Certification Practice Statement
certSIGN ROOT CA

Version 1.45
Date: 15 January 2026

Important Notice

This document is the property of certSIGN SA

Distribution and reproduction without the consent of certSIGN SA are prohibited

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	April 2006	First version publishing	Electronic Services Manager
1.1	July 2006	1 year term for reviewing the classification	Electronic Services Manager
1.2	August 2008	The function responsible for administering the CPS and his contact data	Electronic Services Manager
		Detalils about protecting and backup of customers encryption private keys	Electronic Services Manager
		certSIGN position regarding the use of trademarks in the digital certificates issued	Electronic Services Manager
		For the moment certSIGN does not use external Ras	Electronic Services Manager
		certSIGN does not provide certificate suspension services	Electronic Services Manager
		The error messages in response to OCSP validation requests are not digitally signed	Electronic Services Manager
		certSIGN does not implement tokens/smartcards lifecycle management processes	Electronic Services Manager
		More details provided about the disaster recovery site	Electronic Services Manager
		certSIGN does not provide subscriber key management services	Electronic Services Manager
		certSIGN does not provide certificate rekey services	Electronic Services Manager
1.3	February 2009	Description of the process at RA to verify the owner of the domain for ssl certificates.	Electronic Services Manager
		Description of the process at RA to verify that the email account associated with the email address in the cert is owned by the subscriber	Electronic Services Manager
1.4	July 2009	Change of company's address	Electronic Services Manager
1.5	October 2009	Introduction of prerequisites for third party operated subordinate Cas	Electronic Services Manager
1.6	July 2011	The information reqarding the suspension services were updated	Electronic Services Manager
1.7	September 2011	The conditions of moving to 2048 bits and other measures for increasing the security of the cryptographic algorithms used by certSIGN	Electronic Services Manager
1.8	March 2014	The header was modified. A mention was introduced on verifying the domains of server certificates using the new gTLD and ccTLD from ICANN. Mentions were introduced regarding the SSL OV wildcard certificates and the Unified Communications ones. Setting up of a new CA, certSIGN Enterprise CA Class 3 G2. The certificates	Technical Director

[1] *The effective date is the last day of the month*

		issued with this class can be used to secure binary objects and to protect digital communications using IPSEC, SSL and TLS protocols.	
1.9	August 2014	The father's initial was excluded from the certificate's format. The use of a hyphen to separate first and last names consisting of more words was adopted.	Conformity and IT Security Officer
1.10	July 2015	The new certification authorities were added: certSIGN CA Class 2 G2 certSIGN Qualified CA Class 3 G2 certSIGN Non-Repudiation CA Class 4 G2	Technical Director
1.11	December 2015	The validity period for demo and class 2 certificaets (Table 6.3.2.2) was modified to unspecified for the former, and to 1,2 or 3 years for the latter.	Technical Director
1.12	10 January 2016	Adding the new closed circuit certification authorities that issue certificates for the Electronic Payment System operated by Transfond S.A.	Technical Director
1.13	25 January 2016	Adding a new certification authority designed for issuing code signing certificates. The OID for Non-EV Code Signing 2.23.140.1.4.1. was introduced in the description of the certification policy. Also, the OV 2.23.140.1.2.2. OID was included in the certification policy associated to SSL certificates.	Technical Director
1.14	20 July 2017	The correspondence between our practices and procedures for domain validation and those required by Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates v1.4.1 al CA/Browser Forum the were indicated. The annual review of CPS was made mandatory. The annual review of CPS was made.	
1.15	1 September 2017	A dedicated email address was created for certificate problem report. A new subchapter was added to the Certificate Revocation and Suspension chapter, dedicated to certificate problem reporting.	
1.16	26 November 2017	Clarification of the procedure for the verification of attributes of the subject/organization that appear in the certificate. Introoduction of the "commitment to comply" with the CAB Forum's BR.	
1.17	March 2018	CPS aligned with CA/Browser Forum BR 1.5.6 and version 2.5 of Mozilla Root Store Policy	PKI Policies Manager
1.18	May 2018	CPS compliance with RFC 3647 and GDPR recommendations	PKI Policies Manager

1.19	Iulie 2018	CPS compliance with CA-Browser Forum, about validating the Applicant's ownership or control of the domain	PKI Policies Manager
1.20	September 2018	CPS update with new profiles certificate	PKI Policies Manager
1.21	September 2018	CPS update to remove certified profiles	PKI Policies Manager
1.22	November 2018	CPS update change headquarters	PKI Policies Manager
1.23	January 2019	Annual review Updates determined by removal character underscore "_" in the domain name / dNSName -CA / B Forum / BR 1.6.2	PKI Policies Manager
1.24	September 2019	CPS update with validity certificate certSIGN Enterprise CA Class 3 G2	PKI Policies Manager
1.25	January 2020	Annual review. Minor updates for compliance with CA/Browser Forum BR 1.6.7 and Mozilla Policy v2.7.	PKI Policies Manager
1.26	May 2020	Add validation method 3.2.2.4.2	PKI Policies Manager
1.27	May 2020	Fix OCSP updates, SSL validity 1 year, & add identify method in Table 3.2.3	PKI Policies Manager
1.28	September 2020	CRL & OCS ReasonCode on 7.2 & 7.3	PKI Policies Manager
1.29	January 2021	Annual Review	PKI Policies Manager
1.30	March 2021	Updates with DV & EV CAs (WebTrust NC)	PKI Policies Manager
1.31	May 2021	Add Private Key compromise methods	PLI Policies Manager
1.32	May 2021	Update the PKI Authorities schema	PKI Policies Manager
1.33	July 2021	Removed referrences to md5 & sha1	PKI Policies Manager
1.34	September 2021	Ballot SC42/47/48 + High Risk Cert. Requests + FQDN + OU	PKI Policies Manager
1.35	November 2021	Updates on domain validation methods	PKI Policies Manager
1.36	January 2022	Annual Review	PKI Policies Manager
1.37	June 2022	Updates ref. CAs (WebTrust NC), revocation reasons, SSL validity	PKI Policies Manager
1.38	October 2022	Add CRL Reason	PKI Policies Manager
1.39	January 2023	Annual Review	PKI Policies Manager
1.40	July 2023	Update links & updates acc. CABF BR	PKI Policies Manager
1.41	January 2024	Annual Review	PKI Policies Manager
1.42	18 April 2024	Add cross-certificate	PKI Policies Manager
1.43	15 January 2025	Annual Review	PKI Policies Manager
1.44	15 April 2025	Updates Domain email, ACME & MPIC	PKI Policies Manager
1.45	15 January 2026	Annual Review	PKI Policies Manager

This document was created and is the property of:

Owner	Author	Date created
Electronic Services Manager	Electronic Services Manager	27 January 2006

Distribution List

Destination	Date distributed
Public-Internet	24 March 2014
Public-Internet	25 August 2014
Public-Internet	3 July 2015
Public-Internet	27 December 2015
Public-Internet	10 January 2016
Public-Internet	25 January 2016
Public-Internet	20 July 2017
Public-Internet	1 September 2017
Public-Internet	26 November 2017
Public-Internet	31 March 2018
Public-Internet	24 May 2018
Public-Internet	31 July 2018
Public-Internet	14 September 2018
Public-Internet	27 September 2018
Public-Internet	26 November 2018
Public-Internet	31 January 2019
Public-Internet	16 September 2019
Public-Internet	31 January 2020
Public-Internet	11 May 2020
Public-Internet	21 May 2020
Public-Internet	30 September 2020
Public-Internet	29 January 2021
Public-Internet	23 March 2021
Public-Internet	11 May 2021
Public-Internet	25 May 2021
Public-Internet	02 July 2021
Public-Internet	10 September 2021
Public-Internet	23 November 2021
Public-Internet	31 January 2022
Public-Internet	6 June 2022
Public-Internet	6 October 2022
Public-Internet	31 January 2023
Public-Internet	31 July 2023
Public-Internet	31 January 2024
Public-Internet	18 April 2024
Public-Internet	15 January 2025
Public-Internet	15 April 2025
Public-Internet	15 January 2026

This document was approved by:

Version	Name	Date
1.0	Policies and Procedures Management Body	April 2006
1.1	Policies and Procedures Management Body	July 2006

1.2	Policies and Procedures Management Body	August 2008
1.3	Policies and Procedures Management Body	February 2009
1.4	Policies and Procedures Management Body	July 2009
1.5	Policies and Procedures Management Body	October 2009
1.6	Policies and Procedures Management Body	July 2011
1.7	Policies and Procedures Management Body	August 2011
1.8	Policies and Procedures Management Body	March 2014
1.9	Policies and Procedures Management Body	August 2014
1.10	Policies and Procedures Management Body	June 2015
1.11	Policies and Procedures Management Body	December 2015
1.12	Policies and Procedures Management Body	December 2015
1.13	Policies and Procedures Management Body	January 2016
1.14	Policies and Procedures Management Body	July 2017
1.15	Policies and Procedures Management Body	August 2017
1.16	Policies and Procedures Management Body	November 2017
1.17	Policies and Procedures Management Body	March 2018
1.18	Policies and Procedures Management Body	May 2018
1.19	Policies and Procedures Management Body	July 2018
1.20	Policies and Procedures Management Body	September 2018
1.21	Policies and Procedures Management Body	September 2018
1.22	Policies and Procedures Management Body	November 2018
1.23	Policies and Procedures Management Body	January 2019
1.24	Policies and Procedures Management Body	September 2019
1.25	Policies and Procedures Management Body	January 2020
1.26	Policies and Procedures Management Body	May 2020
1.27	Policies and Procedures Management Body	May 2020
1.28	Policies and Procedures Management Body	September 2020
1.29	Policies and Procedures Management Body	January 2021
1.30	Policies and Procedures Management Body	March 2021
1.31	Policies and Procedures Management Body	May 2021
1.32	Policies and Procedures Management Body	May 2021
1.33	Policies and Procedures Management Body	July 2021
1.34	Policies and Procedures Management Body	September 2021
1.35	Policies and Procedures Management Body	November 2021
1.36	Policies and Procedures Management Body	January 2022
1.37	Policies and Procedures Management Body	June 2022
1.38	Policies and Procedures Management Body	October 2022
1.39	Policies and Procedures Management Body	January 2023
1.40	Policies and Procedures Management Body	July 2023
1.41	Policies and Procedures Management Body	January 2024
1.42	Policies and Procedures Management Body	April 2024
1.43	Policies and Procedures Management Body	January 2025
1.44	Policies and Procedures Management Body	April 2025
1.45	Policies and Procedures Management Body	January 2026

Content

1 Introduction

certSIGN ROOT CA PKI system is on the end-of-life, and it is not issuing anymore certificates.

Certification Practice Statement certSIGN ROOT CA – (further referred as **CPS**) describes the process of public key certification and the applicability range of the certificates resulting from this certification. The CPS is particularly important from the point of view of a Subscriber and a Relying Party. The **CPS** describes the general rules of certification practice stated in the **Certification Policy of certSIGN** (further referred as **Certification Policy** or **CP**). The **Certification Policy** describes what level of trust can be applied to a given type of a certificate issued by **the Certification Services Provider certSIGN** (further referred as **certSIGN**). The **CPS** describes how certSIGN secures the level of trust guaranteed by the policy.

The CPS describes four certification policies applied by certSIGN to issue the certificates for authorities and end users. These policies represent four different levels of credibility (**Class 1, Class 2, Class 3, and Class 4**) corresponding to public key certificates. The applicability ranges of certificates issued in compliance with these policies might be the same. However, the responsibilities (also from legal point of view) of the Certification Authority and of the certificate users are different. The CPS assumes that the reader is familiar with the notions regarding the certificates, electronic signature and Public Key Infrastructure (PKI).

There are many additional documents related to the CPS. These are used by the Certification Authorities of certSIGN to regulate the way they function. Thus these documents have a different status and they are not publicly available due to the importance of the information contained for the system's security. Additional information about the Certification Practice Statements can be obtained by electronic mail from the Electronic Services Manager at the address: office@certSIGN.ro

This document conforms to the latest published version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (https://cabforum.org/baseline-requirements-documents/) and latest published version of Mozilla Root Store Policy.

In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

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

1.1 Overview

The CPS is the ground for **certSIGN** and Certification Authority, Registration Authority and associated Relying Parties' functioning. As well, this document describes the general rules of certification services delivery such as Subscriber's registration, public key certification, key and certificates renewal and certificate revocation.

The Public Key Infrastructure (PKI) architecture of **certSIGN** is divided into two levels (see Figure 1.1). Level 1 contains the **certSIGN ROOT CA**. The Certification Authorities on Level 2 are directly signed by **certSIGN ROOT CA**. **certSIGN ROOT CA** operates only off-line. If level 2 certification authorities are compromised, **certSIGN ROOT CA** will be used to revoke their certificates and to issue new certificates.

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.

Certificate status services are available 24 hours per day, 7 days per week. certSIGN 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.

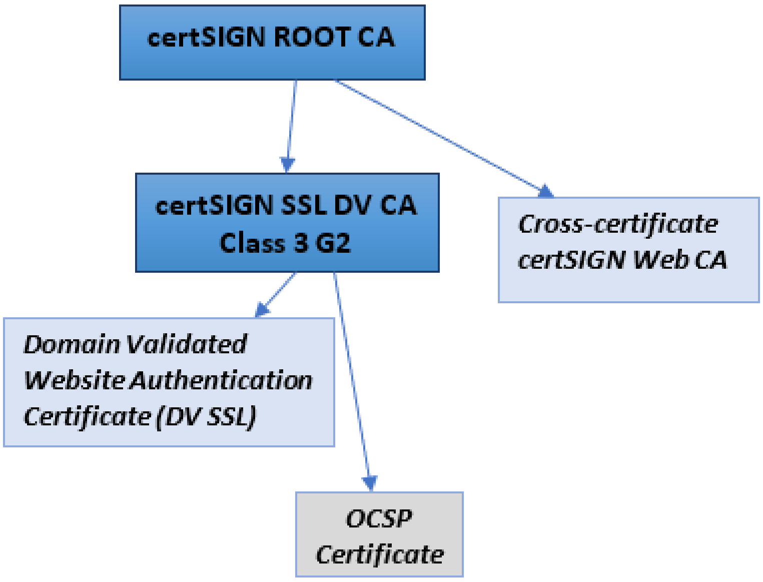
certSIGN ROOT CA
certSIGN SSL DV CA Class 3 G2
Cross-certificate certSIGN Web CA
Domain Validated Website Authentication Certificate (DV SSL)
OCSP Certificate

Figure 1.1. The Certification Authorities issuing certificates operating inside PKI certSIGN ROOT CA

In terms of hierarchy, following Certification Authorities are immediately subordinated to **certSIGN ROOT CA**:

- certSIGN SSL DV CA Class 3 G2
- certSIGN Web CA – cross-certificate

all issuing certificates with different levels of credibility.

