Certification Practice Statement for CADef CA

Version 1.23

Date: January 15, 2026

Important

Note

Address: 29 A Tudor Vladimirescu Avenue,

AFI Tech Park 1, Bucharest, Romania

Telephone: 004-021-31.19.901

Web: www.certsign.ro

Document history

Version	Date effective	Reason	Person who made the change
1.0	30 November 2022	Release of first version	PKI Policies Manager
1.1	31 Janauary 2023	Annual review	PKI Policies Manager
1.2	12 April 2023	Review certificates profiles	PKI Policies Manager
1.21	31 January 2024	Annual review	PKI Policies Manager
1.22	15 January 2025	Annual review	PKI Policies Manager
1.23	15 January 2026	Annual review	PKI Policies Manager

This document was created by and is the property of:

Owner	Author	Date created
certSIGN	PKI Policy Manager	November 2022

Distribution list

Destination	Data distributed
Public-Internet	November 2022
Public-Internet	January 2023
Public-Internet	April 2023
Public-Internet	January 2024
Public-Internet	January 2025
Public-Internet	January 2026

This document was approved by:

Version	Name	Date
1.0	Policies and Procedures Management Body (PPMB)	November 2022
1.1	Policies and Procedures Management Body (PPMB)	January 2023
1.2	Policies and Procedures Management Body (PPMB)	April 2023
1.21	Policies and Procedures Management Body (PPMB)	January 2024
1.22	Policies and Procedures Management Body (PPMB)	January 2025
1.23	Policies and Procedures Management Body (PPMB)	January 2026

Content:

1 Introduction

The Certification Practice statement of **CADef CA** – (hereinafter referred to as the **CPS of CADef CA** or **CPS**) describes the certification policy and practices that certSIGN applies in the issuance of qualified certificates for electronic signature by the **CADef CA** Subordinate Certification Authority.

The structure and content of **CPS CADef CA** are compliant to RFC 3647, ETSI EN 319 411-1 and ETSI EN 319 411-2 recommendations.

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

1.1 Overview

certSIGN, Subscribers, Subjects and Affiliated Parties must adhere to the current **CPS CADef CA** for the issuance of qualified certificates for electronic signature. The document describes the general rules for providing certification services, such as Subject registration, public key certification, certificate rekey and certificate revocation.

1.2 Document name and identification

This document is titled the **Certification Practice Statement of CADef CA**, hereinafter referred to as the **CPS CADef CA** or **CPS**.

The electronic document is available in the Repository, at https://www.certsign.ro/en/document/certsign-cadef-ca-certification-practice-statement/

1.3 PKI Participants

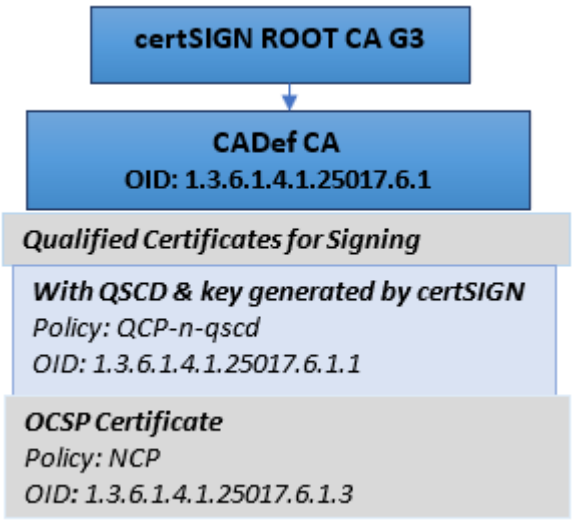
CPS CADef CA governs the most important relations between entities belonging to certSIGN, advisory teams (including auditors) and customers (users of the services provided):

- CADef CA,
- Registration Authority,
- Repository,
- Online certificate status protocol (OCSP Authority),
- Subjects,
- Subscribers,
- Relying Parties,
- Relevant suppliers for CERTSIGN regarding issuance and management of digital certificates.
- Policies and Procedures Management Body
- Auditors.

CERTSIGN provides certification services for every natural or legal entity accepting the regulations of the present CPS. The purpose of this CPS (that includes key generation procedures, certificate issuing procedure and information system security) is to ensure the users of the CERTSIGN services that the declared levels of credibility related to issued certificates comply with the Certification Authorities' practices.

