the subjectKeyIdentifier field of the Issuing CA.

OCSP Responder Extended Key Usage is only OCSP Signing (1.3.6.1.5.5.7.3.9).certSIGN CA includes the ***id-pkix-ocsp-nocheck*** extension (OID: 1.3.6.1.5.5.7.48.1.5).

This extension has an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6960, Section 4.2.2.2.1.

OCSP Responder ***Key Usage*** is only digitalSignature.

subjectAltName, authorityInformationAccess, certificatePolicies, crlDistributionPoints are not set as extensions for OCSP certificates issued after 2023.

OCSP certificate contains extensions described in Table 7.5.

Extension	Value or Value constraint	Extension status
Authority Info Access[4]	[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-webca.crt	Non-critical

[4] Prohibited for certificated issued after 15-Sep-2023

Extension	Value or Value constraint	Extension status
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1)[1]	Critical
Authority Key Identifier	65 29 2b 19 2b 5a 41 d3 01 62 9b 7b 47 00 e2 18 08 71 c3 41	Non-critical
Subject Key Identifier	3c 76 7c 4a 3c 2d 6c 5a 82 c0 2d 62 f9 2e 17 89 e5 55 f0 b6	Non-critical
Certificate Policies[1]	Certificate Policies [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.3.1.4.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution Points [1]	http://crl.certsign.ro/certsign-webca.crl	Non-critical
Subject Alternative Name [1]	Other Name: Principal Name=office@certsign.ro RFC822 Name=office@certsign.ro	Non-critical
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	Non-critical
OCSPNoCheck	-	Non-critical

Table 7.5. OCSP certificate extensions

7.1.3 Algorithm object identifiers

SubjectPublicKeyInfo

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

Signature AlgorithmIdentifier

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

7.1.4 Name forms

Name Encoding

The contents of the fields in DV certificates meet the requirements in section 3.1 and the current CAB Forum Baseline Requirements Certificate Policy.
Issuer Name for all possible certification paths is byte-for-byte identical with Subject Name of the Issuer certificate. Subject attributes do not contain only metadata such as '.', '-', and ' ' (i.e. space) to indicate that the value is absent, incomplete, or not applicable.
For every valid Certification Path (as defined by RFC 5280, Section 6):

• For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate is byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
• For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate is byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

Subject Attribute Encoding
The attributes in the Certificate subject field will be encoded and positioned according to Table 77: "*Encoding and Order Requirements for Selected Attributes*" from CBAF BR section 7.1.4.2 Subject Attribute Encoding.

Subscriber Certificate Common Name Attribute
This attribute contains exactly one entry that is one of the values contained in the Certificate's subjectAltName extension.
If the value is a Fully-Qualified Domain Name or Wildcard Domain Name, then the value is encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name must be encoded as LDH Labels, and P-Labels will NOT be converted to their Unicode representation.

7.1.5 Name constraints
Not stipulated.

7.1.6 Certificate policy object identifier
Certificates policy object identifiers used at certSIGN Web CA level are described in Table 7.6 and Table 7.7.

Certification Policy Name	Policy identifier
certSIGN Web CA	***{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) domain-validated(1)} (2.23.140.1.2.1)*** **{certSIGN} .{id-policy}(3). {id-cp}(1).{id-Web-CA}(4) . *subpolicy ID=1.3.6.1.4.1.25017.3.1.4. subpolicy ID*** See below table for *subpolicyID* values. ***itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) dvcp (6)(0.4.0.2042.1.6)***

Table 7.6.Policies identifiers and their names for DV SSL certificates

CA Level	OID

certSIGN Web CA 1.3.6.1.4.1.25017.3.1.4	*DV certificate for website authentication* - ***.5*** *OCSP certificate* - ***.3***

Table 7.7 Certificate policy object identifiers

7.1.7 Usage of Policy Constraints extension

Not stipulated.

7.1.8 Policy qualifiers syntax and semantics

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

7.1.9 Processing semantics for the critical Certificate Policies extension

Not stipulated.

7.2 CRL profile

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

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

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

CRL profile is described in Table 7.8.