The certificates issued by certSIGN contain the identifiers of the certification policy enabling the Relying Parties to settle if the checked certificate was used in compliance with the declared purpose. The declared purpose is mentioned based on the values in the field *PolicyInformation* of the extension *certificatesPolicies* (see Chapter 7.1.1.2) from every certificate issued by certSIGN.

Certificate types issued by every Certification Authority are described in Table 1.1.

Class	Type	Subtype
Class 1 (Demo)	Simple demonstrative certificate	
	Code signing demonstrative certificate	
	Web servers demonstrative certificate	
	VPN gateways demonstrative certificate	
	CA servers demonstrative certificate	

	TSA server demonstrative certificate	
	Validation servers (OCSP) demonstrative certificate	
Class 2	Simple certificate	Simple certificate for authentication and signing ▪ without SS-CD and key generated by the Subscriber ▪ without SS-CD and key generated by certSIGN ▪ with SS-CD and key generated by the Subscriber ▪ with SS-CD and key generated by certSIGN Simple certificate for encryption ▪ without SS-CD and key generated by the Subscriber ▪ without SS-CD and key generated by certSIGN ▪ with SS-CD and key generated by the Subscriber ▪ with SS-CD and key generated by certSIGN Simple certificate for signing and encryption ▪ without SS-CD and key generated by the Subscriber ▪ without SS-CD and key generated by certSIGN ▪ with SS-CD and key generated by the Subscriber ▪ with SS-CD and key generated by certSIGN
Class 3 Qualified	Qualified certificate	Qualified certificate ▪ with SS-CD and key generated by the Subscriber ▪ with SS-CD and key generated by certSIGN
Class 3 Enterprise	Trusted encryption certificate	Trust encryption certificate ▪ with SS-CD and key generated by the Subscriber ▪ with SS-CD and key generated by certSIGN
	Web servers certificate	
	VPN gateways certificate	
Class 4	CA servers certificate	
	TSA server certificate	
	Validation servers (OCSP) certificate	

Table 1.1. Types of certificates

1.2 Document name and identification

The document name is **Certification Practice Statement certSIGN ROOT CA** and it is available in electronic format within the Repository at address https://www.certsign.ro/en/document/certsigns-certification-practice-statement/ or based on a request sent to office@certsign.ro.
This document conforms to the latest published version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at https://cabforum.org/baseline-requirements-documents/ and latest version of Mozilla Root Store Policy, Apple Root Certificate Program, Microsoft Trusted Root Program and Chrome Root Program Policy; the structure and content of the CPS are in compliance with RFC 3647 recommendations.
In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

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:

- Certification Authorities:
  - certSIGN ROOT CA,
  - certSIGN SSL DV CA Class 3 G2

    - certSIGN Web CA - cross
- Registration Authority,
- The Repository,
- Online certificate status protocol (OCSP)
- Subscribers,
- Relying Parties.

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 ROOT CA** is a Primary Certification Authority for the certSIGN domain. All the other Certification Authorities in this domain are subordinated to the certSIGN ROOT CA (see Figure 1.3).
Currently, the following active Certification Authorities are subordinated to the certSIGN ROOT CA: **certSIGN SSL DV CA Class 3 G2, certSIGN Web CA - cross;**.

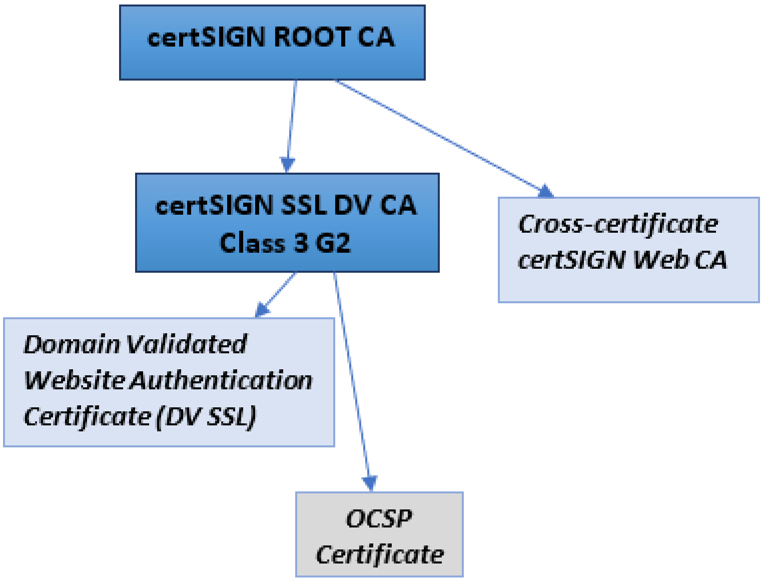
certSIGN ROOT CA
certSIGN SSL DV CA Class 3 G2
Cross-certificate certSIGN Web CA
Domain Validated Website Authentication Certificate (DV SSL)
OCSP Certificate

Figure 1.3. Structure of certification domain certSIGN ROOT CA

The Primary Certification Authority, **certSIGN ROOT CA**, can register and issue certificates only to Certification Authorities and authorities that issue electronic confirmations of non-repudiation that belong to the certSIGN domain. Before beginning the activity, every Intermediate Certification Authority must send a request to the Primary Certification Authority, **certSIGN ROOT CA** for registration and public key certificate issuance (see also the procedures described in chapter 6.1 of the *present CPS*). **certSIGN ROOT CA** authority operates based on a *self-signed* certificate issued by itself. In such a certificate the **certificatePolicies** extension is missing (see Chapter 7.1.1), which means that there are no limitations for the set of **certification paths** to which certSIGN ROOT CA certificate can be attached.
certSIGN ROOT CA Certification Authority is a **point of trust** for certSIGN's customers. Thus, every certification path must start with the certSIGN ROOT CA authority's certificate.
certSIGN ROOT CA Certification Authority renders certification services to:

- itself (issues and renews own certificates),
- the Certification Authorities registered in the certSIGN certification domain,
- entities that provide on-line certificate status verification services and other entities that provide non-repudiation services (such as time stamp services).

The Intermediate Certification Authorities **certSIGN SSL DV CA Class 3 G2**, issued certificates to Subscribers in compliance with the policies with the identifiers from Table 1.3.

Certification Authority	Certification Policy
certSIGN SSL DV CA Class 3 G2	**{certSIGN} id-policy(1) id-cp(1)id-DV-CA(5) {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) domain-validated(1)} (2.23.140.1.2.1)**

Table 1.3. Names of the Certification Authorities and corresponding certification policies

Intermediate Certification Authorities are configured to issue certificates to:

- suppliers of services connected with mobile telecommunications,
- network devices providing encrypted connections over VPN,
- hardware devices owned by private or legal entities to provide services based on public key certificates such as on-line certificate status verification (OCSP),
- other Certification Authorities.

Any external entity wishing to operate a CA subordinated to the certSIGN ROOT CA has to sign first an agreement stating its obligations to follow the current CP and CPS versions and to pass an external audit for verifying compliance with the WebTrust for CA standard, or equivalent.

1.3.2 Registration Authority

Registration Authority receives, checks and approves or rejects the registration and certificate issuance, certificate renewal and revocation requests. Verification of applications intends to authenticate (based on the documents enclosed to the applications) both the solicitor and the data specified in the request. Registration Authority can submit applications to the corresponding Certification Authority – to cancel a Subscriber's request and to withdraw his certificate.

The level of precision of the customer's identity identification process results from the Subscriber's needs and it is imposed by the level of the certificate requested by the Subscriber (see Chapter 3). In the case of the simplest identification a Registration Authority checks only the correctness of the submitted e-mail address. The most precise identification requires the subscriber's attendance in person to one of the Registration Authority and submission of proofs for his identity. The identification might be done either automatically or manually by one of the Registration Authority's operators.

Registration Authority functions on the basis of the authorization obtained from certSIGN Certification Authority.

The RA carries out the above activities directly or with the contribution of the delegated registration authorities. In all cases, the certSIGN remains responsible.

Unless otherwise specified in this document, the "RA" covers the registration authority and the delegated registration authorities.

1.3.3 Subscribers

The Subscriber is an entity whose identifier is placed in the field *Subject* of a certificate and who does not issue a certificate to other entities. A Relying Party is an entity that uses the certificate of a Subscriber and may check its electronic signature to ensure the confidentiality of the information sent.

Any natural or legal entities, as well as hardware devices owned by them can be Subscribers of certSIGN – CA, provided that they fulfill the terms of the Subscriber's definition.

In particular, the Registration Authority's operators, certSIGN's employees and indispensable equipment to ensure the quality of certSIGN's security (firewalls, routers, and authentication servers) represent Beneficiaries.

The organizations that want to obtain certificates issued by certSIGN for their employees ought to do it by means of their representatives, whereas the individual Subscribers must ask themselves a certificate.

certSIGN issues different types of certificates and of different credibility levels. Subscribers must decide what type of certificate is the most suitable for their needs (see Chapter 1.3.1).

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 Subscriber's identity and the public key (connection confirmed by one of the Certification Authorities subordinated to certSIGN ROOT CA).

A Relying Party is responsible for how it is checked the current status of a Subscriber's certificate. Such a decision must be taken every time a Relying Party is willing to use a certificate to check an electronic signature, to check the identity of the source or the author of a message or to create a secret communication channel with the owner of the certificate.

A Relying Party must use the information in a certificate (for example, identifiers and qualifiers of certification policy) to decide whether a certificate was used according to the stated purpose.

1.3.5 Other Participants

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

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

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

Qualified Electronic Signature Devices Providers: External providers that support certSIGN activities under a signed contractual agreement that provides the provision of physical cryptographic devices used by the Subjects.

Delegated Registration Authority (DRA): The CA may rely on a DRA to outsource some of the functions of the RA. A DRA operator has the power to:

- requests the generation or renewal of the certificate;
- requests the revocation of the certificate;

It works for the authority, in the context of issuing the certificate, verify the identity of the future subscriber to the certificate under the same conditions and with the same level of security as those required for the RA operator.

The DRA operator's commitments to the CA are specified in an agreement drawn up and signed with the responsible entity of the operator. The agreement specifies that the operator must carry out an impartial and scrupulous verification of the identity and possible attributes and services of the Subscriber. The DRA operator must also comply with its parts of the CPS.

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 (for example, electronic signature, confidentiality),
- The other is a list or a description of the allowed and prohibited applications.

Certificates issued by certSIGN can be used to process and ensure the information security (including authentication) with different credibility levels. The credibility level of information and its vulnerability must be assessed by the Subscriber. In the Certification Policy and the CPS hereby are defined four levels of sensibility: Class 1 (test level), Class 2 (basic level), Class 3 (intermediate level), and Class 4 (high level). These levels correspond to the four credibility levels of the certificates (see Table 1.4).

Information Sensitivity Level	Certification Policy Name	Applicability Area
Class 1 (test)	certSIGN Class 1	The lowest credibility level for the identity of an entity. Class 1 certificates are recommended to be used to test the compatibility of certSIGN's services with those provided by other suppliers of PKI services and to test the certificates' functionality inside the tested applications. As well, these certificates can be used for other purposes as long as ensuring the credibility of the sent or received messages is not important.
Class 2 (basic)	certSIGN Class 2	This level provides basic security for information in environment of slight risk (risk without major consequences). From these we mention the access to private information where the probability of an unauthorized access is not really big. These certificates can be used to authenticate and control the integrity of the information that was signed on to insure information confidentiality especially in case of electronic mail.
Class 3 (intermediate)	certSIGN Class 3	This level is recommended to ensure the information security in environments where the risk of security breaches exists and their consequences are moderate. Certificates might be used to protect the financial transactions or the transactions with risk of frauds occurrence. As well, these certificates can be used to create extended electronic signatures.
Class 4 (high)	certSIGN Class 4	This level corresponds to environments where the chances of data compromising are very high and where the consequences of a security incident are very serious. These certificates might be used to protect transactions of unlimited value (unless it is stated differently in a certificate) and transactions with high level of fraud occurrence.

Table 1.4. Sensitivity level of information and policy name

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 must decide what type of certificate issued by certSIGN meets the formulated requests. Subscribers must 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

certSIGN issues 9 basic types of certificates with different applicability areas. These are:

1. **certificates for Certification Authorities** – their usage is not restricted to a definite area; the applicability area might result from the extension in the certificate that settles how the private key may be used (see the field **keyUsage**, Chapter 7), or its role (for example, Subscriber, Certification Authority or other authority that provides PKI services); this type also contains operational certificates of the Certification Authorities;
2. **certificates for server authentication confirmation** – are used by services that operate based on SSL/TLS/WTLS protocols;
3. **certificates confirming certificate status** – they are issued for servers that function in compliance with OCSP protocol and provide information regarding the certificates' status;

Certificates issued in compliance with one of the four certification policies may be used in applications that satisfy at least the following conditions:

- manages **properly** the public and private keys,
- certificates and associated public keys are used in compliance with their declared purpose, confirmed by certSIGN,
- have built-in mechanisms of certificate status verification, certification path creation and validation control (signature availability, expiration date etc.),
- provides relevant information regarding certificates and their status for users.

The list of recommended applications (by certSIGN) is published on site at address: https://www.certsign.ro/en/products/eidas-trust-services/applications/

The applications are included in the list of applications recommended based on written statements of producers and/or tests made by certSIGN. certSIGN allows every Subscriber to generate himself the cryptographic keys used during certification process by means of recommended devices. The Certification Authority may also generate keys on a cryptographic device and then to deliver the device along with the keys to the Subscriber. Thus, certSIGN uses cryptographic devices that comply at least with the FIPS PUB 140-2 standard requirements.

1.4.2 Prohibited certificate uses

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

1.5 Policy Administration

1.5.1 Organization administering the document

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

Name	S.C. certSIGN S.A. Office: Address: 29 A Tudor Vladimirescu Avenue, AFI Tech Park 1, Bucharest, Romania Register Number: J2006000484402 Tax registration code: RO 18288250 Registered office: 107A Oltenitei Street. building C1, floor 1, room 16, Sector 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.

Subjects/Subscribers shall adhere to the CPS published at:

https://www.certsign.ro/en/document/certsigns-certification-practice-statement/

Subjects/Subscribers who do not accept new, modified terms and regulations of CPS are obligated to make a suitable statement within 15 days of the date of the new version of CPS approval. This thing results in 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-Certified Subordinate CA Certificate: A certificate that is used to establish a trust relationship between two CAs.