1.3.1 Certification authorities

CADef CA is a Subordinate Certification Authority for the CERTSIGN domain. It is subordinated to certSIGN ROOT CA G3. CADef CA identifies by the following OID: 1.3.6.1.4.1.25017.6.1



Before starting the activity, CADef CA sends a request to the Primary Certification Authority, certSIGN ROOT CA G3, for registration and issuance of the public key certificate.

1.3.2 Registration authorities

The Registration Authority receives, verifies and approves or rejects the applications for registration and issuance of certificates, the certificate rekey or the revocation of certificates. The verification of the requests aims at authenticating (based on the documents included in the requests) both the subscriber/subject and the data included in the request. The Registration Authority may send requests to the appropriate Certification Authority to cancel an application or to revoke a certificate.

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

External RAs must comply with the same security requirements that the TSP respects in terms of human resources, operational security, network and personal data as specified in clauses 6.4.4, 6.5.6, 6.5.7 and 6.8.4 of ETSI 319 411-1.

1.3.3 Subscribers

Subscriber

Subscribers are natural persons that request to Certsign the issuance of a certificate and with whom they sign the Subscriber Agreement.

Subscribers may be:

- Natural persons - in this case, the Subscriber is the Subject of the certificate issued by Certsign,

A Subscriber is responsible for immediately notifying Certsign upon (suspicion of) private key compromise;

Subject

The subject is the entity to whom a certificate is issued and is identified in a certificate as the holder of the private key associated to the public key in the certificate.

The Subject can be:

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

A Subject is also responsible for:

- Immediately notifying Certsign upon (suspicion of) private key compromise;
- Submitting requests for renewal of keys and/or certificates to Certsign in due time;
- Protecting the confidentiality of their private key according to the document herein;
- Making sure that the access to the private key is controlled in accordance with this document.

1.3.4 Relying parties

A Relying Party can be any entity that uses CertSign services and makes decisions based on the correctness of the connection between a Subject's identity and the public key.

A Relying Party is in charge of how it verifies the current status of a Subject's certificate. Such a decision shall be taken every time a Relying Party is willing to use a certificate to verify an electronic signature, the identity of the source or the author of a message or to create a secure communication channel with the Subject of the certificate. A Relying Party shall use the information in a certificate (for example, identifiers and qualifiers of certification policy) to decide whether a certificate was used according to the stated purpose.

A particular type of Relying Parties is the e-Government IT Systems that are using qualified certificates conforming to the legislation in force. certSIGN may accept exceptions regarding the usage of the certificates only for such type of IT Systems, and only if these exceptions are not in conflict with ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 standards". certSIGN will keep public an updated record of these exceptions, if any.

1.3.5 Other participants

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

CERTSIGN service providers: external providers supporting CERTSIGN activities under a signed contractual agreement.

Public Notaries: may perform identification and guarantee for the real identity of the Subjects, under the laws of Romania.

Qualified Electronic Signature Creation Device Providers: the external providers supporting CERTSIGN activities under a signed contractual agreement that ensure the supply of physical cryptographic devices utilized by Subjects.

1.4 Certificate usage

The scope of certificates sets the purpose in which a certificate may be used. This scope is defined by two elements:

- One that defines the certificate applicability (for example electronic signature, confidentiality),
- And another that entails a list or a description of the allowed and prohibited applications.

The Relying Party is responsible for setting the credibility level necessary for a certificate to be used for a certain purpose. The Relying Party shall decide, by taking into consideration the significant risk factors, what type of certificate issued by CERTSIGN meets the formulated requests. Subjects shall know the requests of the Relying Parties (for example, these requests might be published as a signature policy or as an information security policy) and then to request CERTSIGN to issue certificates corresponding to these requests.

1.4.1 Appropriate certificate uses

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

- Properly manage public and private keys,
- certificates and associated public keys are used in compliance with their declared purpose, confirmed by CERTSIGN,
- Have built-in mechanisms of certificate status verification, certification path creation and validation control (signature availability, expiration date etc.),
- Provide relevant information regarding certificates and their status to users.

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

It is the responsibility of the Subject to use the certificates according to this CPS. It is the Subject's or the Subscriber's responsibility to use software applications that correctly interpret, display and use the information and restrictions encoded in the certificates, such as but not limited to key usage, limited liability per transaction, etc.

