Certification Practice Statement certSIGN

SSL DV CA Class 3 G2

for SSL DV certificates

Version 1.19

Date: 31 January 2024

Important Notice

Address: 29 A Tudor Vladimirescu Avenue,
AFI Tech Park 1, Bucharest, Romania
Phone: 004-021-31.19.901

Web: www.certsign.ro

Document History

Version	Effective Date[1]	Reason	The person who made the change
1.0	January 2018	First version publishing	Information Security Officer
1.1	May 2018	CPS compliance with GDPR recommendations	PKI Policies Manager
1.2	July 2018	CPS compliance with CA-Browser Forum, about validating the Applicant's ownership or control of the domain	PKI Policies Manager
1.3	November 2018	Update change headquarters	PKI Policies Manager
1.4	January 2019	Annual review. Updates determined by removal character underscore "_" in the domain name/dNSName CA/Browser Forum BR 1.6.2	PKI Policies Manager
1.5	January 2020	Annual review. Minor updates for compliance with CA/Browser Forum BR 1.6.7 and Mozilla Policy v2.7.	PKI Policies Manager
1.6	May 2020	Add validation method 3.2.2.4.2	PKI Policies Manager
1.7	May 2020	Fix OCSP updates, SSL validity 1 year	PKI Policies Manager
1.8	September 2020	Add 7.2 CRL acc. CAB BR v1.7.2	PKI Policies Manager
1.9	January 2021	Annual Review	PKI Policies Manager
1.10	May 2021	Add Private Key compromise methods	PKI Policies Manager
1.11	September 2021	Ballot SC48 – FQDN	PKI Policies Manager
1.12	November 2021	Updates on domain validation methods	PKI Policies Manager
1.13	January 2022	Annual Review	PKI Policies Manager
1.14	June 2022	Updates ref. Subordinated CA, revocation reasons and validity	PKI Policies Manager
1.15	October 2022	Updates on identity validation, certificate request & CRL Reason	PKI Policies Manager
1.16	January 2023	Annual Review	PKI Policies Manager
1.17	May 2023	Various updates, links, OIDs	PKI Policies Manager
1.18	July 2023	Move #7 Profiles in external doc	PKI Policies Manager
1.19	January 2024	Annualreview	PKI Policies Manager

This document was created and is the property of:

Owner	Author	Date created
BU Trust Services	Information Security Officer	January 2018

Distribution List

Destination	Date distributed
Public-Internet	January 2018
Public-Internet	May 2018
Public-Internet	July 2018
Public-Internet	November 2018
Public-Internet	January 2019

[1] *Effective date is the last day of the month*

Public-Internet	January 2020
Public-Internet	May 2020
Public-Internet	September 2020
Public-Internet	January 2021
Public-Internet	May 2021
Public-Internet	September 2021
Public-Internet	November 2021
Public-Internet	January 2022
Public-Internet	June 2022
Public-Internet	October 2022
Public-Internet	January 2023
Public-Internet	May 2023
Public-Internet	July 2023
Public-Internet	January 2024

This document was approved by:

Version	Name	Date
1.0	Policies and Procedures Management Body	January 2018
1.1	Policies and Procedures Management Body	May 2018
1.2	Policies and Procedures Management Body	July 2018
1.3	Policies and Procedures Management Body	November 2018
1.4	Policies and Procedures Management Body	January 2019
1.5	Policies and Procedures Management Body	January 2020
1.6	Policies and Procedures Management Body	May 2020
1.7	Policies and Procedures Management Body	May 2020
1.8	Policies and Procedures Management Body	September 2020
1.9	Policies and Procedures Management Body	January 2021
1.10	Policies and Procedures Management Body	May 2021
1.11	Policies and Procedures Management Body	September 2021
1.12	Policies and Procedures Management Body	November 2021
1.13	Policies and Procedures Management Body	January 2022
1.14	Policies and Procedures Management Body	June 2022
1.15	Policies and Procedures Management Body	October 2022
1.16	Policies and Procedures Management Body	January 2023
1.17	Policies and Procedures Management Body	May 2023
1.18	Policies and Procedures Management Body	July 2023
1.19	Policies and Procedures Management Body	January 2024

Content

1 Introduction

The **Certification Practice Statement certSIGN SSL DV CA Class 3 G2 for SSL DV 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

- ETSI EN 319 411-1
- CA/B Forum Baseline Requirements (Policy DV 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 — SSL Baseline with Network Security
- Mozilla Root Store Policy,
- Apple Root Certificate Program,
- Microsoft Trusted Root Program,
- Chrome Root Program Policy.

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 certSIGN SSL DV CA Class 3 G2 for SSL DV certificates,** further referred as **CPS**.

The document is available in electronic format within the Repository at address http://www.certsign.ro/Repository.