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

Delegated Third Party: A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits, but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

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

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

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

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

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

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

(i) the Internet Corporation for Assigned Names and Numbers (ICANN),

(ii) a national Domain Name authority/registry, or

(iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

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

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

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

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

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

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

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

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

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

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

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

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

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

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

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

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

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.

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

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

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

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

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

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

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

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

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

Request Token: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request.
The Request Token SHALL incorporate the key used in the certificate request.
A Request Token MAY include a timestamp to indicate when it was created.
A Request Token MAY include other information to ensure its uniqueness.
A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.
A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.

A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation.
The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.6.2 Acronyms

Acronim	**Original**
AICPA	American Institute of Certified Public Accountants
ADN	Authorization Domain Name
CA	Certification Authority
CAA	Certification Authority Authorization
CARL	Certification Authority Revocation List
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
DV	Domain Validated
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
IM	Instant Messaging

Acronim	Original
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validated
PKI	Public Key Infrastructure
PPMB	Policies and Procedures Management Body
QSCD	Qualified Electronic Signature Creation Device
QWAC	Qualified Certificate for Website Authentication
RA	Registration Authority
RSA	Rivest, Shamir, Adleman asymmetric cryptographic algorithm
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TSP	Trust Services Provider
UTC	Coordinated Universal Time
VoIP	Voice Over Internet Protocol

2 Publication and Repository Responsibilities

2.1 Repositories

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

- Certificate Policy and Certificate Practice Statement for the ROOT CA and CAs operated by certSIGN https://www.certsign.ro/en/document/certsigns-certification-practice-statement/
- 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/
    - 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 Certification Policy, of the CPS, the 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 questions to HTTP,
- 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 Certification Policy,
- Ensure secure and controlled access to information in the Repository.

Liability for Repository service and its service consequences belong to certSIGN (see Chapter 9).

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.

The Repository is a public interface to the following information:

- The current and previous versions of the CPS and the Certification Policy
- Templates for contracts with the Subscribers and Relying Parties,
- certSIGN's statement regarding the insuring of confidentiality of the information received and processed
- the register (as in the electronic signature law)
- the certificates certSIGN ROOT CA, certSIGN SSL DV CA Class 3 G2, as well as the certificates of all Certification Authorities that belong or are connected to the certSIGN domain (for example, certificates of the Certification Authorities newly registered by RA),
- end subscribers' certificates (natural and legal entities, including certSIGN's employees and machines / software applications owned by them and which are indispensable for PKI services) in compliance with the electronic signature law.

Additionally, in the Repository there is information related to the certificates' functioning, such as:

- The Certificates Revocation List (CRL); The CRLs are available in the so called CRL distribution points which addresses are specified in each certificate issued by certSIGN; the main CRLs distribution point is in the Repository at the url: https://www.certsign.ro/en/resources/certificate-revocation-list/
- Other information that changes in real time,

The content of the Repository is available via Internet on the address: https://www.certsign.ro/en/repository/ or by means of LDAP v3 protocol, on the address ldap.certsign.ro, port 389

2.3 Time or frequency of publication

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

- Certification Policy and CPS – see Chapter 1.5,
- Certificate of the Certification Authorities – after issuing a new certificate;
- Certificate of the Registration Authority – after issuing a new certificate;
- Subscribers' certificates – on certificate approval, after every issue of a new certificate;
- Certificate Revocation List – see Chapter 4.9.7;
- Audit reports performed by authorized institutions – when certSIGN receives them;
- Additional information – after every update.

2.4 Access controls on repositories

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

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

Beneficiaries, Subjects and Partner Entities have read-only access via the Internet to all repositories mentioned in section 2.1.

certSIGN may take reasonable steps to protect against and prevent the misuse of the repository, OCSP or 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

The chapter hereby describes general rules for checking the Subscriber's identity, rules that apply when issuing a certificate by certSIGN. These are based on information included in certificates and mention the indispensable means to ensure that the information is precise and credible when issuing the certificate.

The checking is mandatory performed in the stage of Subscriber's data registration and modification as well as upon certSIGN's request in case of any other certification service. The type of verification depends on the type of certificate. The basic principle that is followed is that all information that is supplied by the certificate subscriber MUST be verified by using an independent source of information or an alternative communication channel before it is included in the certificate.

3.1 Naming

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

certSIGN does NOT allow 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 Subscriber's name in compliance with X.509 standard (with referring to X.500 series' recommendations). Basic names of the Subscribers 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 Subscribers 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 Subscriber.

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

The names of the directories where the certificates, the CRLs and the Certification policy are stored, as well as the names of the distribution points of the CRLs, comply with the provisions of LDAP protocol regarding the name syntax (see RFC 1778).

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

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 current version. FQDN consists solely of P-Labels and Non-Reserved LDH Labels.

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

For SSL certificates, while FQDN or an authenticated domain name 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.

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) must not 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.

3.1.2 Need for names to be meaningful

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

For private entities (natural persons or company's employees), DN consists of the following fields, mandatory or not (the description of the field is followed by its abbreviation that complies with RFC 3280 and X.520 recommendations):

- Field C – international abbreviation for country name (RO for Romania),
- Field S – county / district where the Subscriber lives,
- Field L – residence city of the Subscriber,
- Street – address,
- Field CN – Subscriber's name; name of a product or equipment that might also be mentioned here,
- Field O – name of the institution where the Subscriber works, in case it is a professional certificate
- Field OU – name of the department[2] where the Subscriber is hired, in case it is a professional certificate
- Field T – function
- Field SN – Subscriber's surname,
- Field G – Subscriber's first name,
- Field P – Subscriber's nickname used in his environment or which wants to use not to disclose his real first name or surname,
- Field Phone – phone number,
- Field Serial Number – personal identification code of the Subscriber related to the Digital signature law.

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

- Field C – international abbreviation for country name (RO for Romania),
- Field O – name of the institution,
- Field OU – name of the organization's department[3],
- Field S – county / district where the organization functions,
- Field L – residence city of the Subscriber,
- Field CN – name of the institution,
- Field Phone – phone number,

The name of the Subscriber must 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.

[2] *Forbidden for SSL certificates issued on or after 1 September 2022*

[3] *Forbidden for SSL certificates issued on or after 1 September 2022*

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.

3.1.3 Anonymity or pseudonymity of subscribers

N/A

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 Distinctive Name (DN). *certSIGN ensures the uniqueness of the DN assigned to every Subscriber.*

The Subscriber's DN is suggested by him in his request. If the name is in accordance with the general requests mentioned in Chapters 3.1.1 and 3.1.2 an operator of the Registration Authority temporary accepts the suggestion. If the operator of the Registration Authority has access to the DN database this will also check the uniqueness of the name within certSIGN domain. If the test confirms the uniqueness the DN is accepted. In case of lack of access to certSIGN's database the decision concerning the acceptance or rejection of the DN is taken by the Certification Authority's operator.

If a suggested DN violates the rights of other entities to this name, certSIGN may add other attributes to the DN (for example, the serial number) that ensures the uniqueness of this name within certSIGN's domain. A Subscriber is entitled to refuse a DN suggested in the procedure mentioned in Chapter 4.4.

The form of the global unique name for a Subscriber is as it follows:

certSIGN.ro / issuer name /Subscriber name

where **certSIGN.ro** is the name of the certSIGN domain, the issuer's name is the DN of a Certification Authority and the Subscriber's name is the DN of the field *subject* within the certificate. The values of the last two fields are extracted from the certificate.

If a Subscriber renounces to certSIGN's services the possible request for assigning its DN to a Subscriber must be rejected.

certSIGN may register a Subscriber with a Distinctive Name used in the past by another Subscriber only with the written consent of the former.

For SSL certificates, the name's uniqueness is ensured by integrating in the Common Name attribute of a domain name that is approved by ICANN as being unique.

3.1.6 Recognition, authentication and role of trademarks

Certsign does not verify whether the Subscriber (the user / holder of a certificate) is the person on whose behalf the trademark is registered in the National Book of Trademarks or if it enjoys the right granted by the trademark owner to use it, the Subscriber being solely responsible for the correctness of the information provided in to issue the certificate. The State Office for Inventions and Trademarks is the specialized body of central public administration, the only authority that ensures the protection of trademarks and geographical indications in Romania. In accordance with the provisions of Law no. 84/1998 on trademarks and geographical indications, "The right to the trademark is acquired and protected by its registration at the State Office for Inventions and Trademarks" (Article 4). "

3.2 Initial Identity Validation

Subscriber registration takes place when a Subscriber requesting registration does not hold a valid certificate issued by any Certification Authority affiliated to certSIGN.

Registration involves a number of procedures that allow a Certification Authority - before issuing a certificate to a Subscriber - to gather valid data about a particular entity to identify it.

Each Subscriber undergoes a registration process only once. After verifying the data provided by a Subscriber, he is included in the list of authorized users of certSIGN services and is granted a public key certificate.

The checking is mandatory performed in the stage of Subscriber’s data registration and modification as well as upon certSIGN’s request in case of any other certification service. The type of verification depends on the type of certificate. The basic principle that is followed is that all information that is supplied by the certificate subscriber MUST be verified by using an independent source of information or an alternative communication channel before it is included in the certificate.

Every Subscriber that requests services specific to public key infrastructures and requests the issuing a certificate must (prior to certificate’s issuing):

- Fill in an on-line registration form or a document that may be downloaded from certSIGN’s Web site,
- Generate an RSA asymmetric key pair and provide the Registration Authority the prove of owning a private key; optionally, the Subscriber may delegate a Certification Authority or the Registration Authority to generate this key pair,
- Suggest a distinctive name (DN, see Chapter 3.1.1),
- Fill in and send a registration form that contains a public key and the prove of owning its corresponding private key,
- Optionally, attend the Registration Authority and provide the required documents (if required by the certification policy based on which the certificate is issued),
- Conclude an agreement with an agent on behalf of the Registration Authority concerning the services provided by certSIGN; the present CPS is part of this agreement.

The registration procedure might request the Subscriber or one of his representatives to personally contact the Registration Authority. Nevertheless, certSIGN allows sending the requests via mail, e-mail, Web sites, etc.

3.2.1 Method to prove possession of private key

If an entity owns a private key when it requests the issuing of a certificate, the Certification Authorities and the Registration Authority functioning inside certSIGN must ensure that the entity owns a private key corresponding to the provided public key.

The checking of the private key possession is made based on the so-called possession prove (DP) of the private key. These prove represent the confirmation that a public key undergoing the certification procedure is the pair of a private key owned exclusively by a Subscriber.

The form of the proof depends on the type of key pair that will be certified (key pair for creating an electronic signature for encrypting or for key negotiation).

The basic proof is realized by cryptographic mechanisms (electronic signature and / or encrypting) applied in the process of registration and modification of the data and recurrent on the renewal request of the key / certificate.

The request of presenting the possession proof of the private key does not apply if, on Subscriber’s request, the key pair is generated by the Certification Authority or by the Registration Authority.
It is recommended that the private keys should be generated inside a cryptographic device (token) or, in case they are generated outside the token, by means of a software or hardware generator following to be imported on token. Any entity may have a token when generating and importing the key or the token may be provided to the entity after the process of key generation. In the latter case, certSIGN warranties that the token and the key will securely reach straight to the respective entity

3.2.2 Authentication of organization identity

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

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

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

3.2.3 Authentication of individual Identity

Not applicable

3.2.4 Non-verified Subscriber information

Not applicable

3.2.5 Validation of authority

Not applicable

3.2.6 Criteria for interoperation

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

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Not applicable.

3.3.2 Identification and authentication for re-key after revocation

Not applicable.

3.4 Identification and authentication for revocation request

The following entities may apply to revoke a Subscriber's certificate:

- the subscriber, who owns the certificate,
- an authorized representative of the Certification Authority (in the case of certSIGN this role is reserved for the security administrator),
- a subscriber's mandate, for example his / her employer; The subscriber must be immediately informed of this,

- Registration Authority that may request revocation on behalf of a Subscriber or in its own name if it has information that warrants the revocation of the certificate.

The Registration Authority should act with caution when processing requests that have not been sent by a Subscriber and accepting only those requests in accordance with Chapter 4.9.1.

When the party requesting the revocation of the certificate is not the owner of the certificate (Subscriber), the Certifying Authority must:

- verify that the party is entitled to issue such a request
- request a justification for that request
- submit a notice to the Subscriber about revocation, or about initiating the revocation process.
- each application must be submitted:
- directly to the Certification Authority in electronic form, with or without confirmation of the Registration Authority,
- directly or indirectly (via the Registration Authority) to the Certification Authority, in non-electronic form (paper, fax, telephone, etc.)

4 Certificate life-cycle operational requirements

This chapter describes the basic procedures that are common to all types of Subject certificates within the certification process.

The in-depth procedures relating to PKI component services (CAs, RAs, CRLs signers, OCSP responder, Timestamping Authority, etc.) and the related personals/roles involved in the operational process of these components are described in internal confidential documentation. The following section provides a description of these documents that can be disclosed publicly.

In basic lines the certification process begins with the Subject: *indirectly* sending a request (after original confirmation of the request by the Registration Authority). Based on the request, the Certification Authority takes a decision concerning the provisioning / rejection of the service requested. The requests sent shall contain necessary information for correct identification of the Subject and Subscriber.

certSIGN provides access to the following basic services:

a. registration, certification, rekey;
b. certificate revocation;
c. verification of the certificate availability.

Work schedule

Services are rendered both on-line, and at the counter. Online services are rendered continuously while those at the counter are rendered from Monday to Friday, between 9 and 18. For all certificates classes, the certificate revocation services are rendered in maximum 24 hours from the request.

If the request submitted contains a public key, the key must be prepared so that the public key can be linked with other data specified in the request, in particular with the beneficiary identification data. A request may contain, instead of the public key, the Beneficiary's request to generate an asymmetric key in its name. This can be done by a certification authority or the registration authority. After generation, the keys are sent on a protected path to the subject so that they can not be activated by an unauthorized person.

4.1 Certificate Application

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 (for example, electronic signature, confidentiality),
- The other is a list or a description of the allowed and prohibited applications.

Certificates issued by certSIGN can be used to process and insure the information security (including authentication) with different credibility levels. The credibility level of information and its vulnerability must be assessed by the Subscriber. In the Certification Policy and the CPS hereby are defined four levels of sensibility: Class 1 (test level), Class 2 (basic level), Class 3 (intermediate level), and Class 4 (high level). These levels correspond to the four credibility levels of the certificates (see Table 1.4).