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

1.4.2 Prohibited certificate uses

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

1.5 Policy management

1.5.1 Organization managing the document

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

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

Web	www.certsign.ro

Table: 1.5.1 Organization managing 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

1.5.3 Person determining CPS compliance with the policy

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

Table: 1.5.3 Person determining CPS compliance with the policy

1.5.4 CPS approval procedures

The Policies and Procedures Management Body is in charge with the approval of the CPS.

Subjects/Subscribers shall adhere to the CPS implemented and published at https://www.certsign.ro/en/document/certsign-cadef-ca-certification-practice-statement.

Subjects/Beneficiaries who do not accept the new amended terms and regulations of the CPS are obliged to submit, within 15 days from the date on which the new version of the CPS was published, a statement to this effect. This will result in the termination of the Certification Services Agreement and the revocation of the certificate issued under it.

1.6 Definitions and acronyms

1.6.1 Definitions

Auditor – person who assesses the compliance with the requirements as specified in given requirements documents

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

Certificate – a Subject's public key, together with some additional information, rendered un-forgeable by encryption with the private key issued by a certification authority

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

Certification Authority Revocation List - a revocation list with CA-certificates issued to certification authorities that are no longer considered valid by the TSP

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

Cross- certification – a certificate that is used in order to establish a reliable relationship between two certification authorities

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

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

Private key – one of the asymmetric keys belonging to a Subject and used only by that Subject. In the case of asymmetric key system, a private key describes the transformation of

a signature. In the case of asymmetric encryption system, a private key describes decrypting transformation. The private key is (1) the key whose purpose is decryption or signature creation, for the sole usage of the owner; (2) that key from a key pair which is known only to the owner.

Public key – one of the keys from a Subject's asymmetric key pair which may be available to the public. In the case of asymmetric cryptography system, the public key defines the signature verification transformation. In the case of asymmetric encryption, a public key defines messages' encryption transformation.

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

Qualified Certificate for Electronic Signature - a certificate for electronic signatures, that is issued by a qualified trust service provider and which meets the requirements laid down in Annex I of the Regulation (EU) 910/2014;

Qualified Electronic Signature Creation Device refers to an electronic signature creation device that meets the requirements laid down in Annex II of the Regulation (EU) 910/2014

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

Registration Authority - entity that is responsible for identification and authentication of subjects of certificates mainly

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

Short-term certificate: certificate whose validity period, i.e. the period of time from notBefore through notAfter, inclusive, is shorter than the maximum time to process a revocation request as specified in this certificate practice statement. NOTE: Validity period as defined by IETF RFC 5280.

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

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

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

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

1.6.2 Acronyms

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

OCSP On-line Certificate Status Protocol

PKI	Public Key Infrastructure
PPMB	Policies and Procedures Management Body
QSCD	Qualified Electronic Signature Creation Device
RA	Registration Authority
RSA	Rivest, Shamir, Adleman asymmetric cryptographic algorithm
TSP	Trust Services Provider
UTC	Coordinated Universal Time

2 Publication and Repository responsibilities

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

2.1 Repository

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

- The Certificate Practice Statement for the CAs operated by certSIGN
- Terms and conditions for the use of digital certificates

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

- Ensure the publishing and archiving of the CPS, the recommended applications' lists and recommended devices,
- Provide access to information about the certificate status by publishing Certificate Revocation Lists (CRL), by means of OCSP servers or HTTP requests,
- Provide constant access to information in the Repository for Certification Authorities, Registration Authority, Subjects and Relying Parties,
- Publish CRLs or other information in due time and in compliance with deadlines mentioned in the CPS,
- Ensure secure and controlled access to information in the Repository.

2.2 Publication of certification information

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

For all issued certificates, the certificate status information is available through accessing the URLs inside the certificates for CRL or OCSP. Similarly, certificates in the trust chain can be accessed.

Availability

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

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

In case of unavailability due to a catastrophe, failure of infrastructure outside the control of CERTSIGN or any other reason, certSIGN will use its best endeavours to restore service within 24 hours.

Expired certificates, which have been revoked before their expiry shall not be removed from the revocation certificate lists.