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

Table 7.8 CRL profile for certSIGN Web CA

7.2.1 Version numbers (s)

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

7.2.2 CRL and CRL entry extensions

CRLNumber extension contains an INTEGER greater than or equal to zero (0) and less than 2^{159}, and convey a strictly increasing sequence.

CRL extensions for certSIGN Web CA are described in Table 7.9.

Extension	Value or Value constraint	Extension status
Authority Key Identifier	65 29 2b 19 2b 5a 41 d3 01 62 9b 7b 47 00 e2 18 08 71 c3 41	Non-critical
CRL Number	monotonically increasing sequence number	Non-critical
ExpiredCertsOnCRL	Generalized Time	Non-critical

Table 7.9. CRL extensions for certSIGN Web CA

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

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

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

Table 7.10. revokedCertificates Component for certSIGN Web CA

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

1. No reason provided or unspecified (RFC 5280 CRLReason #0)
   - When the reason codes do not apply to the revocation request, the subscriber MUST NOT provide a reason code other than "unspecified".
2. keyCompromise (RFC 5280 CRLReason #1)
   - The certificate subscriber MUST choose the "keyCompromise" revocation reason when they have reason to believe that the private key of their certificate has been compromised, e.g. an unauthorized person has had access to the private key of their certificate.
3. affiliationChanged (RFC 5280 CRLReason #3)
   - The certificate subscriber SHOULD choose the "affiliationChanged" revocation reason when their Subject's name or other Subject Identity Information in the Certificate has

changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.

4. superseded (RFC 5280 CRLReason #4)
   - The certificate subscriber SHOULD choose the "superseded" revocation reason when the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with the Baseline Requirements or the CA's CPS.
5. cessationOfOperation (RFC 5280 CRLReason #5)
   - The certificate subscriber SHOULD choose the "cessationOfOperation" revocation reason when the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate.
6. privilegeWithdrawn (RFC 5280 CRLReason #9)[5]
   - The CRLReason privilegeWithdrawn is intended to be used when there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the certificate subscriber provided misleading information in their certificate request or has not upheld their material obligations under the subscriber agreement or terms of use.

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

7.3 OCSP profile

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

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

OCSP server certificate contains the extension extKeyUsage, described in RFC 5280.

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

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

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

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

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

- GOOD – indicates the valid status of certificate

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

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

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

7.3.1 Version numbers (s)

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

7.3.2 OCSP extensions

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

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

8 Compliance audit and other assessments

In respect to the conformity audits and the competence, consistent operation and impartiality of conformity of assessment bodies assessing and certifying CA conformity as certification services provider and the conformity of CA services towards the criteria from Regulation 910/2014 and its implementing acts and CA/B Forum Baseline Requirements, we follow the requirements from standard ETSI EN 319 401 and ESTI EN 319 411-1, and comply with:

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

8.1 Frequency or circumstances of assessment

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

The audit verifies the compliance with the present CPS and technical standards ETSI 319 401 and ETSI 319 411 and CA/B Forum Baseline Requirements.

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

8.2 Identity/qualifications of assessor

The assessment will be performed by a Conformity Assessment Body, as defined in the Regulation EU 910/2014 and CA/B Forum Baseline Requirements specifications.

8.3 Assessor's relationship to assessed entity

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

8.4 Topics covered by assessment

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

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

- system configuration management
- certSIGN's physical security,
- procedures of Subscriber's identity verification,
- certification services and procedures of service delivery,
- security of software applications and network access,
- security of certSIGN's personnel,
- event journals and procedures for system monitoring,
- data archiving and restoration,
- archiving procedures,

- records concerning the modification of configuration parameters for certSIGN,
- records concerning verifications and analysis carried out for software applications and hardware devices.