Information Sensitivity Level	Certification Policy Name	Applicability Area
Class 1 (test)	certSIGN Class 1	The lowest credibility level for the identity of an entity. Class 1 certificates are recommended to be used to test the compatibility of certSIGN's services with those provided by other suppliers of PKI services and to test the certificates' functionality inside the tested applications. As well, these certificates can be used for other purposes as long as insuring

Information Sensitivity Level	Certification Policy Name	Applicability Area
		the credibility of the sent or received messages is not important.
Class 2 (basic)	certSIGN Class 2	This level provides basic security for information in environment of slight risk (risk without major consequences). From these we mention the access to private information where the probability of an unauthorized access is not really big. These certificates can be used to authenticate and control the integrity of the information that was signed an to insure information confidentiality especially in case of electronic mail.
Class 3 (intermediate)	certSIGN Class 3	This level is recommended to ensure the information security in environments where the risk of security breaches exists and their consequences are moderate. Certificates might be used to protect the financial transactions or the transactions with risk of frauds occurrence. As well, these certificates can be used to create extended electronic signatures.
Class 4 (high)	certSIGN Class 4	This level corresponds to environments where the chances of data compromising are very high and where the consequences of a security incident are very serious. These certificates might be used to protect transactions of unlimited value (unless it is stated differently in a certificate) and transactions with high level of fraud occurrence.

Table 4.1 Sensitivity level of information and policy name

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 must decide what type of certificate issued by certSIGN meets the formulated requests. Subscribers must know the requests of the Relying Parties (for example, these requests might be published as a signature policy or an information security policy) and than to request certSIGN to issue certificates corresponding to these requests.

4.1.1 Who can submit a certificate application

Requests for one of the Certification Authorities may be sent directly by a Subscriber or indirectly by a Registration Authority's operator. Subscriber's applications are directly sent to a Certification Authority or indirectly to the Registration Authority. Applications sent directly may aim a certificate registration or modification; other applications concerning the certification services rendered by a Certification Authority are also allowed.

The operator may send to a Certification Authority the applications of other Subscribers confirmed by the operator and in well-founded cases even revocation requests for certificates belonging to Subscribers that violate the present CPS.

The applications are sent via communication protocols such as HTTP, S/MIME or TCP/IP.

certSIGN issues certificates only based on registration requests, modification, rekey, certificate renewal or modification sent by a Subscriber.

Applications may be submitted by different entities and may aim certificate which applicability depends on the entity's needs:

- Certificates for natural entities – issued as following the submission of a request by the representatives or employees of an organization that empowers them with the respective authorization.

- Certificates for devices (that apply to servers for instance) or certificates of the applications owned by the natural entities (employees of the organization or their agents) authorized to use that device or application.

4.1.2 Enrollment process and responsibilities

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

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

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

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

The Subject is provided with the following information which is part of the Subscribers' Agreement:

- The registration forms
- 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 deemed as formal acceptance by the Subject of the Subscriber Agreement whereby the Subject 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 from the date of certificate issuance for all the information related to the registration and enrolment, to the certificate request and to the certificate revocation
- That in case certSIGN (as CA and RA) ceases its activities, this data may be transferred to a third party, in accordance with the same terms and conditions as defined in the Subscriber Agreement,
- Acknowledges the rights, obligations and responsibilities of certSIGN and of other PKI Participants, as defined in the Subscriber Agreement and by national laws,
- That the Subject has the obligation to inform certSIGN on any change or event that may affect the validity or the content of the certificate

Enrolment Process

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

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

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

The RA is responsible for providing and/or verifying information regarding the Subscriber's/ Subject's attributes (professional attributes, organizational attributes, etc.). The RA verifies and completes the enrolment data. 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 Subjects and for supplying the CA with the correct content for the variable fields in the certificate.

4.2 Certificate application processing

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

The request sent on-line is realized via pages on the certSIGN's server on the address: https://www.certsign.ro. A Subscriber that visits the respective site fills in (in compliance with the instructions on site) a request form and sends it to a Certification Authority. Requests for certSIGN certificates Class 1 are automatically processed while requests for certificates with other levels are manually processed.

The requests for SSL certificates in electronic format may be transmitted through a secure authenticated channel, in which case they are processed automatically.

The request sent off-line may be done:

- By Subscriber's personal attendance or the attendance of the company's representative at the Registration Authority or at the Certification Authority, case when the request is filled in and hand signed, it is signed the agreement concerning certification services providing and it is generated a password which helps the Subscriber to manage the certificate and generate a PIN code for secured access to the cryptographic device that contains the keys and certificates.
- By sending via mail the request and the copies of the documents (in compliance with provisions in Table 3.1.8) necessary to check the solicitor's identity; the checking is followed by the generation of a password which helps the Subscriber to manage the certificate or generation of a PIN code for secured access to the cryptographic device that contains the keys and certificates; the cryptographic device is sent back to the solicitor (the PIN code is sent separated).

The off-line sending also concerns the collective requests. These requests are confirmed by a Certification or Registration Authority's operator and processed in group.

Request Processing in Registration Authority

Every request written on paper is processed (the processing must be done in the presence of the solicitor's if it is specified in the document hereby) as it follows:

- Registration Authority's operator receives the Subscriber's request
- The operator verifies the data from the request such as Subscriber's personal data (see the procedure described in Chapter 3.2.3) and verifies the existence of the proof of the private key possession (see Chapter 3.2.1),
- Following the verification, the operator confirms the identity between the data stated and those included in the request; if the request contains non-compliant data it is rejected,
- The request confirmed is sent to the Certification Authority,
- The Registration Authority checks also other data that are not specified in the request but they are also necessary for issuing the certificate.

Request Processing in the Certification Authority

The Certification Authority checks if the requests were confirmed by the Registration Authority.

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 in accordance with the procedure defined in Chapter 3.2 and in the confidential internal documentation.
The RA collects and validates information about the identity and attributes of the Subscriber and Beneficiary.
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 to verify certificate information for validation of Domain Names and IP Addresses according to Section 3.2.2.4 and 3.2.2.5, 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 HighRisk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified.

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

4.2.2 Approval or rejection of certificate applications

certSIGN can refuse a certificate issuance to any solicitor without taking any obligations or responsibility for the possible losses or damages affecting the Subscriber as following the denial. The Certification Authority will refund the solicitor the certificate fee (if he paid it), excepting the case when the solicitor mentioned false data in his request. The certificate issuance denial may occur in the following situations:

- If the Subscriber's identifier (DN) coincides with the identifier of another Subscriber,
- If there are suspicions or certainties concerning the forgery or usage of false data by the Subscriber,
- If the Subscriber, in an inconvenient manner, engages resources and processing means of certSIGN by submitting a number of requests clearly in excess of his needs,
- Other reasons besides those stated above.

Information concerning the denial decision for issuing a certificate and its reasons are sent to the solicitor. The solicitor may request again the issuance of a certificate only after the reasons that lead to the denial are solved.
From time to time, certSIGN may modify the requirements related to application information requested, based on certSIGN requirements, business context of the usage of certificates, or as it may be required by law.
Following successful completion of all required validations of a certificate application, certSIGN will approve an application.

If the information in the certificate application cannot be confirmed, then certSIGN will reject the certificate application. certSIGN reserves the right to reject an application for an certificate if, in its own assessment, the good and trusted name of certSIGN might be tarnished or diminished and may do so without incurring any liability or responsibility for any loss or expenses arising out of such refusal. certSIGN reserves the right not to disclose reasons for such a refusal.

Applicants whose applications have been rejected may subsequently re-apply.

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 received from the RA therefore the certificates are not immediately available to the Subscriber when the certificates are created by the CA.

The registration and certification or renewal request (key or certificates) will be examined, and the Certification Authority will issue a certificate during the period of time specified in Table 4.2.3. These periods depend on first hand on the accuracy of the data sent and the cooperation way between certSIGN and the solicitor.

Credibility level of the certificate	Expectation Period
certSIGN Class 1	1 day
certSIGN Class 2	5 days
certSIGN Class 3	5 days
certSIGN Class 4	5 days

Table 4.2.3. Maximum waiting period for certificate issuance

In case the necessary data are not made available for the Certification Authority in time, or it is necessary a completion of the documentation, the issuance term for the documentation will be extended.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

After receiving and processing a request (see Chapters 4.1 and 4.2) the Certification Authority issues a certificate.

Certificate issuance by the Root CA require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

A certificate is considered valid (in active status or prepared) when it is accepted by a Subscriber (see Chapter 4.4). The issued certificates' availability period depends on the certificate's type and the Subscriber's category and is compliant with the periods presented in Tables 6.3.2.1

certSIGN implemented its own certificate Linting tool, that uses also external Linting tools, to test the technical conformity of each to-be-signed artifact prior to signing it.

Every certificate is issued on-line. The procedure issuance is as it follows:

- The request processed is sent to the certificate issuance server,
- If the application contains the request to generate a key pair, the server asks the hardware key generator this thing,

- The quality of the public key generated/issued by the Certification Authority is tested
- If the procedures are successfully concluded, the server issues a certificate and delegates the security hardware module to sign the certificate; the certificate is stored in the database of the Certification Authority,
- The Certification Authority prepares the response containing the issued certificate (if it was issued) and sends it to the Subscriber; the certificate is not published in the Repository until the receiving of the Subscriber's confirmation concerning the certificate's acceptance (see Chapter 4.4).

4.3.2 Notification to Subscriber by the CA of issuance of certificate

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

- When the keys are generated on the QSCD by Certsign the QSCD where the digital certificate is stored is either delivered in person to the Subject or it is sent, using 34 postal or courier services, to the Subject. The secret activation data (i.e. PIN code) required to access the QSCD is sent using a tamper-evident envelope.

Every certificate issued is published in certSIGN's Repository. The certificate publication is equivalent with the notification of other Relying Parties about the fact that a certificate was issued for a Subject. certSIGN publishes a certificate in the Repository after the acceptance of the certificate by the Subscriber

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

When receiving a certificate, the Subscriber is committed to check its content, especially the data correctness and the complementariness of the public key with the private key he owns. If the certificate has any faults or mistakes that cannot be accepted by the Subscriber, the latter will immediately inform the Certification Authority concerning the certification revocation.

The certificate is considered accepted in case of occurrence of the following events in term of maximum 7 calendar days from the date of the certificate receiving by the Subscriber:

- The explicit acceptance of the issued certificate at the moment of obtaining the certificate from certSIGN's site
- Receiving a registered package (sent by certSIGN) containing the certificate

If a certificate is not rejected in 7 calendar days from its receiving then the certificate is considered accepted.

Every certificate accepted is published in certSIGN's Repository and is available for the public. Certificate acceptance is univocal to the Subscriber, prior to its usage an its applying to any cryptographic operation through which it is considered that he accepted the terms and conditions specified in the present CPS, Certification Policy and Service providing agreement. In case of electronic submission of the request, the solicitor automatically accepts the certificate at the moment of applying for this certificate.

By accepting the certificate, the Subscriber accepts the rules of the CPS and of the Certification Policy and agrees to follow the provisions of the agreement concluded with certSIGN.

4.4.2 Publication of the certificate by the CA

See chapter 2 "PUBLICATION AND REPOSITORY RESPONSIBILITIES"

4.4.3 Notification of certificate issuance by the CA to other entities

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

Subscribers must use the private key and certificates:

- consistent with the purpose stated in this Code of Practice and Procedure and in accordance with the content of the certificate (keyUsage and extendedKeyUsage fields, see Chapter 4.3);
- In accordance with the provisions of the agreement between the Subscriber and certSIGN,
- only during the validity period (does not apply to certificates for digital signature verification),

If the certificate is suspended, the Subscriber can not use the private key to create a signature until it is revoked.

Partner organizations must use public keys and certificates:

- consistent with the purpose stated in this Code of Practice and Procedure and in accordance with the content of the certificate (*keyUsage* and *extendedKeyUsage* fields, see Chapter 4.3);
- In accordance with the provisions of the agreement between the Subscriber and certSIGN,
- only after checking their status (see Chapter 4.8) and verifying the signature of the Certification Authority issuing that certificate.

4.5.2 Relying party public key and certificate usage

certSIGN assumes that all software applications comply with the X.509 standard, the SSL / TLS protocol, and other applicable standards that impose the requirements and set of requirements mentioned in this CPP. certSIGN does not guarantee that the software of any partner entity will support or impose such controls and requirements, and all partner entities are advised to identify appropriate technical and legal support.

Parties that rely on a certificate at any time verify a digital signature by checking the validity of a digital certificate using the OCSP service at http://ocsp.certsign.ro or the relevant CRLs published by certSIGN.

Partner organizations are warned that an unverified digital signature can not be attributed as a valid signature of the Beneficiary.

The final decision on the possibility of trusting or not in a verified digital signature is exclusive to the trusted party. Granting the trust of a digital signature should only take place if:

- The digital signature was created during the validity of a valid certificate and can be verified by sending a validated certificate.
- The Partner Entity verified the revocation status of the certificate by sending it to the relevant CRL and the certificate was not revoked.

- The Affiliate understands that a digital certificate is issued to a beneficiary for a particular purpose and that the private key associated with the digital certificate can only be used in accordance with the customary practices specified in this CPC and contained in the certificate.

Trust in the certificate is accepted as reasonable if the conditions set forth in the CPC and the contract with the Partner Entity are fulfilled. If the insurance provided by certSIGN in accordance with the provisions of this CPC is not met, the partner entity must obtain additional insurance.

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

Confidence in a non-verifiable digital signature can lead to risks that the partner entity assumes entirely and which certSIGN does not assume in any way.

4.6 Certificate Renewal

A Subscriber or a Certification Authority uses the renewal if they already own a certificate and a private key associated to it and wishes to continue to use the same key pair. The new certificate created as result of the renewal consists of the same public key, same name and the rest of the information that are taken from the previous certificate, but the availability period, serial number and the issuer's signature are different from the data in the previous certificate.

Renewal applies only to certificates issued by certSIGN which availability period did not expire, were not revoked and the contented information is still intact.

Every signed renewal request is processed off-line, that means it requires the manual acceptance of the operator of the Certification Authority.

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

In order to maintain the continuity of the certificate, the user must request a new certificate before its expiration. The new certificate may contain the same key (renewal – see previous chapter) provided that the life of the keys does not exceed twice the lifetime of a certificate. Otherwise, a new certificate will be issued.

4.7.2 Who may request certification of a new public key

certSIGN always informs the Subjects (at least 30 days in advance) of the expiration date close.