1.3 PKI Participants

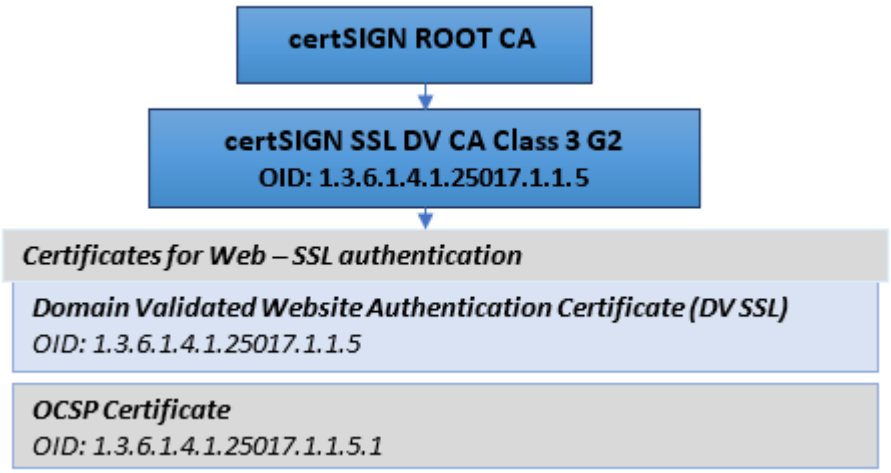
The CPS regulates the most important relations between entities belonging to certSIGN, the advisory teams (including auditors) and customers (users of the provided services) of this:

- certSIGN SSL DV CA Class 3 G2
- Registration Authority,
- The 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

certSIGN provides certification services for every natural or 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 ensure 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

The Certification Authority certSIGN SSL DV CA Class 3 G2 is an Intermediate Certification Authority for the certSIGN domain. It is subordinated to the certSIGN ROOT CA. certSIGN SSL DV CA Class 3 G2 is identified by the following OID: 1.3.6.1.4.1.25017.1.1.5.



Before beginning the activity, certSIGN SSL DV CA Class 3 G2 sent a request to the Primary Certification Authority, certSIGN ROOT CA for registration and public key certificate issuance.

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) both the subscriber/subject and 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, if the legislation allows this. Before certSIGN authorizes a Delegated Third Party to perform a delegated function, certSIGN contractually requires the Delegated Third Party to fulfill the conditions specified in the document "Requirements for Delegated Registration Authority for certSIGN SSL DV CA Class 3 G2 certificates".

1.3.3 Subscribers

Subscriber

Subscriber is the natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use. Subscribers may request issuance, revocation or rekey of end-entity certificates for Subjects under their care. A Subscriber is also responsible for immediately notifying certSIGN upon (suspicion of) private key compromise.

Subject

The subject is the entity (legal or natural person) to which a certificate is issued and is identified in a certificate as the holder of the private key associated with the public key from the certificate.

The subject can be:

- The Subscriber in case of requesting the certificate for himself,
- A natural person for whom the Subscriber requests the certificate, having a legally binding agreement or acting as his/her employer
- A legal entity for whom the Subscriber requests the certificate

A Subject is also responsible for:

- Immediately notifying certSIGN upon (suspicion of) private key compromise;
- Submitting requests for renewal of keys and/or certificates 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.

1.3.4 Relying parties

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

A Relying Party is responsible for how it verifies the current status of a Subject's certificate. Such a decision shall be taken every time a Relying Party is willing to use a certificate to verify the identity of the source or to create a secure communication channel with the Subject of the certificate. A Relying Party shall use the information in a certificate to decide whether a certificate was used according to the stated purpose.

1.3.5 Other participants

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

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

Public Notaries: may perform identification and guarantee for the real identity of the Subjects.

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 settling 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. Subjects shall know the requests of the Relying Parties (for example, these requests might be published as a signature policy or an information security policy) and then to request certSIGN to issue certificates corresponding to these requests.

1.4.1 Appropriate certificate uses

SSL DV server certificates are used to activate the TLS/SSL protocol on one or more web sites, whose domain was validated by certSIGN.

It is assumed that the subscriber possesses the competence and tools required to request, install and use the certificate.

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

1.4.2 Prohibited certificate uses

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

1.5 Policy administration

1.5.1 Organization administering the document

The present document is administered by the 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: J40/484/2006 Tax registration code: RO 18288250 Registered office: 107A Oltenitei Street. building C1, ground floor, District 4, Bucharest, Romania, PC 041303
Phone	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Table: 1.5.1 Organization administering the document

1.5.2 Contact person

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

Table: 1.5.2 Contact person

Procedure for certificate problem reporting

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

1. The nature of the alleged problem;

2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;

3. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and

4. Relevant legislation.

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

1.5.3 Person determining CPS suitability for the policy

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

Table: 1.5.3 Person determining CPS suitability for the policy

1.5.4 CPS approval procedures

Policies and Procedures Management Body is responsible for the approval of the CPS.
The approval procedure is described in an internal instruction document.
Subscribers shall adhere to the CPS published at: http://certsign.ro/repository
Subjects/ 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 6844 (http:tools.ietf.org/html/rfc6844): "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."

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 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 Certificate: A certificate that is used to establish a trust relationship between two Root 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.