2.3 Time of frequency of publication

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

- CPS updates,

- Certificate Revocation List is created either every 24 hours or when a certificate is revoked;
- Audit reports performed by authorized institutions – when CERTSIGN receives them;
- Additional information – after every update.

2.4 Access control to the Repository

All the information published by CERTSIGN in the Repository at the address https://www.certsign.ro/en/repository/ is publicly available.

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

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

CERTSIGN may take reasonable measures to protect against and prevent from abusive usage of the repository, the OCSP, and CRL download services.

Upon the discovery of breaches affecting the integrity of the information in the Repository, CERTSIGN shall take appropriate measures to restore the integrity of the information, shall hold guilty persons liable and shall immediately notify the affected entities.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

Certificates issued by CERTSIGN are in compliance with the X.509 v3 standard. This means that the certificate issuer and the Registration Authority that acts on behalf of the issuer approve the Subject's name in compliance with theX.509 standard (with reference to X.500 series' recommendations). Basic names of the Subjects and of the certificate issuers with certSIGN certificates are compliant with the Distinctive Name (DN) name structure – (also known as Directory Name type of structures), created according to X.500 and X.520 recommendations.

3.1.2 Need for the Names to have a logical meaning

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

The DN consists of mandatory and optional fields according to RFC 5280 and X.520 recommendations

The mandatory DN fields for natural persons are the following:

- C – international abbreviation for country name (e.g. RO for Romania),
- SN – Subject's surname and
- G – Subject's first name
- CN – Subject's name
- Serial number - – The unique serial number of the Subject assigned by the CA. The semantics of the SerialNumber is: First letter of surname + First letter of first name + index number

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

3.1.3 Anonymity or pseudonymity of Subscribers

certSIGN does not issue personal qualified certificates under a pseudonym.

3.1.4 Rules for interpreting various name formats

The interpretation of the fields in the certificates issued by CERTSIGN is made in accordance with the certificate profiles described in the Certificate Profile and CRLs (Chapter 7). The creation and interpretation of the DN will be carried out according to the recommendations specified in Chapter 3.1.2.

3.1.5 Uniqueness of names

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

3.1.6 Recognition, authentication and role of trademarks

Not applicable.

3.2 Initial identity validation

3.2.1 Proof of Private Key Possession

The requirement to present proof of possession of the private key does not apply as the pair of keys is generated by the Registration Authority.

3.2.2 Authentication of company identity

Not applicable

3.2.3 Authentication of natural person's identity

The identity documents necessary to verify the identity of individuals must be valid and meet the minimum security standards. These documents are:

- identity card or passport, for Romanian citizens,
- identity card, Passport or identity document issued by the Romanian Authorities, for foreign citizens

Verification of individuals' identity is required:

- When the natural person is the Subject of a digital certificate issued by certSIGN

All documents necessary for the identification of natural persons shall be submitted to the representatives of the Registration Authority in original or in copy accompanied by the Statement authenticated by a Notary Public or certified by a Lawyer, regarding the acceptance of the Terms and Conditions for the provision of certification services and CPS.

certSIGN reserves the right NOT to provide qualified certificates if there are reasonable indications as to the validity or truthfulness of the documents submitted by the Subject (damaged identity card or passport or which do not meet the minimum security requirements).

Issuing Certification Authority	Registration Authority identifies the natural person by one of the following methods:
CADef CA	• by personal attendance at the Registration Authority
	• by submitting a statement made available by CERTSIGN authenticated by a notary
	• by submitting a statement made available by CERTSIGN certified by a lawyer, in accordance with Article 3 paragraph (1) letter c) of Law no. 51/1995
	• based on a qualified electronic signature or qualified seal issued by the certSIGN

Table 1 Requirements for the verification of the natural persons' identity

*The procedure described in this chapter on the verification of natural person's identity shall be applied upon the first issuance of a qualified certificate to a Subject, and at every 6 years If at the date of issue of the first certificate under this CPS, the natural person have a valid qualified certificate issued by certSIGN based on the certSIGN Code of Practices and Procedures of certSIGN ROOT CA - certSIGN Qualified CA Class 3 G2, the certification can be done based on the identification done upon the issuance of the qualified certificate held.