Re-Key certification is only at the Subscriber's request and must be preceded by an application on the appropriate form, completed by the Subscriber.
Applications must be confirmed if the operator of the Registration Authority so requests.

4.7.3 Processing certificate re-keying requests

The procedure for processing the re-key certification request is equivalent to the procedures for processing the certificate requests described in Chapter 4.2 and the issuance procedures described in Chapter 4.3.

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

Certificate modification means creating a new certificate based on the certificate owned at the time by the Subscriber. A new certificate has a different public key, a new serial number, but differs by at least one field (by its content or the occurrence of a completely new field) from the certificate on the basis of which it is being issued. The modification might be necessary, for example, in case of position changing inside the company or of name change, on the condition that these data were previously stated in the certificate or if they should be added. If data that are verified based on documents in accordance with Subscriber’s authentication procedures on the basis of appropriate documents have been modified, every request must be confirmed by the Registration Authority (see Chapter 4.8). Only valid certificates that have not been revoked and which Subscriber’s name and other characteristics have not changed are subject to modification.

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

A certificate revocation has a significant influence on its usage and on Subscriber's obligations. Shortly after a Subject's certificate revocation, the certificate shall be considered invalid (under revocation). Similarly, in case of the Certification Authority's certificate – the cancellation of a certificate's validity means the withdrawal of the certificate issuance rights for its owner and the revocation of all certificates issued by him.

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.

Suspension of a certificate is a reversible revocation, so it can be considered a temporary revocation.

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

4.9.1 Circumstances for certificate revocation

A basic reason for revoking a Subscriber's certificate is loss of control (or suspicion of such a loss) over the private key owned by the Subscriber or the Subscriber's violation of obligations/requests included in the Certification Policy, or contract concluded with the Certification Authority or the CPS.

4.9.1.1 Reasons for Revoking an End Entity Certificate

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

1. The Subscriber requests in writing, without specifying a CRLreason, that the CA revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL)

2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization(CRLReason #9, privilegeWithdrawn);

3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);

4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) (CRLReason #1, keyCompromise);

5. The CA obtains evidence that the validation of domain authorization or control for any FullyQualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).

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

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

7. The CA obtains evidence that the certificate was misused (CRLReason #9, privilegeWithdrawn);

8. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms and conditions (CRLReason #9, privilegeWithdrawn);

9. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant

licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);

10. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);

11. The CA is made aware of a material change in the information contained in the certificate (CRLReason #9, privilegeWithdrawn);

12. The CA is made aware that the certificate was not issued in accordance with CA/Browser Forum Baseline Requirements or certSIGN CPS (CRLReason #4, superseded);

13. The CA determines or is made aware that any of the information appearing in the certificate is inaccurate (CRLReason #9, privilegeWithdrawn);

14. The CA's right to issue certificates under CA/Browser Forum Baseline Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason “unspecified (0)” which results in no reasonCode extension being provided in the CRL);

15. Revocation is required by the certSIGN Certification Practice Statement for a reason that is not otherwise required to be specified by this section (CRLReason “unspecified (0)” which results in no reasonCode extension being provided in the CRL);;

16. The CA is made aware of a demonstrated or proven method that exposes the Subscriber’s Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Issuing CA, certSIGN ROOT CA, will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:
1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise and/or no longer complies with the CABF BR requirements of Sections 6.1.5 and 6.1.6;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.

In any other situation where the Beneficiary does not comply with this CPS, the Contractual Agreement, the Terms and Conditions, or other agreements entered into between the parties regarding the services provided by certSIGN CA.

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.
The revocation request can be sent through the Registration Authority (this implies the Subscriber to contact the authority), or directly to a Certification Authority (the request may be authenticated by signature). The revocation request must contain information that allow the secure authentication of the Subscriber by the Registration Authority in compliance with provisions of Chapter 3.3. If the Subscriber's identity authentication is not successful, the Certification Authority rejects the revocation request and suspends the certificate until the revocation request will be examined in detail.

The short-term certificates are not revoked.

4.9.2 Who can request certificate revocation

The following entities can send certificate revocation requests to a Subscriber:

- The Subscriber who is the owner of the certificate,
- An authorized representative of the Certification Authority (in certSIGN case this role is reserved for the security administrator),
- A Subscriber's representative, for example his employer; the Subscriber must immediately be informed about this thing,
- The Registration Authority that can request the revocation on behalf of a Subscriber or for its own if it has information that justifies the certificate revocation.

Registration Authority must act with extreme caution when processing revocation requests that were not sent by the Subscriber and accept only those requests in compliance with this document.

When the party that requests the certificate revocation is not the owner of the certificate (Subscriber), the certification Authority must:

- Check if the respective party has the right to issue such a request
- Request a justification for the respective request
- Send a notification concerning the revocation or the starting of the revocation process to the Subscriber.

Every request must be sent:

- Directly to the Certification Authority in electronic format with or without the confirmation of the Registration Authority,
- Directly or indirectly (through the Registration Authority) to the Certification Authority not in electronic format (paper document, fax, telephone etc.)

  The revocation request may refer to multiple certificates

4.9.3 Procedure for revocation request

The certificate revocation request may be sent in the following manners:

- First method is based on sending an electronic revocation request authorized by a password to a Certification Authority; such a revocation may be initialized only upon Subscriber's request
- The second method requires the sending of an electronic revocation request to certSIGN, confirmed (by electronic signature) by the Registration Authority; this method applies in situations when (a) the Subscriber lost its private key or its password, or the private key was stolen or (b) the revocation request was sent to the representative of the Subscriber, an authorized representative of the Certification

Authority or of the Registration Authority under the condition that there are enough reasons to request such a revocation;

- The third method implies sending a non-electronic authenticated request (paper document, fax, telephone etc.) to certSIGN; the authentication of a paper document (including a fax) may be done at the Registration Authority, for example with a stamp and a hand signature of a person known by certSIGN, or by placing a password in the document, the password known only to the person requesting the revocation; a request made by phone is fulfilled only after the password is sent; after successful verification of the application, the Registration Authority prepares the electronic confirmation of the revocation application and submits it to the Certification Authority.

The information about the revoked or suspended certificates is placed in the Certificate Revocation List (see Chapter 7.2), issued by the Certification Authority. The Certification Authority notifies the entity that requests the certificate's revocation about this thing or about the decision to cancel the request along with the reasons for cancellation.

Every certificate revocation request must provide means of univocal identification of the revoked certificate, must contain reasons for which the revocation is requested, according to chapter 7.2, and must be authenticated, according to chapter 3.4.

A certificate revocation process takes place as it follows:

- The Certification Authority following the receiving of a certificate revocation request checks it; if the request is electronic the Certification Authority verifies the correctness of the revoked certificate and (optionally) the correctness of the certificate attached to the request; the request on paper requires the solicitor's authorization; such a confirmation may be obtained on the phone, by fax, or while the Subscriber personally visits an authorized representative of the Certification Authority (or vice versa);
- If the request is successfully verified, the Certification Authority places the information concerning the certificate revocation in the Certificate Revocation List (CRL) along with information concerning the reasons for revocation (see Chapter 7.2);
- The Certification Authority notifies electronic or by mail the entity that requests the revocation about the revocation or about the decision of request cancellation along with the reasons for this cancellation.
- Moreover, if the party requesting the revocation is not the Subscriber, the Certification Authority must notify the Subscriber about the certificate revocation or about the starting of the revocation process.

If a certificate or a private key corresponding to a certificate to be revoked were stored on a cryptographic device as following the certificate revocation, the cryptographic device must be physically destroyed or deleted in high security conditions. This action is taken by the owner of the cryptographic device – a natural or legal entity (a representative of such an entity). The owner of the cryptographic device must keep it thus to prevent the robbery or unauthorized usage until its physical destruction or until the deletion of the private key.

4.9.3.1 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**.

4.9.4 Revocation request grace period

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

4.9.5 Time within which CA must process the revocation request

certSIGN guarantees the following maximum period for processing a certificate revocation request,

- Electronically sent (in the correct format) or by phone,
- Sent as paper document,

As it is described in Table 4.9.4.

Certification Policy	**Allowable grace period**
certSIGN Class 1	No obligation to revoke
certSIGN Class 2	Within 24 hours
certSIGN Class 3	Within 24 hours
certSIGN Class 4	Within 24 hours

Table 4.9.6. The maximum period for processing a certificate revocation request

certSIGN will consider if revocation or other action is needed based on the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered);
5. Relevant legislation.

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 publishing periods of CRL.

At the time of certificate revocation, the operators of the Registration Authority and Subscribers involved are automatically informed about this revocation. Information about the current status of the certificate is available by means of the certificate status verification service immediately after the stated grace period. This service may be requested, for example, by a Relying Party that checks the availability of an electronic signature applied to a document received from the Subscriber.

4.9.6 Revocation checking requirements for relying parties

certSIGN provides the certificate's status verification service in real time. This service is realized based on the OCSP protocol described in RFC 6960. Using OCSP it is possible to obtain more exact data (compared to the exclusive usage of the CRL) concerning a certificate status.

OCSP functions on the basis of the request-response model. As response to a request the OCSP server provides the following information about the certificate status:

- *good* – meaning a positive response to a request that must be seen as confirmation for the certificate validity,
- *revoked* – meaning the certificate was revoked,
- *unknown* – meaning the certificate was not issued by any of the affiliated Certification Authorities.

The OCSP service is available for any Subscriber and Relying Party which signed the contract with certSIGN regarding the rendering of these services.

Certificate status is always provided in real time (immediately after the certificate's revocation) based on information from certSIGN's database and contains information newer that those from the published CRL.

A Relying Party is not obliged to verify on-line the certificate status based on the abovementioned services and mechanisms. Although, it is recommended the usage of the OCSP service when the electronic document forgery risk by using electronic signature is higher or if this thing is required by other regulations concerning such situations.

4.9.7 CRL issuance frequency

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

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

certSIGN ROOT CA continues issuing CRLs until one of the following is true:

- all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; OR
- the corresponding Subordinate CA Private Key is destroyed.

4.9.8 Maximum latency for CRLs

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

4.9.9 On-line revocation/status checking availability

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.

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

For the status of Subscriber Certificates, the CA updates information provided via an Online Certificate Status Protocol at least 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

(i) Every twelve months and

(ii) 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.

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

Other forms of revocation are described in chapter 4.9.3.

4.9.12 Special requirements re key compromise

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

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

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

Acceptable methods that third parties may use to demonstrate private key compromise:
1. Perform the procedure described in Section 7.6 of RFC 8555 and sign the revocation request with the compromised private key.
2. Sign a challenge provided by certSIGN using the compromised private key.
3. Submit the private key itself.

4.9.13 Circumstances for suspension

N/A

4.9.14 Who can request suspension

N/A

4.9.15 Procedure for suspension request

N/A

4.9.16 Limits on suspension period

N/A

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 "certsign.ro" and the on line "ocsp.certsign.ro". The certificate status services provide information on the status of valid certificates. The integrity and authenticity of the status information is protected by a digital signature of the respective CA.

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

4.10.2 Service availability

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 revoke a Certificate that is the subject of such a complaint.

4.10.3 Optional features

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

4.11 End of subscription

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 Subscriber data and documentation for a period of 10 years after termination of a subscription.

4.12 Key escrow and recovery

Certification authorities operating within certSIGN create a backup copy of their private key. The copies are used in the case of execution of standard or emergency (e.g. after disaster) key recovery procedure. The copies of the private keys are protected by shared secrets.

certSIGN does not retain copies of Certification Authority operator private keys. Copies of a Subscriber's private keys are created solely on Subscriber's demand and in accordance with the methods presented in 6.2.3.

"The users private encryption keys copies are kept encrypted in the Certification Authority database.

In this way, every user’s private key is symmetrically encrypted with a session key. The session keys are encrypted with a master decryption key. The access to this decryption key is made by apportioned secrets, on the K principle of N. The user’s private signing key are not saved.”

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

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

As a certificate service provider, certSIGN places security at the core of its activities. In order that all of its assets, activities and services are secure, certSIGN has implemented, maintains and continuously improves an information security management system ISO 27001:2013 certified. In accord 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 latest version of the following standards:

- ETSI EN 319 401, General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1, Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2, Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 421, Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates

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

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

The Certificate Management Process includes:

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

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

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

Based on the Risk Assessment, the CA developed, implemented, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan takes into account then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical Controls

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

5.1.1 Site location and construction

certSIGN CA is located in Bucharest, 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 environment protected with controls based on the risk assessment that deter, prevent, detect and counteract the materialization of risks to 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. Among the most important security controls are:

- A clearly defined and protected perimeter through which all entry and exit is controlled;
- Critical components are protected with several perimeters
- An entry control system which admits only those individuals appropriately cleared and specifically authorised to enter the area;
- Manned and electronic monitoring for unauthorized intrusion at all times;
- Personnel not on the access list are properly escorted and supervised;
- A site access log is maintained and inspected periodically;
- Equipment is correctly maintained to ensure its continued availability and integrity.

5.1.2 Physical access

The physical access within certSIGN area is controlled and monitored by the integrated alarm system. Fire prevention system, intrusion detection system and emergency power system are employed.

certSIGN facility is publicly available every working day between 9.00 and 18.00. In the remaining time (including non-working days), the facility is available only to persons authorized by the Management of certSIGN. Visitors to areas occupied by certSIGN may access this area only if they are permanently escorted by the authorized personnel.

Areas occupied by certSIGN 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 the access rights is carried out on the basis of identity cards and appropriate readers, mounted next to the area entry. Every entry and exit to and from the area is automatically recorded in the event journal.

Access to the ***operators' area*** is enforced through the use of an electronic card and their appropriate reader. Since all sensitive information is protected by the use of safes, while access to operator's or administrator's terminal requires prior authorization, the employed physical security is assumed as 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.

Unaccompanied persons are not allowed in this area.

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

5.1.3 Power and air conditioning

All areas, are air conditioned. In the server areas, the air conditioning units are redundant and temperature is monitored both automatically (with an alert when a threshold is reached) and manually. From the moment of power cut, emergency power source (UPS) allows to continue the activity until the automatic intervention of backup generator within the building. The electrical power infrastructure is designed as such that if the main power of the building is cut, all activities can continue for at least 24 hours due the diesel 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 physical security protection system are also connected to UPSes and to the diesel generator.

5.1.4 Water exposure

The risk of flood in the servers' area is controlled trough racks. All equipment is placed in racks and the distance from the ground to the first equipment is of minimum 15 cm. Additionally all data rooms are monitored by humidity sensors.