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant,

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.

Domain Name: The label 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

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 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, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) or if there is clear evidence that the specific method used to generate the Private Key was flawed.

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.

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

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.

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.

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.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.3.

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 this 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.

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 Subordinate CA is similar to an Intermediate or Issuing CA in that it also chains off of the Root CA, however the distinction is that a Subordinate CA is generally operated by a different party than the Root or Intermediate CA above it.

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 **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.

Test Certificate: A Certificate with a maximum validity period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID (2.23.140.2.1), or (ii) is issued under a CA where there are no certificate paths/chains to a root certificate subject to these Requirements.

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: Prior to 2020-09-01, the period of time measured from the date when the Certificate is issued until the Expiry Date. For Certificates issued on or after 2020-09-01, the

validity period is as defined within RFC 5280, Section 4.1.2.5: the period of time from notBefore through notAfter, inclusive.

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.

1.6.2 Acronyms

CA Certification Authority
CPS certification Practice Statement
CRL certificate Revocation List
CARL Certification Authority Revocation List
DN Distinguished Name
NIMB National Institute of Metrology Bucharest

OCSP On-line Certificate Status Protocol
PKI Public Key Infrastructure
PPMB Policies and Procedures Management Body
QSCD Qualified Electronic Signature Creation Device
RA Registration Authority
RSA Rivest, Shamir, Adleman asymmetric cryptographic algorithm
SSL Secure Sockets Layer
TSP Trust Services Provider
UTC Coordinated Universal Time

2 Publication and repository responsibilities

2.1 Repositories

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

- Certificate Practice Statement for the ROOT & CAs operated by certSIGN
- Root CA and Intermediate CA certificates https://www.certsign.ro/en/resources/chain-of-trust/
- The certificates of the subjects https://registru.certsign.ro/cgi-bin/pubral/pubra/get_cert
- Certificate Revocation Lists https://www.certsign.ro/en/resources/certificate-revocation-list/
- Terms and conditions for the use of digital certificates https://www.certsign.ro/en/document/general-terms-and-conditions-for-ssl-dv-and-ov-certificates/

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

- Make all necessary efforts to ensure that all certificates published in the Repository belong to the Subjects' registered in certificates, and Subjects 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 Subject'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, Subjects and Relying Parties,
- Publish CRLs or other information in due time and in compliance with deadlines mentioned in the CPS,
- Ensure secure and controlled access to information in the Repository.

2.2 Publication of certification information

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

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

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 3 web pages that allow Application Software Suppliers to test software with Subscriber Certificates issued by certSIGN SSL DV CA:

https://testssl-valid.certsign.ro/
https://testssl-expired.certsign.ro/
https://testssl-revoked.certsign.ro/
certSIGN makes available to relying parties the terms and conditions regarding the use of the SSL DV certificates.

Availability

Availability of the document 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 outside the control of certSIGN or any other reason, certSIGN SA shall make best endeavors to reinstate availability of the service within 5 working days.

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

2.3 Time or frequency of publication

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

CPS – annual review, and updates, as per Chapter 1.5,

Certificate of the Certification Authorities – after issuing a new certificate;

Subjects' certificates – when the consent has been obtained, after every issue of a new certificate;

Certificate Revocation List – see Chapter 7;

Audit reports performed by authorized institutions – when certSIGN receives them;

Additional information – after every update.

2.4 Access control on repositories

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

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

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

certSIGN may take reasonable measures to protect 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.

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. Within DN, it is possible to define attributes of Domain Name Service (DNS). This allows the Subjects to use two types of names: DN and DNS simultaneous. This is a very important option in case of issuing certificates to servers administrated by the Subject.

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

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 is placed in the Common Name (CN) attribute of the Subject field, it can also be copied 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, this is in compliancy with the CA / Browser Forum BR recommendations latest published version. FQDN consists solely of P-Labels and Non-Reserved LDH Labels.

SSL certificates may include public IP addresses, in accordance with RFC 2460 (IP version 6) or RFC791 (IP version 4).

Type Unified Communications SSL certificates (multi domain) may include non-routable domains (i.e. .local) or private IPs (in accordance with RFC 1918) within the Subject Alternative Name extension. Issuing SSL certificates for non-routable domains, private IP

addresses or reserved IP addresses (in accordance with http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml) is deemed outdated. Currently, there are no certificates issued according to these specifications whose expiry date is after 1st November 2015.

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.

DN consists of the following optional 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.

The name of the Subject shall be confirmed by an operator of the Registration Authority and approved by a Certification Authority. certSIGN ensures (within its domain) the uniqueness of the DN-s.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation.

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

The identification of every holder of certificates issued by certSIGN is performed based on the DN. certSIGN ensures the uniqueness of the DN assigned to every Subject.

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.