3.2.4 Non-verified subscriber information

The Subject or the Subscriber, as the case may be, is responsible for providing up-to-date, accurate and correct information during the registration process. The phone number is the unverified information of the Subject.

3.2.5 Validation of authority

CERTSIGN verifies whether a natural person has specific rights, entitlements, or permissions, including the mandate to act on behalf of a legal entity to obtain a certificate.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Chapters 4.7 and 4.8 of this document describe this process.

3.3.2 Identification and authentication for re-key after revocation

The same process **as for initial identity validation** is used.

3.4 Identification and authentication for revocation requests

The following entities can send certificate revocation requests:

- The Subject who is the holder of the private key associated with the public key from the certificate shall send the revocation request using any of the following methods:
  - In electronic format, by sending an authenticated request signed with a qualified electronic signature created using a qualified digital certificate issued by certSIGN to the Subject (i.e. with the same Common Name). In this case, the certificate is revoked after certSIGN verifies and validates the request.
  - By completing and submitting the request to an employee of the Registration Authority. In this case, the certificate is revoked after the CERTSIGN verifies and validates the request.
- The Subscriber who enters into a contractual agreement with Certsign for the issuance of certificates to Subjects shall send the revocation request using any of the following methods:
  - In electronic format, by sending a request signed with a qualified electronic signature or qualified electronic seal. In this situation, the certificate is revoked after Certsign verifies and validates the request.
  - In a format other than electronic, by sending an authenticated request. In this case, the certificate is revoked after Certsign verifies and validates the request.
- The Registration Authority that can request the revocation either on behalf of a Subject or because it holds information that justifies the certificate revocation, by creating an

authenticated request using the security mechanisms of the Registration Authority software.
- CADef CA associated trusted roles, under the supervision of the Policies and Procedures Management Body (PPMB), by creating an authenticated request using the security mechanisms of the Certification Authority software.

4 Certificate life-cycle operational requirements

This chapter describes the basic procedures that apply to all types of certificates issued by CADef CA.
The detailed procedures related to PKI component services (CAs, RAs, CRLs signers, OCSP responder, etc.) and the persons/roles involved in the operational process of these components are described in the internal confidential documentation.
certSIGN provides access to the following services:

a) Registration, certification, re-key;
b) Certificate revocation;
c) Verification of certificate validity.

4.1 Certificate request/application/Application for a certificate

4.1.1 Who can submit a certificate application

Natural persons

Who may apply for a certificate:
- Natural persons, in case of application for the certificate on a personal basis,
- The natural person(s) (Subjects) for whom the Subscriber has requested the certificate, having a contractual agreement or acting as their employer.

The Subscriber and the Subject shall comply with the provisions and obligations set forth in contractual agreement with the Subscriber and the Terms and Conditions of certification services that incorporate this CPS.

The Certification Authority only issues certificates in response to an authenticated request from the Registration Authority operated by CERTSIGN, or a delegated third party.

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

4.1.2 Registration process and responsibilities

The registration process is handled by a specific entity referred to as the Registration Authority or RA, which is operated by certSIGN either directly or by relying on a third party, under the national law.

certSIGN may delegate the identification of subjects to third parties that can provide identification methods / procedures that provide a level of assurance equivalent to the Registration Authority (see Chapter 3.2.3.)

In any event, certSIGN, as a trusted service provider, assumes liability, within the limits set forth in this CPP, for the acts or omissions of all its agents, employees and collaborators involved in the registration process.

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 registration 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 following information and documents are made available to the Subject/Subscriber:

- Contractual agreement
- Terms and conditions
- online address for the Terms and conditions regarding the certificate use,
- online address of the CPS, notifications or other documents to be submitted by the Subject (laid down in the Contractual Agreement with the Subscriber).

By signing the contractual agreement and the Terms and Conditions, the Subject/Subscriber understands and accepts the following:

- his responsibility that the information provided by the Subject to the RA is correct, complete, valid and up to date,
- that the CERTSIGN retains for a period of at least 7 years from the date of expiry/revocation of the certificate all the information regarding the registration and enrolment, the application for the certificate and the revocation of the certificate,
- that, if certSIGN (as CA and RA) ceases its business, this data may be transferred ro a third party,
- 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/Subscriber has the obligation to inform CERTSIGN on any change or event that may affect the validity or the content of the certificate

Registration process

The registration process starts at the RA.
The responsibility of the RA entity is to collect the required documents and approvals 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.