5.1.5 Fire prevention and protection

certSIGN location benefits of 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 disposed 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 storage

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 seat or an auxiliary seat.

5.2 Procedural controls

5.2.1 Trusted roles

Trusted roles in certSIGN

In certSIGN there might be manned the following trusted roles with one or more individuals:

- **Security administrator** – Overall responsibility for the implementation of the security practices and policies. Additionally approve the generation/revocation of certificates.
    - Initiates installation, configuration and management of software applications and hardware (including network resources) of certSIGN; initiates and suspends services provided by certSIGN; manages the administrators, initiates and supervises key and shared secret generation; assigns rights in the field of security and user's access privileges; assigns passwords for new users' accounts; reviews event journals; supervises internal and external audits; receives and answers post-audit reports; supervises post-audit deficiency removal.
    - Oversees Certification Authority operators; configures the systems and the network; activates and configures network protections; creates accounts for certSIGN users; reviews system logs; verifies compliance of Certification Policy and CPS; generates shared secrets and keys; manages Certificate Revocation List; creates emergency backup copies; modifies server names and addresses.

- **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 equipments.
- **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 Subscribers' certificates; revokes Subscribers' certificates; provides continuity of backup copies and archives of database and system logs creation; manages databases; has access to confidential information about Subscribers but is not allowed to physically access any other system resources; transfers archive copies and current backup copies outside certSIGN seat.
- **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 on Registration Authority, operating within certSIGN.
- **Repository administrator** – manages folders of certSIGN available to the public, creates and updates contents of repository folders, creates Web page and manages links.

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

Trusted roles in Registration Authority

certSIGN has to make sure that the personnel of the Registration Authority is aware of their responsibility, arising from verification of information about Subscribers. Therefore, at least three following trusted roles have to be defined:

- **System administrator** – installs hardware devices and operating systems; installs programs; configures system and applications; activates and configures security resources; creates operators' accounts and passwords; creates backup copies and archives information; reviews events journals (logs) and (together with the Registration Authority's operator) and by the order of the secret administrator, deletes excessive information;
- **Secret administrator** – supervises and transfers secrets (cryptographic keys and other protected data) to Registration Authority operators; takes part in cryptographic module activation and operators' keys loading (in their presence); transfers and activates operators' identity cards (if the cards are subjected to blockage); mediates between the Registration Authority and a Certification Authority;
- **Operator** – verifies Subscriber's identity and correctness of provided requests; issues confirmation of requests and sends them to a Certification Authority; he/she generates keys and takes part in certificate generation, submitting information from a request to a Certification Authority; archives (in paper form) requests and issued confirmation which are subjected to erasure by the order of the secret administrator and in the administrator's presence,

Subscriber's trusted roles

The subscriber may assign an individual (operator) operating application supporting electronic data interchange. The individual is personally responsible for signing, encrypting and submitting messages.

5.2.2 Number of persons required per task

Keys – for the needs of certificate and CRL signing – generation process is the one of the operations requiring particular attention. The generation requires presence of at least three trusted roles, Presence of the security officer, Certification Authority administrator and an appropriate number of persons, being holders of a shared secret are required when loading Certification Authority cryptographic key into hardware security module.

For tasks related to critical CA functions such as but not limited to key management and in particular CA key generation, more than two persons are required for extended security and control reasons. Certificate issuance by the ROOT CA is under at least dual control by authorized, trusted personnel such that one person cannot sign Intermediate certificates on his/her own.

5.2.3 Identification and authentication for each role

certSIGN personnel are subjected to identification and authentication procedure in the following situation:

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

Every assigned account:

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

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

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

All actions, 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 defined from the view point of roles fulfilled with segregation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. These include skills and experience requirements.

Procedures are established and implemented for all trusted and administrative roles that 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,
- Is a Romanian citizen,

- Has signed 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 an agreement containing clause concerning sensitive (from the point of view of certSIGN security) information protection 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 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 acting for the provision of certSIGN’s certification services are checked prior to employment regarding qualifications, expert knowledge, experiences and clearance needed and as appropriate to fill trusted roles and to perform the related specific job function. Managerial personnel possess 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 makes or 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 following trainings:

- Requirements of Certification Practice Statement,
- Requirements of Certification Policy,
- Procedures and security controls employed by a Certification Authority and a 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, Certification Policy 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 Re Training frequency and requirements

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

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

Policies or procedures violations, unauthorized actions, unauthorized use of authority and unauthorized use of systems are penalized by certSIGN or steps are taken that relevant sanctions are provided to those responsible. This may include among others revocation of privileges, administrative discipline, sanctions regulated by the Romanian labor laws and/or criminal pursuit.

5.3.7 Independent contractor requirements

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

Controls on personnel that are independent contractors rather than employees of the entity include auditing and monitoring of contractor personnel; and other controls on contracting personnel.

5.3.8 Documentation supplied to personnel

certSIGN has to provide their personnel with access to the following documents:

- Certification policy,
- CPS,
- Range 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 allow for the audit of 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 has to be 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 archived 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 be it automatically created or by hand is preserved and disclosed during an audit, if required. The time accuracy of logs is ensured by three time servers. Two of them use as a reference time source GPS satellites and one is synchronized with the system that provides the official time of Romania (NIMB). The time used to record events as required in the audit log are synchronized with UTC at least once a day.

5.4.1 Types of events recorded

Every critical activity from certSIGN's security point of view is recorded in event logs and archived. The archives are stored on storage environments 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 entries** – 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 data to record are: 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, it is automatically created a log version. The previous log is archived and deleted from the disk.

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

The CA record at least the following events:

1. **CA certificate and key lifecycle events**, including:
   - Key generation, backup, storage, recovery, archival, and destruction;
   - Certificate requests, renewal, and re-key requests, and revocation;
   - Approval and rejection of certificate requests;
   - Cryptographic device lifecycle management events;
   - Generation of Certificate Revocation Lists;
   - Signing of OCSP Responses
   - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. **Subscriber Certificate lifecycle management events**, including:
   - Certificate requests, renewal, and re-key requests, and revocation;
   - All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
   - Approval and rejection of certificate requests;
   - Issuance of Certificates;
   - Generation of Certificate Revocation Lists;
   - Signing of OCSP Responses.
3. **Security events**, including:
   - Successful and unsuccessful PKI system access attempts;
   - PKI and security system actions performed;
   - Security profile changes;
   - Installation, update and removal of software on a Certificate System;

- System start-up and shutdown, crashes, hardware failures, and other anomalies;
- Relevant router and firewall activities (as described below);
- Entries to and exits from the CA facility.

Every automatic or manual recording contains the following information:

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

Logging of router and firewall activities at a minimum include:

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

All registration information including the following is recorded:

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

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

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

Events’ records are stored in files on the system disk until they reach the maximum allowed capacity. During this time, they are available on-line, upon every authorized person’s or process request. After exceeding the allowed capacity, journals are kept as archives and can be accessed exclusively off-line, from a certain workstation.
The archived journals of logs are kept at least 10 years.
The CA and each Delegated Third Party retain, for at least two (2) years:
1. CA certificate and key lifecycle management event records after the later occurrence of:

- the destruction of the CA Private Key; or
- the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;

2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1) after the expiration of the Subscriber Certificate;
3. Any security event records (as set forth in Section 5.4.1) after the event occurred.

5.4.4 Protection of audit log

The log files are properly protected by an access control mechanism. Appropriate protection against modification and deletion of the audit logs is implemented such that no one may modify or delete audit records except after transfer to long term media for archiving purposes. Only the security officer, the administrators, 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,
- Only the security officer can archive or delete 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 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

The event log analysis module implemented in the system examines current events and automatically senses suspicious activities or those that compromise security. For activities that have an impact on system security, the security administrator and the Certification Authority administrator are automatically notified. In other cases, the notification is directed only to the system administrator. The transmission of information to authorized persons about critical situations - from the point of view of system security - is done by other means of communication, properly protected, for example, pager, mobile phone, e-mail. Notified Entities take appropriate measures to protect the system against the detected threat.

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 archiving

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 *off-line* archive contains certificates (including revoked certificates) expired up to 10 years before the current date. Revoked certificate archive contains information about a certificate identified, reason of revocation, date when the certificate was placed on CRL. The archive is used for dispute resolving, applying to old documents, electronically signed by a Subject.

Backup copies are created and retained outside certSIGN location.

5.5.1 Types of records archived

The CA and each Delegated Third Party archive all audit logs (as set forth in Section 5.4.1).

Additionally, the CA and each Delegated Third Party archive:

1. Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems;
2. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

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 maintenance 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

System time for certSIGN computers is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours (Windows default). The following archived items on the certificate approval checklist are time-stamped with the date, the time and the name of the certSIGN employee checking the information and making the record:

- Organizational status screen shot;
- Screen shot of web site.

The following records are time-stamped by the certificate administration system when an item is either automatically received or is checked in by the certSIGN employee:

- Receipt of certificate application and PKCS#10 CSR;
- Letter of authorization;
- Name, e-mail, and IP address of person acknowledging organizational authority; and other application information, as applicable.

Certificate issuance is time-stamped as a function of the "Valid From" field in accordance with the X.509 Certificate Profile.

Certificate revocation is time-stamped as a function of the "Revocation Date" field in accordance with the X.509 Certificate Revocation List Profile.

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 Section 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 breaches of security. 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.

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 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 important network services, important for certSIGN's activity. It primary addresses power cuts and damages of the network connections,
- Corruption of a part of the Intranet, 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 primary facility is restored to service. The distance between the primary and the emergency facilities is 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 application creating backup copy from data, allowing system recovery at any moment and performance of an audit. Backup copies include all the relevant data from security point of view.
- All the systems that made up the IT infrastructure for providing 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 will address any critical vulnerability not previously addressed, within a period of 48 hours after its discovery. certSIGN prepares and implements a mitigation plan for the new vulnerabilities, if this is cost effective compared to their impact, or documents the decision that the vulnerability does not require remediation.

5.7.3 Entity private key compromise procedures

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

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

- Notification of the compromise to all Subjects/ subscribers and other entities with which certSIGN has agreements or other form of established relations, among which relying parties and other trust services providers. In addition, this information will be made available to other relying parties by means of mass media system and electronic mail
- Notification of the public through several channels, including a message on the certSIGN’s CA repository and web site, a press release in 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 without charging any fees.
- If a Certificate is revoked because of CA key compromise, certSIGN Root CA will issue a new CRL within 24 hours after receiving notice of the compromise and publish online CRLs immediately.

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

5.7.4 Business continuity capabilities after a disaster

certSIGN has established in a Business Continuity and Disaster Recovery Plan all the necessary measures to ensure full recovery of our certification and time stamping services in case of a disaster, or a discontinuity 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 systems data necessary to resume CA operations are backed up and stored in a remote and safe place, suitable to allow certification and time stamping services to timely go back to operations in case of incident/disasters.

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

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

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

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

5.8 CA or RA termination

certSIGN has an up-to-date termination plan Obligations described below are developed to minimize disruptions to Subjects/ Subscribers and Relying Parties which might arise from a decision of a Certification Authority to cease operation and include 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 of other Certification Authority.

5.8.1 Requirements associated to duty transition

Before a Certification Authority ceases its activity, it shall:

- 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 the 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;
- Handling of the revocation status for 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 and timestamping services for a reasonable period, unless it can be demonstrated that we do not hold any such information; The information refers to registration information, revocation status for unexpired certificates that have been issued. and event log archives for their respective period of time as indicated to the Subjects/ Subscriber and relying party
- CA private keys, including backup copies, will be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved;
- Where possible arrangements should be made 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 transfer of part or the entirety 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.

5.8.2 Certificate issuance by the successor of terminated Certification Authority

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

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 case of cessation of the activity of the authority certSIGN SSL DV CA Class 3 G2) or the institution with which the contract was signed (in case of cessation of activity certSIGN ROOT CA).

6 Technical security controls

6.1 Key pair generation and installation

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

certSIGN ROOT CA Certification Authority owns at least one self-signed certificate. The private key corresponding to the public key contained in the self-signed certificate is used exclusively to sign the public keys of the Certification Authorities **certSIGN SSL DV CA Class 3 G2** by signing the operational certificates and the Certificate Revocation List necessary for the authorities' functioning. A similar purpose is intended for private keys held by each authority: **certSIGN SSL DV CA Class 3 G2** corresponding to public keys included in certificates issued by **certSIGN ROOT CA** for each of the authorities.

Key pairs owned by each Certification Authority should allow certificate and CRL signing – a public key associated with a private key authenticated with a self-signed certificate (in case of **certSIGN ROOT CA**) or certificate (in case of **certSIGN SSL DV CA Class 3 G2**).

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

6.1.1 Key pair generation

The keys of **certSIGN SSL DV CA Class 3 G2** as well as the keys of other Intermediate authorities are generated within certSIGN's location, in the presence of a trusted group of persons (the security administrator and the Certification Authority administrator have to be members of this group).

Key pairs of Certification Authorities operating within certSIGN are generated on designated, authenticated workstation and connected to hardware security module, complying with the requirements of FIPS 140-2 Level 3. They are permanently retained encrypted on these devices.

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

Registration Authority operators possess only keys to authenticate all their actions. These keys are generated by the operator (in the presence of the secret administrators) by means of authenticated software supplied by a Certification Authority and connected with certified hardware security module complying with requirements of FIPS 140-2 Level 2.

Generally, every Subscriber generates his/her/its key pair by himself/herself/itself. In this respect there will be used the application available on the request generation moment on certSIGN's web site. The application allows key generation both on secured devices (tokens, smart cards), and as encrypted p12 format. A Certification Authority can perform the generation, as well.

The CA rejects a SSL 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 SSL 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 SSL certificate request using a Key Pair previously generated by the CA.

certSIGN may, on Subscriber's demand or on Certification Authority operator's demand generate a key pair and submit it securely to the Subscriber. In such cases software applications and cryptographic devices complying with the regulations of FIPS 140-2 Level 2 (see Chapter 6.1.2) are employed.

In all cases, the CA will:

- prepare and follow a Key Generation Script,
- have a Qualified Auditor witness the CA Key Pair generation process
- generate the CA Key Pair in a physically secured environment as described in this CPS;
- generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;
- generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in this CPS;
- log its CA Key Pair generation activities; and
- maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this CPS and in the Key Generation Script.