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

3.2.2 Authentication of organization and domain 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 representatives of the institution are bind to the following documents:

- Purchasing request;

The procedure performed by RA to verify domain:

- 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 (if the request supposes a key pair to create an electronic signature) 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– cap 3.2.2.4.2 (Email, Fax, SMS, or Postal Mail to Domain Contact), cap. 3.2.2.4.4 *(Constructed Email to Domain Contact)* or 3.2.2.4.7 (DNS Change)
- 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,
- Copies all the documents and certificates used by the operator,
- On behalf of the Certification Authority concludes a contract with a legal entity concerning the rendering of certification services.

The confirmation is sent to the Certification Authority that verifies if this was issued by an authorized Registration Authority.

The authentication process is registered. The type of registered information and actions depend on the credibility level of the certificate that makes the object of the request and concerns:

- The identity of the Registration Authority's operator that verifies the solicitor's request,
- Verification data,
- The identifier of the operator and the solicitor in case the latter is personally present at the Registration Authority (supposing that the solicitor was assigned with such an identifier),

3.2.2.2 DBA (Doing Business As)/Trade Name

N/A

3.2.2.3 Verification of country

The RA verifies the country associated with the Subject 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) A method identified in Section 3.2.2.1.
The CA has implemented 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 Subject's ownership or control of the domain.

certSIGN confirms that, before issuing a certificate, it validated each fully qualified domain name (FQDN) appearing in the certificate, using at least one of the bellow methods. 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 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

certSIGN will send an Email to the 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 the address of the Domain contact 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.
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.
This method is suitable for validating Wildcard Domain Names.

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

In all cases, 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.
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.
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 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.
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.
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 Contact
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
This method of domain validation is not used.

3.2.2.4.20 TLS Using ALPN
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, certSIGN evaluates the source for its reliability, accuracy, and resistance to alteration or falsification. certSIGN 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. The issuance is within the TTL of the CAA record, or 8 hours, whichever is greater.

3.2.3 Authentication of individual identity

certSIGN do not issue TLS certificates for physical persons

3.2.4 Non-verified subscriber information

All information that is supplied by the certificate subscriber will be verified by using an independent source of information or an alternative communication channel before it is included in the certificate.

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 legal person or for a device belonging to a legal or natural person. In both cases, 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 or certification

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.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Chapters 4.7 and 4.8 of the present document describe the process.

3.3.2 Identification and authentication for re-key after revocation

The same process as for initial identity validation is used.

3.4 Identification and authentication for revocation request

Revocation requests can be sent via e-mail (office@certsign.ro) 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.
- The Subscriber is unable to send and electronic revocation request shall use a second method. 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 Subject who is the holder of the private key associated with the public key from the certificate
- The Subscriber who enters into a contractual agreement with certSIGN for issuing certificates to Subjects
- The Registration Authority that can request the revocation either on behalf of a Subject or if it has information that justifies the certificate revocation, by creating an authenticated request using the security mechanisms of the Registration Authority software
- Trusted roles associated to certSIGN SSL DV CA Class 3 G2, 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 all types of certificates issued by certSIGN SSL DV CA Class 3 G2.
The detailed procedures related to PKI component services (CAs, RAs, CRLs signers, OCSP responder, etc.) and the persons/roles involved in the operational process of these components are described in internal confidential documentation.
certSIGN provides access to the following services:

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

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 issues certificates:

- To natural persons, in case of requesting the certificate for himself
- To natural person(s) (Subjects) for whom the Subscriber requests the certificate, having a legally binding agreement or acting as his/her employer.

The Subscriber and the Subject shall comply with the provisions and obligations set forth in the registration form, in the applicable Subscriber Agreement and the certificate services Terms and Conditions that incorporate this CPS and the PKI Disclosure Statements.
The Certification Authority only issues certificates as a response to an authenticated request from the Registration Authority operated by certSIGN, or a delegated third party, if the legislation allows this.
certSIGN archives the information related to enrolment. The archive is maintained according to the requirements defined in the CPS and applicable legislation.

Certificate Application by Legal Persons (Organizations)
The Subject shall comply with the provisions and obligations set forth in the registration form, in the applicable Subscriber Agreement and the certificate services Terms and Conditions that incorporate this CPS.

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

Prior to the issuance of a certificate, the RA 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.

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

- The certificate request,
- The control on the requested domain(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 and the applicable law.
The Subscriber is provided with the following information which are part of the Subscribers' Agreement:

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

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

- His responsibility that the information provided by the Subject 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/or 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 Subject 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 data and for supplying the CA with the correct content for the variable fields in the certificate.

4.2 Certificate application processing

The requests may be sent *on-line*.

The certificate request is filled in electronic format:

- The request form (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 it to the Certification Authority via e-mail or
- The certificate request may be filled in and posted on site: https://www.shop.certsign.ro
- The certificate request is filled in electronic format sent via an authenticated channel

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 6844 as amended by Errata 5065 (Appendix A). 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 RA performs identification and authentication according to the procedure defined in chapter 3.2. and within internal confidential documentation.
The RA collects the Subscriber's identity information.
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.

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 SSL DV CA Class 3 G2 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.

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

4.3.1 CA actions during certificate issuance

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

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.

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.