RA verifies and fills in registration data. RA is responsible for the accuracy of data that will be included in the certificate request submitted to CA. RA is responsible for the correct

registration/enrolment of Subjects/Subscribers and for submitting to CA the correct content for the variable fields in the certificate.

4.2 Processing certificate requests

certSIGN RA accepts requests submitted individually or collectively by Subjects. Requests may be sent on paper.
The certificate request submitted on paper:

- By Subject's personal attendance to the Registration Authority, in which case, the Agreement and the Terms and conditions are signed with a handwritten signature. or
- The Subject submits the statement authenticated by a notary public or certified by a lawyer, through postal/courier services to RA, together with the contractual Agreement and the Terms and Conditions signed with a handwritten signature, and a copy of the identity document of the Subject.

4.2.1 Performing identification and authentication functions

The RA performs identification and authentication according to the procedure defined in chapter 3.2. and in the internal confidential documentation.
RA collects and validates the information on the identity and attributes of the Subject and of the Subscriber.

4.2.2 Approval or rejection of certificate requests

Approval or rejection of certificate applications is undertaken by the RA. The RA validates each request and may reject a certificate request if the request cannot be authenticated or if the request does not comply with the rules and standards governing CADef CA or for other reasons, at the discretion of and under the responsibility of RA.

4.2.3 Processing time of certificate requests

certSIGN does not issue the certificate right after the request registration. Certificates must be issued by the Certification Authority by approving the certificate request after it has been validated by RA.

The certificates are stored ona QSCD. The entity may have a QSCD when generating the keys. The delivery process of certificates may take several hours or several days and depends on the availability of the Subject to to store the certificate on the QSCD already in possession.

4.3 Certificate issuing

4.3.1 CA actions during certificate issuance

The certificate is issued by the CA only after receiving a certificate request from the RA. CA and RA are integrated systems and communicate over closed network connections. CA only processes requests originating from the trusted RA of certSIGN.
CA ensure the uniqueness of each certificate it issues using the certificateSerialNumber field in each certificate.

4.3.2 Notification of the Subject by the CA about certificate issuance

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

The keys are generated on the QSCD by Certsign and the QSCD where the digital certificate is stored is detained by the Subject. The confidential activation data (PIN code) required to access the QSCD is applied directly by the Subject on certificate loading.

certSIGN may use "Test certificates' that are certificates with a usage limited only to testing, that have a validity of maximum 30 days, and are identified by the Common Name attribute starting with the "TEST" text. The "Test certificate" will be issued by a certSIGN Registration Operator, using certSIGN procedure for test certificates. The "Test certificate" may be revoked after the testing period on request

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The certificate is deemed accepted by the Subject after the first use or after the timeframe set in the Terms and Conditions, whichever occurs first.

RA and the Subject have the right to reject the certificate or the QSCD and return the QSCD, provided at least one of the following objections applies:

- Information in the certificate is incorrect,
- Information in the certificate became invalid since the date of registration,
- QSCD shows signs of damage or tampering,
- QSCD malfunctions or cannot be activated,

Obligations of the RA in case of rejection:

- RA asks for certificate revocation,
- RA performs certificate revocation.

4.4.2 Publication of the certificate by CA

Certificates issued by CADef CA are not published, according to the contract with the Beneficiary.

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

certSIGN notifies other entities of the certificate issuance through publication in the Repository, as described in Chapter 2.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The Subject is personally responsible for:

- Using the keys only for the intended use as defined in the CPS and as encoded in the certificates;
- The private keys corresponding to qualified certificates issued under this CPS shall be used to create electronic signatures.
- Using tools that can correctly interpret the key usage as encoded in the certificate and that respect the key usage conditions

- The correct use of the QSCD
- Not sharing the QSCD to another person
- Deleting the confidential activation data (PIN code) that is unique and comply with the directives in the CPS
- Keeping confidentiality of this data
- Safe storage of any document or medium containing transcripts of part or all of the associated confidential activation data (PIN code)
- Separation of storage for the QSCD and the associated secret activation data (i.e. PIN code)
- Not disclosing the confidential activation data (i.e. PIN code) to another person.