6.1.1.1 Procedures of generation of certSIGN ROOT CA initial keys

Procedures of generation of initial certSIGN ROOT CA keys are always deployed during certSIGN system initiation or in the case of suspicion that a subsequent private Certification Authority key has been compromised. The procedure includes:

- secure generation of a main key pair for certificate and CRL signing, distribution of private key,
- issuance of a public key self-signed certificate.

issuance by the Qualified Auditor of a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.Upon key pair generation for certificate and CRL signing, private key distribution and its activation in hardware security module, the keys can be used in cryptographic operations until the validity period has expired or the keys have been revealed.

6.1.1.2 Procedures of generation of certSIGN CA initial keys

Procedures of generation of initial certSIGN CA keys include:

- secure generation of a main key pair for certificate and CRL signing, distribution of private key,
- issuance of a public key certificate, signed by certSIGN ROOT CA.

Upon key pair generation for certificate and CRL signing, private key distribution and its activation in hardware security module, the keys can be used in cryptographic operations until the validity period has expired or the keys have been revealed.

6.1.1.3 certSIGN ROOT CA certificate rekey procedure

certSIGN ROOT CA cryptographic keys have a limited lifetime period; if the period has expired, the keys should be updated.

A particular procedure is applied for update of key pair used for certificate and CRL signing. It is based on the issuance of special certificates by certSIGN. The certificates enable Subscribers who have already installed an expired certificate of certSIGN ROOT CA to securely migrate to work with a new certificate: new Subscribers already possessing a new certificate are enabled to securely retrieve expired certificate, which may be needed for verification of the data signed in the past.

To achieve effect described above**,** certSIGN ROOT CA deploys a procedure, owing to which new key pair generation will allow to authenticate a new public key with the use of the former private key and vice-versa (an old public key is secured with a new private key). It means that as a result of update of the certificate of certification authority, certSIGN ROOT CA, apart from a new certificate, two additional certificates are created. After the key update four certificates are created for certificates and CRL signing: the former certificate **OldWithOld** (old public key signed with old private key), the new certificate **NewWithNew** (new public key signed with new private key), certificate **OldWithNew** (old public key signed with new private key) and certificate **NewWithOld** (new public key signed with old private key).

Procedure for a key pair for certSIGN ROOT CA update, designated to certificate and CRL signing, is executed as it follows:

- generation of a new key pair,
- creation of a certificate, containing new public key of certSIGN ROOT CA, signed with old private key (certificate **NewWithOld**),
- deactivation of old private key and activation of new private key within hardware security module a new private key for certificate and CRL signing is loaded,
- creation of a certificate, containing old public key certSIGN ROOT CA, signed with new private key (certificate **OldWithNew**),
- creation of a certificate containing new public key of certSIGN ROOT CA, signed with new private key (certificate **NewWithNew**),
- publication of new certificates in the repository, submission of the information about new available certificates and, optionally, placement of the cryptographic digest of the new public key in newspapers.

After generation and activation of a new private key (it may be executed in any moment within the validity period of the old certificate), certSIGN ROOT CA authority signs certificates solely by means of new private key.

The old public key (old certificate) is available to the public until all Subscribers obtain the new certificate (new public key) of certSIGN ROOT CA (it should be achieved before the expiry date of the old certificate).

Beginning and expiration of the validity period of certificate **OldWithNew** should be the same as beginning and expiration date of the old certificate.

Validity period of certificate **NewWithOld** starts in the moment of a new key pair generation and expires in the moment when all the Subscribers will obtain new certificates (certificate of the new public key) of certSIGN ROOT CA. Its expiration date should not be later than the expiry date of the old certificate.

Validity period of certificate **NewWithNew** begins in the moment of a new key pair generation and expires at least 180 days after the next anticipated date of succeeding key pair generation. This requirement means the certification authority certSIGN ROOT CA terminates usage of the private key for signing certificates and CRL at least 180 days before the expiry date of the certificate corresponding to this private key.

6.1.1.4 Intermediate certification authority rekey procedure

Procedures for certification authority rekey (key update) of Certification Authority for **certSIGN SSL DV CA Class 3 G2** are executed similarly as for certSIGN **ROOT CA** (see Chapter 6.1.1.3) except one step: certificate **NewWithNew** is issued by superior authority.

6.1.2 Private key delivery to subscriber

If the Subscriber's key pair is generated by a Certification Authority, the keys may be delivered to the Subscriber in one of the following ways:

- keys are stored on a cryptographic device (e.g. a token) or in PKCS#12 format for certain cases and are delivered to the Subscriber personally or by means of registered mail; data for the card activation (PIN code) or key decryption (password) are submitted separately from the media containing the key pair; the issued cards are personalized and registered by the Certification Authority.

certSIGN guarantees that in any moment after generation of a key pair on Subscriber's demand the keys will not be used for creating an electronic signature and that the Certification Authority will not create conditions for making the signature by any unauthorized entity, except for the owner of the private key.

6.1.3 Public key delivery to the certificate issuer

Subjects submit their generated public keys as an electronic request whose format has to comply with protocols of PKCS#10 (CSR).
Requests submitted to a Certification Authority may, in particular cases, require confirmation issued by the Registration Authority (see Chapter 3 and 4).

Submission of a public key is expendable in the case when a key pair is generated on Subscriber's demand or on Registration Authority operator's demand by a Certification Authority, which simultaneously issues a certificate for the generated key pair.

6.1.4 CA public key delivery to relying parties

Public keys of a Certification Authority issuing certificates to Subscribers are distributed solely in a form of certificates complying with ITU-T X.509 v.3 recommendations. In the case of certSIGN ROOT CA Certification Authority, certificates are self-signed.

certSIGN Certification Authorities distribute their certificates in two different methods:

- placement in the publicly available repository of certSIGN; retrieval of the certificates requires the subscribers to visit web page available at https://registru.certsign.ro/cgi-bin/pubral/pubra/get_cert

- distribution together with the software (Web browsers, email clients, etc.), which allows usage of services offered by certSIGN.

In the case of certSIGN Certification Authority key rekey (update), the repository should contain all additional self-signed certificates or certificates issued as a result of execution of the procedure described in Chapter 6.1.1.3.

6.1.5 Key sizes

Sizes of keys deployed by Certification Authorities, Registration Authority operators and Subscribers are presented in Table 6.1. Only these algorithms and key sizes are permitted for the CAs listed in the table:

Key owner	**Primary key usage**		
	RSA for certificate and CRL signing	**RSA for message signing**	**RSA for key exchange**
certSIGN ROOT CA	2048 bit	-	-
certSIGN SSL DV CA Class 3 G2	2048 bit		

Table 6.1. Size of keys used

6.1.6 Public keys parameters generation and parameter quality checking

The creator of a key is responsible for checking parameter quality of the generated key. He/she is required to verify:

- ability to execute encryption and decryption operation, including electronic signature creation and its verification,
- key generation process, which should be based on strong random cryptographic number generators – physical sources of white noise, if possible,
- immunity to known attacks (applies to RSA and DSA algorithms).

certSIGN has a documented procedure for conducting CA key pair generation. The verification procedures include steps checking that the value of the public exponent is an odd number equal to 3 or more. The modulus must have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. Additionally, the public exponent is in the recommended range, between 2^{16}+1 and 2^{256}-1.

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

Allowed key usage purposes are described in KeyUsage field (see Chapter 7.1.1.) of standard extension of a certificate complying with X.509 v3. This field has to be obligatorily 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 verification of electronic signature,

b) nonRepudiation: certificate intended to provide a non-repudiation service by private individuals, as well as for other purposes than described in f) and g). NonRepudiation bit may be set only in a public key certificate intended to verify electronic signatures and should not be combined with purposes described in points c)-e) and connected with providing confidentiality,

c) keyEncipherment: intended to encrypt symmetric algorithm keys, providing data confidentiality,

d) dataEncipherment: intended to encryption of Subject's data, other than described in c) and e),

e) keyAgreement: intended for protocols of key exchange,

f) keyCertSign: public key is used for electronic signature verification in certificates issued by entities providing certification services,
g) cRLSign: public key is used for verification of electronic signatures on revoked and suspended certificates lists issued by the entities providing certification services,
h) encipherOnly: may be used solely with keyAgreement bit to indicate its purpose of data encryption in key exchange protocols,
i) decipherOnly: may be used solely with keyAgreement bit to indicate its purpose of data decryption in key exchange protocols.

Private Keys corresponding to Root Certificates is used only to sign Certificates in the following cases:
1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Intermediate CAs and Cross Certificates.

6.2 Private key protection and Cryptographic Module Engineering Controls

Every Subscriber, Certification Authority operator and Certification Authority generates and stores his/her/its private key employing a credible system preventing from private key loss, revelation, modification or unauthorized access. If a Certification Authority generates a key pair on authorized Subscriber's demand, it has to deliver it securely to the Subscriber and enforce the subscriber to protect his/her/its private key.
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.

6.2.1 Cryptographic module standards and controls

Hardware security modules employed by a Certification Authority and a Registration Authority comply with the requirements of FIPS 140-2 standard. In the case of Subscriber's using hardware key protection, it is also recommended to comply with FIPS 140-2 or Common Criteria.

Electronic signature creation and data encryption comply with PKCS#7 standard requirements. Private keys (as well as public keys) may have one of the following states (according to ISO/IEC 11770-1 standard):

- **waiting for activation (ready)** – key has already been generated but is not available for usage (the present date is not yet the date of beginning of the certificate validity period),
- **active** – key may be used in cryptographic operations (for example, for electronic signature creation), the present date is within the certificate validity period, key has not been was not revoked,
- **inactive** – key in this state may be used solely for electronic signature verification or decryption operations (the Subscriber is not allowed to use this private key to create electronic signature – validity of the key expired; in the case of a public key, the subscriber is not allowed to encrypt information); the present date is beyond the certificate validity period.

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

Multi-person control of a private key applies to private keys of certification authorities' **certSIGN SSL DV CA Class 3 G2** used for certificate and CRL signing.

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

For operations such as: initiating a security cryptographic hardware module, Certification Authorities private keys' transfer, there is implemented a bridge access scheme (k of n type) by delivering **shared secrets**. The accepted number of shared secrets and the necessary number of secrets allowing the private key restoration are disclosed in Table 6.2.2.

Certificate issuing authority	Number of shared secrets	Total number of distributed secrets
certSIGN ROOT CA	2	3
certSIGN SSL DV CA Class 3 G2	2	3

Table 6.2.2. Distribution of shared secrets to initiate and transfer the private keys

Shared secret transfer procedure has to include secret holder presence during key generation and distribution process, acceptance of a delivered secret and resulting responsibilities for its storage.

6.2.2.1 Acceptance of secret shared by its holders

Every shared secret holder, before receiving his/her secret, should personally observe secret shares creation, 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 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 a hand-written signature on an appropriate form whose copy is retained in Certification Authority archives and by the secret holder.

6.2.2.2 Protection of shared secret

Holders of shared secret have to protect their share from revelation. 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,

6.2.2.3 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.

6.2.2.4 Responsibilities of shared secret holder

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 share in the case of the secret theft, loss, unauthorized revelation or security violation immediately after the incident occurrence. A shared secret holder is not responsible for neglecting his/her duties because of the reasons that are impossible to control by the holder, but is responsible for inappropriate revelation of the secret or neglecting the obligation to notify the issuer of the secret about inappropriate revelation or security violation of the secret, resulting from the holder mistake, neglect or irresponsibility.

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

6.2.3 Private key escrow

Subject’s private keys are not subject to custody.
Copies of subscriber's private encryption keys are only created at the request of the subscriber and are subject to custody.

6.2.4 Private key backup

Certification authorities operating within certSIGN create a backup copy of their private key. The copies are used in the case of execution of standard or emergency (e.g. after disaster) key recovery procedure. When located outside the secure cryptographic device, CA private keys are protected in a way that provides the same level of protection as 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.
Copies of a Subscriber’s private keys are created solely on Subscriber’s demand and in accordance with the methods presented in 6.2.3.
“The users private encryption keys copies are kept in the encrypted in the Certification Authority database.
In this way, every user’s private key is symmetrically encrypted with a session key. The session keys are encrypted with a master decryption key. The access to this decryption key is made by apportioned secrets, by the K principle of N. The user’s private signing key are not saved.”

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

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

- keys are generated outside the cryptographic module; this situation occurs for example in the case of Subscriber's key generation (on his/her demand) by a Certification Authority, their entry into a cryptographic card or any other hardware token prior to transfer of the media to Subscriber. A similar operation of key entry into a cryptographic module may be carried out by a Subscriber when the keys are delivered in an encrypted form and require local storage on a cryptographic device,
- in the case of creation of backup copies of private keys stored in a cryptographic module, it may be occasionally necessary (e.g. in the case of the module corruption or malfunction) to enter a key pair into a different security module,
- it is necessary to transfer a private key from the operational module used for standard operations by the entity to another module; the situation may occur in the case of the module defection or necessity of its destruction.

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

Introducing a private key into a security hardware module of the Certification Authority **certSIGN ROOT CA** or **certSIGN SSL DV CA Class 3 G2** requires the restoration of the key on cards in the presence of a corresponding number of shared secret owners that protects the module containing the private keys (see Chapter 6.2.2). Due to the fact that every Certification Authority can retain an encrypted copy of its private key (see Chapter 6.2.4), the keys may also be transferred between modules.

6.2.7 Private key storage on cryptographic module

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

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

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

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

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

Operators use qualified electronic signature creation devices (tokens/cards) 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 private key

Methods of activation of a private key, possessed by various users or Subscribers of certSIGN system, apply to the method of key activation before every use of them or beginning of a work session (e.g. the Internet connection) employing these keys. Once an activated key is ready for usage it can be used until the moment of its deactivation.

Activation (and deactivation) of private key procedure execution depends on the type of the entity holding the key (Subscriber, Registration Authority, Certification Authority, hardware device, etc.), on sensitivity of the data protected by the key, and on, the fact whether the key remains active (for the time of one operation, session or for unlimited time).

All private keys of **certSIGN ROOT CA** or **certSIGN SSL DV CA Class 3 G2** entered into the module after their generation, import in an encrypted form from another module or restoration from shared secret remain in the active state until their physical erasure from the module or removal from certSIGN services. 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 insertion of the card into the cryptographic module and provision of the PIN number, the private key remains in the active state until removal of the card from the module.

Private keys of Registration Authority operators are activated after authentication of the operator (using PIN number) and only for the time of a single cryptographic operation requiring usage of this key. Upon the completion of this operation the private key is automatically deactivated and has to be activated again before execution of another cryptographic operation.

Activation of a Subscriber's private key is carried out similarly to private keys of Certification Authority operators, regardless whether they are stored on a cryptographic card or in an encrypted form as a file on a floppy disc or any other media. In the case of Subscribers who represent legal entities (organizations, institutions, etc) activation should be carried out by a person possessing a suitable authorization of the Subscriber.