The Subject is bound by the conditions and obligations mentioned the Subscriber Agreement, which includes this CPS. The Subscriber shall protect the keys and any associated Activation

Data (e.g. password, PIN code, etc.) or other information against loss, theft, disclosure, compromise or modification.

The Subscriber is personally responsible for:

- Using the keys only for the intended use as defined in the Certificate Policy and as encoded in the certificates
- Using tools that can correctly interpret the key usage as encoded in the certificate and that respect the key usage conditions
- Setting Activation Data that is unique and that comply with the guidelines given in the Certificate Policy
- Keeping these secret information confidential
- Safe storage of any document or medium containing transcripts of part or all of the associated Activation Data
- Not disclosing the Activation Data to another person
- Installing the certificate only on servers that are accessible at the subjectAltName(s) listed in the certificate, and to use the certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms and Conditions

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.

The Subjects shall use the private key and certificates:

- In compliance with the purpose stated in the present CPS and in compliance with the certificate's content (fields *keyUsage* and *extendedKeyUsage*),
- In compliance with the provisions of the agreement between the Subscriber and certSIGN,
- Only during the validity period,

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

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal
No stipulation.
4.6.3 Processing certificate renewal requests
No stipulation.
4.6.4 Notification of new certificate issuance to subscriber
No stipulation.
4.6.5 Conduct constituting acceptance of a renewal certificate
No stipulation.
4.6.6 Publication of the renewal certificate by the CA
No stipulation.
4.6.7 Notification of certificate issuance by the CA to other entities
No stipulation.

4.7 Certificate Re- key

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

Rekey is performed when a Subject holding a valid (not revoked and not expired) digital certificate generates a new key pair and requests the issuance of a new certificate to confirm the possession of a new created public key.
Certificate rekey is performed only upon Subject's request and shall be preceded by the submission of a request on a corresponding form filled in by the Subscriber/Subject.
4.7.3 Processing certificate re-keying requests
The process of the initial certificate request will be amended as follows:

- The identification of the requester and validation results from previous requests are considered valid while the validated information has not changed and those information are obtained from a source specified under Section 3.2 no more than twelve (12) months prior to issuing the Certificate.
- Any data that has changed is to be validating as if this was a new request.

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 does not modify the issued certificates.
The Subject or the Subscriber, as the case may be, shall request certSIGN to revoke the certificate as soon as the information included in the certificate is no longer in accordance with the reality.

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

Certificates issued by certSIGN SSL DV CA Class 3 G2 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 Subject's control, after revocation it should be safely stored until it is destroyed.

4.9.1 Circumstances for revocation

The certificate is revoked within 24 hours 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 employment relationship or the legal binding agreements between the Subscriber and the Subject are concluded,
- The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6
- The CA obtains evidence that the certificate was misused;

- 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;
- 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 Subscriber/Subject has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- The CA is made aware of a material change in the information contained in the certificate;
- The CA is made aware that the certificate was not issued in accordance with this CPS
- The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
- The CA's right to issue certificates under CA/B Forum Baseline Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- The CA is made aware of a possible compromise of the Private Key of the certSIGN SSL DV CA Class 3 G2;
- The technical content or format of the certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced within a given period of time)
- The Subject, holder of the private key associated with the public key from the certificate, requests the revocation,
- The Subscriber requests the revocation of an end-entity certificates for Subjects under its care,
- Subjects/ Subscribers do not accept new, modified terms and regulations of CPS
- The Certification Authority terminates its activity; in this case all certificates issued by this Certification Authority before the stated period for terminating the services shall be revoked along with the certSIGN SSL DV CA Class 3 G2 certificate,
- The Subject delays or does not pay the value of the services provided by certSIGN SSL DV CA Class 3 G2,
- The private key or the security of certSIGN SSL DV CA Class 3 G2 were compromised in a manner that threatens the certificates' credibility,
- In other cases when the Subject does not comply with the rules of this CPS, Subscriber agreement, Terms and conditions or other agreements concluded between the parties related to the services provided by certSIGN SSL DV CA Class 3 G2.

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 Registration Authority that can request the revocation either on behalf of a Subject or if it has information that justifies the certificate revocation
- Trusted roles associated to certSIGN SSL DV CA Class 3 G2, under the supervision of the Policies and Procedures Management Body (PPMB)

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 revocation procedures is described in section 3.4 of this CPS.

The revocation reason may be only from the ones specified in chapter 7.2.

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 on a best effort basis, to ensure that the time needed to process the revocation request and to publish the revocation notification (updated CRL) is as reduced as possible.

4.9.5 Time within which CA must process the revocation request

certSIGN guarantees a maximum period of 24 hours for processing a certificate revocation request.
CA decides 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; The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities will carry more weight than a complaint from a consumer alleging that she or he didn't receive the goods she ordered); and
3. Relevant legislation.

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

4.9.6 Revocation checking requirements for relying parties

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

4.9.7 CRL issuance frequency

A new CRL is published in the Repository after every certificate revocation, within maximum one day. If the key compromising is the reason for the revocation the new CRL is issued immediately after the revocation request processing. The CRL's availability period is of 48 hours and it is updated daily.