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

8.5 Actions taken as a result of deficiency

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

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

8.6 Communication of results

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

The Audit Report will state explicitly that it covers the relevant systems and processes used in the issuance of all certificates that assert the policy identifiers declared. The CA makes the Audit Report publicly available no later than three months after the end of the audit period. The audit report will comply with ETSI EN 319 403, chapter 7.4.4, and CABF Baseline Requirements, chapter 8.6.
An authoritative English language version of the publicly available audit information will be provided by the Qualified Auditor and the CA will ensure it is publicly available.
The Audit Report will be available as a PDF, and will be text searchable for all information required. Each SHA - 256 fingerprint within the Audit Report will be uppercase letters and will not contain colons, spaces, or line feeds.

8.7 Self-audits

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

certSIGN CA strictly controls the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist or an Internal Auditor employed by the CA to perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken. certSIGN uses a Linting process to verify the technical accuracy of Certificates within the selected sample set independently of previous linting performed on the same Certificates.

certSIGN CA reviews each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement.

certSIGN CA performs an internally audit with each Delegated Third Party for the compliance with these Requirements on an annual basis.

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.

Services provided by certSIGN are set as follows:

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

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

9.1.1 Certificate issuance or renewal fees

Prices are formed according to the internal price policy.

9.1.2 Certificate access fees

Free service.

9.1.3 Revocation or status information access fees

Prices are formed according to the internal price policy.

9.1.4 Fees for other services

Prices are formed according to the internal price policy.

9.1.5 Refund policy

Payments may be reimbursed according to the applicable contractual conditions.

9.2 Financial Responsibility

9.2.1 Insurance coverage

certSIGN has professional insurance policies in place and will cover damages that it may cause due to certification services for persons building their ethics on the legal effects of certificates

issued by certSIGN Web CA within the limits set by this CPP, contractual agreements entered into, as applicable.

9.2.2 Other assets

No Stipulation.

9.2.3 Insurance or warranty coverage for end-entities

certSIGN benefits from insurance covering professional responsibilities.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

All information related to the Subscriber/Partner Entities that certSIGN processes are obtained, stored and processed in accordance with the provisions of Regulation (EU) No. 910/2014. Relationships between a Subscriber, a Beneficiary, a Partner Entity, and certSIGN are based on trust.

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

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

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

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

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

Disclosing any piece of information to the parties involved in fulfilling their obligations will be made in a confidential manner and will cover only information necessary to fulfill the obligations.

Types of Information Considered Confidential and Private

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

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

- Records of system transactions (all types of transactions, as well as data for transactions control, the so called system transactions logs)
- Record of events (logs) related to certification services, kept by certSIGN,
- Results of external audits will be made public,
- Emergency plans,
- Information about measures taken to protect hardware devices and software applications, information about management of the certification services and planned registration rules.

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

Disclosure of Certificate Revocation Reason

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

Disclosure of Non-Public Information to Law Enforcement Officials

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

9.3.2 Information not within the scope of confidential information

All information required for proper functioning of certification services are not considered confidential or private. It particularly concerns information included in a certificate by the issuing Certification Authority, in accordance with specifications in Chapter 7. A Subscriber that applies for obtaining a certificate is aware of the type of information included in the certificate and agrees with their publishing.Part of the information provided by or to the Subscriber might be made available to other entities only with the written consent of the Subscriber and for the stated purpose in the contract concluded with the Subscriber.

9.3.3 Responsibility to protect confidential information

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

9.4 Privacy of personal information

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

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

9.4.1 Privacy Plan

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

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

- Appropriate technical and organizational measures are taken to ensure the security of the data processed, to protect the rights of the Subjects and to comply with the principles laid down in Regulation No 679/2016 and the provisions of Regulation (EU) No 910/2014.
- Access to certSIGN services concerns only the processing of those identification data which are adequate, relevant and not excessive to grant access to the respective service.
- the confidentiality and integrity of the registration data is ensured: when exchanged with the subscriber, when exchanged between certSIGN system components as well as when store

9.4.2 Information Treated as Private

certSIGN treats all personal information about a Subscriber that is not publicly available in the contents of a Certificate or CRL as private information.

9.4.3 Information not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

certSIGN undertakes to maintain the confidentiality of personal information during certification services and after certificate termination.

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

9.4.5 Notice and Consent to use Private Information

In the process of issuing a digital certificate, the persons designated by or the representatives of the Subscribers are informed about the need to use their personal data for the service. If data Subjects do not agree to certSIGN processing their data, certSIGN cannot issue digital certificates.