6.2.9 Method of deactivating private key

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

In the case of a Subscriber or a Registration Authority operator, private signing key deactivation is carried out immediately after creation of an electronic signature or session completion (e.g. application logoff). If during execution of this cryptographic operation the private key was stored in the operational memory of the application, the application has to prevent unauthorized restoration of the private key. If a private key is held by a Subscriber that is a legal entity, the key may be deactivated solely by the authorized representative of this Subscriber.

In the case of certSIGN, deactivation of a private key is carried out by the security officer only in the situation when the validity period of the private key has expired, the key has been revoked or there is immediate requirement to temporary suspend the activity of the system. Deactivation of a private key is carried out by the removal of the card from the module.

6.2.10Method of destroying private key

At the end of their lifetime, the CA private keys are destroyed by trusted CA roles in the presence of more than one representative of the Policies and Procedures Management Body (PPMB) in order to ensure that these private keys can never be retrieved or used again.
The CA private key can be destroyed by deleting all HSM Cards (Operator and Administrator). Furthermore, the HSMs allow device zeroization by physical access and settings on the device. This reinitializes the device and overwrites all of the data on it with binary zeros. In cases when this zeroization or re-initialization procedure fails, certSIGN will crush, shred and/or incinerate the device in a manner that destroys the ability to extract any secret.

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

6.2.11 Cryptographic Module Rating

See above.

6.3 Other aspects of key pair management

certSIGN uses appropriately the CA private signing keys and does not use them beyond the end of their life cycle.
CA signing key(s) used for generating certificates and certificate revocation lists shall not be used for other purposes.
The certificate signing keys shall only be used within physically secured premises.
The use of the CA's private key shall be compatible with the hash algorithm, the signature algorithm and the signature key length used for generating certificates, in line with current practices (the selected key length and algorithm for CA signing key are RSA 4096 bits in agreement with requirements in ETSI TS 119 312 for the CA's signing purposes)
All copies of the CA private signing keys shall be destroyed at the end of their life cycle.

6.3.1 Public key archival

The purpose of public key archive is to create possibility of electronic signature verification after removal of a certificate from the repository (see Chapter 2.6). It is extremely important in the case of providing of non-repudiation services, such as timestamp service or certificate status verification service.

Archive of public keys involves archive of the certificates containing these keys.

Every authority issuing certificates archives public keys of Subscribers to whom certificates were issued. Certification Authority public keys are archived together with private keys, in the manner described in Chapter 6.2.5. Certificates may also be archived locally by Subscribers, especially when it is required by used application (e.g. electronic mail systems).

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

Within certSIGN, only the keys used for electronic signature verification are subjected to archival. Any other types of public keys (e.g. keys used for encrypting messages) are destroyed immediately after their removal from the repository.

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

Public keys are retained in the digital certificate archive for a period of 15 years from expiration.

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 twice the life period of a certificate, which period is mentioned below.

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

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

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

Key owner	Main purpose of key usage
	RSA for certificate and CRL signing
certSIGN ROOT CA	25 years
certSIGN SSL DV CA Class 3 G2	10 years

Table 6.3.2.1 Maximum usage period of CA certificates

6.4 Activation data

Activation data are used for activation of a private key operated by a Registration Authority, a Certification Authority or by Subscribers. They are usually used on the stage of entity authentication and control of the access to a private key.

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 administrator, 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, created in accordance with the requirements of FIPS-112. 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 revelation. Activation data protection control methods depend on the fact whether they are authentication phrases and whether control in enforced on the basis of private key or its activation data distribution into shared secrets. In the case of the authentication phrase, the recommendations described in FIPS 112 should be enforced, while protection of shared secrets requires implementation of FIPS 140 standard.

It is recommended that activation data used for private key activation should be protected by means of cryptographic controls and physical access controls. Activation data should be biometric data or should be remembered (not written down) by the entity being authenticated. If the authentication 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 should never be retained together with the cryptographic card.

6.4.3 Other aspects of activation data

Activation data are stored always as a single copy. Activation data protecting access to private keys stored on cryptographic cards can be periodically changed. Activation data are subjected to archive.

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

Technical requirements, presented in this Chapter, apply to single computer security control and installed software control, used for certSIGN. Security means protecting computer systems are executed on the level of operating system, application and physical protections. Computers located in Certification Authorities and in their associated components (e.g. Registration Authority) are equipped with the following security means:

- Mandatory authenticated registration on the level of operating system and applications,
- 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 re-usage of an object by another processes after the object release by an authorized process,
- Cryptographic protection of information exchange and protection of databases,
- Archive of history of operation carried out on the computer and data required by audits,
- A secure path allowing credible identification and authentication of roles and personnel performing these roles,
- Key restoration methods (only in the case of hardware security modules) and application and operating system,

- Monitoring and alerting mean in the case of unauthorized compute resource 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 within the period of time that records are required to be retained.

Sensitive data shall be protected against being revealed through re-used storage 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 technical controls

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

6.6.1 System development controls

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

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

Similar rules apply to hardware components replacement, as follows:

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

6.6.2 Security management controls

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

Controls applied to certSIGN system allow continuous verification of application integrity, their version and 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 to the configuration which applies certSIGN's security policy.

Current configuration of Certsign system, any changes to them as well as any to releases, modifications and emergency software fixes of any operational software are documented.

certSIGN implement internal security procedures for ensuring that:

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

The reasons for not applying any security patches are documented

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

6.7 Network security controls

certSIGN protects its network and systems from attack accordding to CA/Browser Forum Network and Certificate System Security Requirements. For that purpose and based on risk assessments and best practices we implement an integrated set of security controls:

a) our systems are segmented into networks or zones based considering functional, logical, and physical (including location) relationship between trustworthy systems and services. certSIGN applies the same security controls to all systems co-located in the same zone.

b) access and communications between zones are restricted to those necessary for the operation of certification services. Not needed connections and services are explicitly forbidden or deactivated. The established rule set is reviewed on a regular basis.

c) all systems that are critical to the certification services operation are kept in one or more secured zone(s)

d) Dedicated network for administration of IT systems and operational network are separated. Systems used for administration of the security policy implementation are not used for other purposes. The production systems for the certification services are separated from systems used in development and testing (e.g. development, test and staging systems).

e) Communication between distinct trustworthy systems are only established through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

f) If a high level of availability of external access to a specific certification service is required, the external network connection is redundant to ensure availability of the services in case of a single failure.

g) a regular vulnerability scan on public and private IP addresses identified by certSIGN is performed and evidence is recorded that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

h) certSIGN certification services undergo a penetration test on the related systems at set up and after infrastructure or application upgrades or modifications that certSIGN determines are significant. Evidence is recorded that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

Servers and trusted workstations of certSIGN system are connected by a local network (LAN), devised in more sub-networks provided with controlled access. Access from the Internet to any segment is protected by means of intelligent firewall.

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

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

Local network components (e.g. routers) shall be kept in a physically and logically secure environment and their configurations shall be periodically checked for compliance with the requirements specified by certSIGN.

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

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

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

The Root CA system is in a high security zone.

6.8 Time-stamping

The time accuracy of logs is ensured by a time server that is synchronized with at least twotime 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

Following the X.509 v.3 standard, a certificate is the sequence of the following fields: the first the body of certificate (**tbsCertificate**), information about algorithm used for certificate signing (**signatureAlgorithm**), and an electronic signature of the Certification Authority (**signatureValue**).

7.1.1 Version number(s)

The contents of a certificate include values of **basic fields** and **extensions** (standard, described by norms, and private, defined by the issuing authority).

Basic fields

certSIGN supports the basic fields described in the external document "certSIGN ROOT CA - Annex Profiles.docx".
In certificates issued by certSIGN values of the fields are set in accordance with rules described in Table 7.1 from the external document "certSIGN ROOT CA - Annex Profiles.docx".
Profiles of all certificate (Subject fields) are detailed in the external document "certSIGN ROOT CA - Annex Profiles.docx".

7.1.2 Certificate extensions

The certificates basic extensions are described in #7.1.2 of the external document "certSIGN ROOT CA - Annex Profiles.docx".

7.1.3 Algorithm object identifiers

The cryptographic algorithm identifier is described in #7.1.2 of the external document "certSIGN ROOT CA - Annex Profiles.docx".

7.1.4 Name forms

The contents of the fields must meet the requirements in section 3.1 in CPS and the latest published version of CAB Forum BR.
Issuer Name for all possible certification paths is byte-for-byte identical with Subject Name of the Issuer certificate. Subject attributes do not contain only metadata such as '.', '-', and ' ' (i.e. space) to indicate that the value is absent, incomplete, or not applicable.

7.1.5 Name constraints

Not applicable.

7.1.6 Certificate policy object identifier

Certificates policy object identifiers used at certSIGN Root CA are described in Table 7.1.2 from the external document "certSIGN ROOT CA - Annex Profiles.docx".

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

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

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL profile

The basic fields for the CRL profile are described in #7.2 of the external document "certSIGN ROOT CA - 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

Function and meaning of extensions are the same as for certificate extensions (see Chapter 7.1.2). CRL entry extensions (**crlEntryExtensions**) supported by certSIGN contain the fields described in #7.2 of the external document "certSIGN ROOT CA - Annex Profiles.docx".

7.3 OCSP profile

The protocol of on-line certificate status verification (OCSP) is described in #7.3 of the external document "certSIGN ROOT CA - Annex Profiles.docx".

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 extensions described in #7.3.2 of the external document "certSIGN ROOT CA - Annex Profiles.docx".

8 Compliance audit and other assessments

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

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

8.1 Frequency or circumstances of assessment

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

The audit verifies the compliance with the present CPS and ETSI 319401,ETSI 319411, 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, or to demonstrate compliance with specific industry, legal or business requirements.

8.2 Identity/qualifications of assessor

The assessment will be performed by an independent external auditor, as defined in the Regulation UE 910/2014, in compliance with WebTrust Program for CAs criteria.

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 this CPS, in accordance with the following schema:
"WebTrust for CAs" v2.2.2 or newer and "WebTrust for CAs SSL Baseline" v2.8 or newer.
Internal and external assessment/audits are carried out in compliance with the international accepted rules and regulations applied to the Certification Authorities and concern:

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

For Delegated Third Parties which are not Enterprise RAs, the CA obtains an audit report, that provides an opinion whether the Delegated Third Party's performance complies with the CA's

Certification Practice Statement. If the opinion is that the Delegated Third Party does not comply, then the CA will not allow the Delegated Third Party to continue performing delegated functions.

8.5 Actions taken as a result of deficiencies

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

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

8.6 Communication of results

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

The Audit Report will state explicitly that it covers the relevant systems and processes used in the issuance of all certificates that assert the policy identifiers declared. The CA makes the Audit Report publicly available no later than three months after the end of the audit period. The audit report will comply with CABF Baseline Requirements, chapter 8.6.

An authoritative English language version of the publicly available audit information will be provided by the Qualified Auditor and the CA will ensure it is publicly available.

The Audit Report will be available as a PDF, and will be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report will be uppercase letters and will not contain colons, spaces, or line feeds.

8.7 Self-audits

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 set according to the internal price policy.

9.1.2 Certificate access fees

Free service.

9.1.3 Revocation or status information access Fees

Prices are set according to the internal price policy.

9.1.4 Fees for other services

Prices are set according to the internal price policy.

9.1.5 Refund policy

Payments may be reimbursed according to the applicable contractual conditions.

9.2 Financial Responsibility

9.2.1 Insurance coverage

certSIGN complies with requirements of the latest published version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at https://cabforum.org/baseline-requirements-documents/ and current version of Mozilla Root Store Policy.

9.2.2 Other assets

Not applicable.

9.2.3 Insurance or warranty coverage for end-entities

certSIGN has an insurance to cover the professional warranties that complies with requirements of the latest published version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at https://cabforum.org/baseline-requirements-documents/ and current version of Mozilla Root Store Policy.

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 of the the Subject is considered to be personal information.

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information

certSIGN and its employees undertake to maintain the confidentiality of personal information during certification services and after certificate termination.
certSIGN will not disclose personal information to any third party, for any reason, unless it is required to do so by law or by the competent authorities.

9.4.5 Notice and consent to use private information

In the process of issuing a digital certificate Subjects / Beneficiaries are informed about the need to use their personal data for the service and the need for consent. If data Subjects do not agree to certSIGN processing their data, they cannot benefit from certification services.
Subjects / Beneficiaries also have the option of using the personal data for other purposes expressly communicated by certSIGN by contract or otherwise.

9.4.6 Disclosure pursuant to judicial or administrative process

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

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

9.4.7 Other information disclosure circumstances

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

- disclosure of personal information to:
  - auditors in the audits to which certSIGN is subject according to the provisions of Regulation (EU) no. 910/2014 under confidentiality;
  - the courier companies with which certSIGN has a contract, with the agreement of the Subject / 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.
- in any other situations justified with the prior notification 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 the 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, with the relevant section of the applicable CP, and with the certSIGN relevant internal procedures.

9.6.3 Subscriber representations and warranties

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

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

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 it has expired
- Acknowledgement of the provisions of this CPP, guarantees and limits of liability of Certsign SA

9.6.5 Representations and warranties of other participants

No stipulation

9.7 Disclaimers of warranties

Unless otherwise expressly provided in the CPS, the applicable CP 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 (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.) in the event that the data submitted when issuing certificates are false, inaccurate, incomplete or outdated or false identity documents are presented. certSIGN shall not be liable for damages incurred by the Beneficiary or third parties caused by the use of certificates issued by certSIGN by the Subject.
In any event certSIGN's liability in the event of a claim shall be limited to the value of the certificates involved in causing 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 and in paragraph 18. Liability and Indemnification from CA/B Forum.

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

All notices and other communications which may or are required to be given, served or sent pursuant to the CPS shall be in writing and shall be sent, except provided explicitly in the

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

9.12 Amendments

9.12.1 Procedure for amendment

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

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

Errors, updates, or suggested changes to this document shall be communicated as identified in the present CPS, section 1.5.4. Such communication will include a description of the change, a change justification, and contact information of the person requesting the change. The PPMB shall accept, modify or reject the proposed change after completion of a review phase.

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

9.12.2 Notification mechanism and period

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

9.12.3 Circumstances under which OID must be changed

Not applicable.

9.13 Dispute resolution provisions

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

9.14 Governing Law

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

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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

9.16.4 Enforcement

No stipulation.

9.16.5 Force Majeure

CA acts conforming to Romania Laws regarding Force Majeure.

9.17 Other provisions

No stipulation.