4.9.8 Maximum latency for CRLs

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

4.9.9 On-line revocation/status checking availability

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

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

4.9.10 On-line revocation checking requirements

The CA supports an OCSP capability using the GET method for certificates issued in accordance with latest published version of CA/B Forum Baseline Requirements.

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

For the status of Intermediate 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 Intermediate 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.

4.9.11 Other forms of revocation advertisements available
No stipulation.

4.9.12 Special requirements related to key compromise

If a Subject knows or suspects that the integrity of his certificate's private key has been compromised, the Subject 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 Subject 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
No stipulation

4.9.14 Who can request suspension
No stipulation

4.9.15 Procedure for suspension request
No stipulation

4.9.16 Limits on suspension period
No stipulation

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 never removed.

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

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

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

4.10.3 Optional features
certSIGN certificate status services do 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/Subject,
- Expiration of the last certificate of a Subscriber/Subject.

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

4.12 Key escrow and recovery
certSIGN does not allow key escrow for SSL certificates.

4.12.1Key escrow and recovery policy and practices
No stipulation.

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

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

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

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

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 A 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;

Every piece of equipment is correctly maintained to ensure its continuous availability and integrity.

5.1.2 Physical access

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

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

Visitors are permanently escorted by the authorized personnel.

certSIGN premises are divided into:

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

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

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

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

5.1.3 Power and air conditioning

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

5.1.4 Water exposure

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

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

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

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

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

5.1.8 Offsite 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

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

Every assigned account:

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

All actions, in relation to certificates, by employees in trusted roles, are monitored.

5.2.4 Roles requiring separation of duties

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

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

5.3 Personnel control

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

- Has graduated from at least the secondary school,
- Has understood and signed off an agreement describing his/her role in the system and his/her corresponding responsibilities,
- Has been subjected to advanced training on the range of obligations and tasks, associated with his/her position,

- Has been trained in the field of personal data protection and confidential and private information protection,
- Has signed off an agreement containing clauses related to the protection of certSIGN's sensitive information and confidentiality and privacy of Subscriber's data,
- Does not perform tasks which may lead to a conflict of interests between a Certification Authority and a Registration Authority acting on behalf of it.

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

5.3.1 Qualifications, experience and clearance requirements

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

5.3.2 Background check procedures

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

5.3.3 Training requirements

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

- Requirements of Certification Practice Statement,
- Procedures and security controls employed by the Certification Authority and the Registration Authority
- 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 modifications to certSIGN operations are made.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

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

5.3.8 Documentation supplied to personnel

certSIGN provides to personnel the following documents:

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

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

5.4 Audit logging procedures

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

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

5.4.1 Types of events recorded

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

- **System logs** – contain information about customer's requests and server's responses (or vice versa) at the level of the network protocol (for example http,

https); the recorded data is: IP address of the station or server, performed operations (for example: searching, editing, writing etc.) and their results (for example the successful entry of a record in the database),
- **Errors** – contain information about errors at the network protocols level and at the applications' modules level;
- **Audit logs**– contain information specific for the 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.

Every automatic or manual recording contains the following information:

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

All events relating to the life-cycle of CA keys are recorded.

All events relating to the life-cycle of certificates are recorded.

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

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

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

All registration information, including the following, is recorded:

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

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

- Changes to the security policy
- Start and stop of systems;
- Outages;
- System crashes and hardware failures
- Firewall and router activities
- PKI system access attempts
- Physical access of personnel and other persons to sensitive parts of any secure site or area;

- Back-up and restore;
- Report of disaster recovery tests;
- Audit inspections;
- Upgrades and changes to systems, software and infrastructure;
- Security intrusions and attempts at intrusion.

Access to logs is exclusively allowed for the security officer, special appointed personnel, and auditors.

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. In 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.

5.4.4 Protection of audit log

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

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

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

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

- Collect

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

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

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

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

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

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

5.5 Records archival

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

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

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

Backup copies are created and retained outside certSIGN location.

5.5.1 Types of 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 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/Subject may get access to related registration records and other information relating to the Certificate Subject.

5.6 Key Changeover

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, certSIGN ceases using its expiring CA Private Key to sign Certificates (at least 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 implemented a security incident management procedure in order to respond quickly and coordinated to incidents and to limit the impact of security breaches. Employees are assigned to trusted roles to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the procedure. Critical malfunctions are acted upon on the basis of the same procedure.

The security incident management procedure also specifies how to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.

In case of security incident, internal procedures are used. The procedures include the notification of the Supervisory body.

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.

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

- All the certificates signed by the corrupted CA are revoked and a suitable reason for revocation is submitted
- The Certification Authority generates a new key pair and a new certificate
- New certificates for Subject are generated

The new certificates for Subjects are submitted to them free of charge.