Subscribers, also have the option of using the personal data for other purposes expressly communicated by certSIGN by contract or otherwise.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

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

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

9.4.7 Other Information Disclosure Circumstances

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

- disclosure of personal information to:

  - auditors in the audits to which certSIGN is subject according to the provisions of Regulation (EU) no. 910/2014 under confidentiality;
  - the courier companies with which certSIGN has a contract, with the agreement of the Subscribers, if he has opted to transmit the certificate to his/her home address or to another communicated address, respecting the same obligations regarding the security of personal data that he/has and certSIGN;
  - an empowered person to whom I outsource certain services;
  - affiliated companies certSIGN

- personal information appearing in certificates or in the Public Authorities (Depositary), with the agreement of the Subscriber / Beneficiary;

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

9.5 Intellectual Property Rights

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

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

9.6 Representations and warranties

9.6.1 CA representations and warranties

By issuing a certificate, certSIGN makes for the following, certificate warranties:

1. The Subscriber that is a party to the Subscriber Agreement and Terms and Conditions for the Certificate;
1. All Application Software Suppliers with whom certSIGN has entered into a contract for inclusion of its CA certificate in software distributed by such Application Software Supplier; and
2. All Relying Parties who reasonably rely on a valid certificate.

certSIGN represents and warrants to Subscribers and Relying Parties that, during the period when the certificate is valid, the certSIGN has complied with these Requirements and its CPS for issuing and managing the certificate.

The Certificate Warranties specifically include those specified in the latest published version of CA/B Forum Baseline Requirements, paragraph 9.6.1.

9.6.2 RA representations and warranties

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

9.6.3 Subscribers representations and warranties

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

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

The Subscriber Agreement contains provisions imposing on the Subscriber itself the obligations and warranties specified in the CA/B Forum Baseline Requirements, paragraph 9.6.3.

9.6.4 Relying Party representations and warranties

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

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

9.6.5 Representations and warranties of other participants

No Stipulation.

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

Within the limit set by the Romania Law, in no event (except for fraud or willful misconduct by certSIGN) certSIGN will be liable for:

- Any loss of profits;
- Any loss of data;
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures;

- Any other damages.

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

Notwithstanding the above, if Certsign has not issued or managed the Certificate in compliance with the Baseline Requirements and its Certificate Policy and/or Certification Practice Statement, Certsign shall cover any direct damage to Subscribers or Relying Parties for legally recognized and provable claims limited to a monetary amount equal to the value of the certificate, per Subscriber or Relying Party per Certificate.

9.9 Indemnities

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

certSIGN acts as specified in paragraph "9.9 Indemnification by CAs" from CA/B Forum Baseline Requirements.
certSIGN responds and compensates only within the limits shown above.

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

All notices and other communications which may or are required to be given, served or sent pursuant to the CPS shall be in writing and shall be sent, except provided explicitly in the CPS, either by (i) registered mail, return receipt requested, postage prepaid, (ii) an internationally recognized "overnight" or express courier service, (iii) hand delivery or (iv) in electronic format, signed with a qualified electronic signature and be addressed to certSIGN using the contact details provided in chapter 1.5.1 from the present document.

9.12 Amendments

9.12.1 Procedure for amendment

certSIGN is responsible via its Policies and Procedures Management Body for the approval and change of the present CPS. The CPS is reviewed at least once a year.

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

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

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

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

9.12.2 Notification mechanism and period

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

9.12.3 Circumstances under which OID must be changed

No Stipulation.

9.13 Dispute resolution procedures

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

9.14 Governing law

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

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

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

9.16.1 Entire Agreement

No Stipulation.

9.16.2 Assignment

No Stipulation.

9.16.3 Severability

CA acts as specified in paragraph "9.16.3 Severability" from CA/B Forum Baseline Requirements.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No Stipulation.

9.16.5 Force Majeure

CA acts conforming to Romania Laws regarding Force Majeure.

9.17 Other provisions

No Stipulation.