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

5.7.4 Business continuity capabilities after a disaster

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

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

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

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

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

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

5.8 CA or RA termination

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

Requirements associated to duty transition

Before Certification Authority ceases its activity, it will:

- Inform (at least 30 days in advance) the following about the decision to terminate its services: all Subjects/ Subscribers who hold active (unexpired and unrevoked) certificates issued by this authority and other entities with which certSIGN has agreements or other form of established relations, among which relying parties, other trust service providers and relevant authorities such as supervisory bodies. In addition, this information will be made available to other relying parties;

- Revoke the unexpired certificates that have been issued.
- Transfer its obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the certification services for a reasonable period, unless it can be demonstrated that certSIGN does not hold any such information. The information refers to registration information, revocation status for unexpired certificates that have been issued and event log archives for their respective period of time as indicated to the Subjects/ Subscriber and relying party;
- Destroy CA private keys, including backup copies, or withdraw them from use, in such a manner that the private keys cannot be retrieved;
- Where possible, make arrangements to transfer provision of certification services for the existing customers to another certification service provider.

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

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

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 (in the case of termination of services of the certSIGN SSL DV CA Class 3 G2) or to the institution that the contract was signed with (in the case of termination of services of certSIGN ROOT CA).

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 SSL DV CA Class 3 G2 owns at least one certificate signed by certSIGN ROOT CA. 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

6.1.1.1 CA 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 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 SSL DV CA Class 3 G2 are undertaken in a physically secured environment by personnel in trusted roles under, at least, dual control:

- At least three employees in trusted roles

- The security officer
- At least one representative of Policies and Procedures Management Body (PPMB)
- A Master of Key Ceremony
- At least one independent and external 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-generated subject keys are generated using an algorithm recognized as being fit for the uses, during the validity time of the certificate. CA key pair generation is performed using the RSA algorithm with a 4096 bits key length.

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

6.1.1.2 RA Key Pair Generation

No stipulation.

6.1.1.3 Subscriber Key Pair Generation

The Subjects' keys are generatedby the Subject, 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

No stipulation.

6.1.3 Public key delivery to certificate issuer

Subjects 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://registru.certsign.ro/cgi-bin/pubral/pubra/get_cert.

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 SSL DV CA Class 3 G2 uses a 2048 bit key for certificates and CRL signing.

The digital certificates issued by certSIGN SSL DV CA Class 3 G2 use 2048 bit RSA keys.

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

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

6.1.6 Public Keys parameters generation and quality checking

certSIGN has a documented procedure for conducting CA key pair generation for certSIGN SSL DV CA Class 3 G2. 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

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

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

a. digitalSignature: certificate intended for electronic signature verification,
b. keyEncipherment: intended to encrypt symmetric algorithm keys, providing data confidentiality,

The private key of certSIGN ROOT CA (the issuing CA for certSIGN SSL DV CA Class 3 G2) is used only in the following cases:

- Self-signed Certificates to represent the Root CA itself;
- Certificates for Intermediate CAs and Cross Certificates.

6.2 Private Key protection and Cryptographic Module Engineering Controls

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

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 by the holder in a manner allowing share usage for restoration of certSIGN activity to its normal state.

Responsibilities of shared secret holder

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

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

6.2.3 Private Key escrow

Private keys of Certification Authorities are not subject to custody.

Subject's private keys are not subject to custody.

6.2.4 Private Key backup

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 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 2 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.

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

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.

6.2.10 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 destruction of a private key is recorded in the event journal.

The Subject is responsible to destroy the private key.

6.2.11 Cryptographic Module Capabilities

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 SSL DV CA Class 3 G2 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 Subject's keys cannot exceed the validity period of a certificate.

The validity period of certSIGN SSL DV CA Class 3 G2 certificate is 10 years.

The validity period of a Subject certificate issued by certSIGN SSL DV CA Class 3 G2 is up to 397 days, for certificates issued after August 31, 2020.

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.

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

6.4.2 Activation data protection

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

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

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

6.4.3 Other aspects of activation data

No stipulation

6.5 Computer security controls

This chapter describes certSIGN's computer security controls.

Subject 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 Standards: ETSI EN 319 411-1 and CEN CWA 14167 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures).

6.6 Life cycle security controls

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

6.6.1 System development controls

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

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

Similar rules apply to hardware components replacement, as follows:

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

6.6.2 Security management controls

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

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

6.6.3 Life cycle security controls

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

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

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

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.

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.

6.8 Time-stamping

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

7 Certificate, CRL and OCSP profile

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

7.1 Certificate profile

Profile of basic fields for certSIGN SSL DV CA Class 3 G2 certificate is described in Table 7.1 from the external document "certSIGN SSL DV CA Class 3 G2 - Annex Profiles.docx".

Profile of basic fields for certificates issued by certSIGN SSL DV CA Class 3 G2 is described in Table 7.2 from the external document "certSIGN SSL DV CA Class 3 G2 - Annex Profiles.docx".

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

Certificate extensions for certSIGN SSL DV CA Class 3 G2 are described in Table 7.3 from the external document "certSIGN SSL DV CA Class 3 G2 - Annex Profiles.docx".

DV SSL certificate contains extensions described in Table 7.4 from the external document "certSIGN SSL DV CA Class 3 G2 - Annex Profiles.docx".

OCSP certificate contains extensions described in Table 7.5 from the external document "certSIGN SSL DV CA Class 3 G2 - Annex Profiles.docx".

7.1.3 Algorithm object identifiers

According to the external document "certSIGN SSL DV CA Class 3 G2 - Annex Profiles.docx".

7.1.4 Name forms

The contents of the fields in DV certificates must meet the requirements in section 3.1 and the latest published version of 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.

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

Certificates policy object identifiers used at certSIGN SSL DV CA Class 3 G2 level are described in Table 7.6 and Table 7.7 from the external document "certSIGN SSL DV CA Class 3 G2 - Annex Profiles.docx".

7.1.7 Usage of Policy Constraints extension

No stipulation.

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

No stipulation.

7.2 CRL profile

CRL profile is described in Table 7.8 from the external document "certSIGN SSL DV CA Class 3 G2 - Annex Profiles.docx".

7.2.1 Version numbers (s)

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

7.2.2 CRL and CRL entry extensions

CRL extensions for certSIGN SSL DV CA Class 3 G2 are described in Table 7.9 from the external document "certSIGN SSL DV CA Class 3 G2 - Annex Profiles.docx".

CRL entry extensions (crlEntryExtensions) supported by certSIGN contain the following fields according to the external document "certSIGN SSL DV CA Class 3 G2 - Annex Profiles.docx".

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 Intermediate CA and Root CA, generated exclusively for this purpose.

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

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

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

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

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

- GOOD – indicates the valid status of certificate

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

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

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

7.3.1 Version 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 319 403.

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.

The audit verifies the compliance with the present CPS and technical standards ETSI 319401 and ETSI 319411 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.

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 listed in Section 7.1.6.1. The CA makes the Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, the CA provides an explanatory letter signed by the Qualified Auditor. The audit report will comply with CABF Baseline Requirements, chapter 8.6.

8.7 Self-audits

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

9 Other business and legal 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 Fees refund

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 any damages it may cause due to certification services for persons building their ethics on the legal effects of certificates issued by certSIGN CAs 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 liabilities.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

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

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

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

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

or

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

or

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

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

Types of Information Considered Confidential and Private

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

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

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

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

Disclosure of Certificate Revocation Reason

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

Disclosure of Non-Public Information to Law Enforcement Officials

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

9.3.2 Information not within the scope of confidential information

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

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

9.3.3 Responsibility to protect confidential information

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

9.4 Privacy of personal information

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

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

9.4.1 Privacy Plan

In the provision of certification services, certSIGN acts as a personal data controller according to paragraph 7 of art. 4 of the Regulation no. 679/2016.
Security measures required by Regulation (EU) No 910/2014, Regulation No 679/2016 and the Romanian National Supervisory Authority in the field of personal data processing are implemented by certSIGN to ensure that:

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

9.4.2 Information Treated as Private

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

9.4.3 Information Treated as Private

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

9.4.4 Responsibility to Protect Private Information

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

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

9.4.5 Notice and Consent to use Private Information

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

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

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

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

9.4.7 Other Information Disclosure Circumstances

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

- disclosure of personal information to:

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

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

9.5 Intellectual Property Rights

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

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

9.6 Representations and warranties

9.6.1 CA representations and warranties

certSIGN issues X509 v3-compatible Certificates that are compliant with either ETSI TS 102 042 or ETSI TS 101 456 requirements.

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

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

The Certificate Warranties specifically include those specified in the 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 Subject representations and warranties

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

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

CA Terms and Conditions contains provisions imposing on the Subject 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 Subject, Subscribers and Relying Parties.

9.8 Limitations of liability

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

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

CertSIGN shall not be liable to any person (beneficiary, subject, third party, partner entity, etc.) if the data submitted when issuing certificates are false, inaccurate, incomplete or out of date. 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.
In any case certSIGN's liability in the event of a claim for damages shall be limited to the value of the certificates involved in causing the damage.

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

9.10 Term and termination

9.10.1Term

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.

9.10.2Termination

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

9.10.3Effect of termination and survival

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

9.11 Individual notices and communications with participants

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

9.12 Amendments

9.12.1Procedure for amendment

certSIGN is responsible via its Policies and Procedures Management Body for the approval and change of the present CPS. The CPS is reviewed at least once a year.

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

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

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

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

9.12.2Notification mechanism and period
All changes to the present CPS under consideration by the PPMB shall be disseminated to interested parties before publication. The effective date is indicated on the title page of the present CPS.

9.12.3 Circumstances 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

9.16.1 Entire Agreement
No stipulation.

9.16.2Assignment
No stipulation.

9.16.3Severability
CA acts as specified in paragraph "9.16.3 Severability" from CA/B Forum Baseline Requirements.

9.16.4Enforcement
No stipulation.

9.16.5Force Majeure
CA acts conforming to Romania Laws regarding Force Majeure.

9.17 Other provisions
No stipulation.