Private key generated by certSIGN

When certSIGN generates a private key for the Subject, the Subject is in charge for:

- Initializing the QSCD and its initial associated confidential activation data (i.e. PIN code)
- Access control to the QSCD exclusively by the Subject during certificate transfer;

The Subject is bound by the conditions and obligations mentioned in the Subscriber Agreement, which includes this CPS. The Subject shall protect the QSCD and any associated secret activation data (i.e. PIN code) or other information against loss, theft, disclosure, compromise or alteration.

See sections 1.4.1, 6.1.7 and 7.1.

The Subject uses only QSCD that are in a list of validated QSCD maintain by CERTSIGN through an internal procedure, by monitoring the website https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD

certSIGN issues certificates for keys stored on the QSCD:

- The private key cannot be extracted from the QSCD,
- The private key is under the (sole) control of the Subject by means of the secret activation data (i.e. PIN code).

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

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

Parties relying on a certificate shall always verify a digital signature by checking the validity of a digital certificate against the OCSP service at http://ocsp.certsign.ro or the relevant CRL published by CERTSIGN. Under the conditions for a certificate to be validated as an EU Qualified Certificate, the trusted anchor for certificate validation shall be the one specified in the appropriate service digital identifier (SDI) in the EU Trusted List for certSIGN.

Relying Parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the Subscriber.

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the relying party. Reliance on a digital signature should only occur if:

- The digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate.
- The relying party has checked the revocation status of the certificate by referring to the relevant CRLs and the certificate has not been revoked.
- The relying party understands that a digital certificate is issued to a subscriber for a specific purpose and that the private key associated with the digital certificate may only be used in accordance with the usages specified in this CPS and contained in the certificate.

Reliance on the certificate is accepted as reasonable if the conditions set out in the CPS and in the contract concluded with the Relying Party are met. If the insurances provided by CERTSIGN in accordance with the provisions of this CPS are not fulfilled, the relying party must obtain additional insurances.

Warranties are only valid if the steps detailed above have been taken.

Relying on an unverifiable digital signature may result in risks that the relying party undertakes in whole and which CERTSIGN does not undertake in any way.

4.6 Certificate renewal

Not applicable.

4.7 Certificate Re-key

4.7.1 Circumstances for certificate re-keying

certSIGN is rekeying certificates issued for valid certificates (not expired and not revoked) issued by certSIGN, which require no change of certificate data or extensions. The rekey process consists of re-issuing a certificate with a new key pair to extend its expiration date without changing the identity or other extensions of the certificate.

4.7.2 Who can ask for certification of a new public key

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

Rekeying is performed when a Subject holding a valid (not revoked and not expired) digital certificate requests Certsign to generate a new key pair and requests the issuance of a new certificate to confirm the possession of a newly created public key.

Certificate rekeying is performed only at the request of the Subject and it shall be preceded by a request submitted using a form duly filled out by the Subscriber/Subject.

4.7.3 Processing certificate re-keying requests

The process of the initial certificate request will be amended as follows:

- The identification of the applicant is replaced by the verification of the digital signature on the request form.
- Validation results from previous requests are considered valid as long as the information validated has not changed.
- Any data that has changed will be validated as if it was a new request.

4.7.4 Notifying the Subscriber on the new certificate

RA uses the same notification processes as for a newly requested certificate.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

RA uses the same processes as for a newly requested certificate.

4.7.6 Publication of the re-keyed certificate by the CA

RA uses the same processes as for a newly requested certificate.

4.7.7 Notification of certificate issuance by the CA to other entities

RA uses the same processes as for a newly requested certificate.

4.8 Certificate modification

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

4.9 Certificate revocation and suspension

Certificates issued by CADef CA can be revoked. Certificate revocation is irreversible.
The revocation shall affect neither the transactions made prior to the revocation nor the obligations arising from abiding by this CPS.
This chapter sets out the conditions for a Certification Authority to revoke a certificate.
If a private key corresponding to a public key contained in a revoked certificate remains under the control of the Subject, after revocation it should be stored securely until it is destroyed.
Short-term certificates are not revoked. In case of short-term certificates, the mechanism to notify problems is the same mechanism described in #1.5 at "Procedure for certificate problem reporting".

4.9.1 Circumstances for certificate revocation

A certificate is revoked when:

- Information in the certificate has changed,
- A private key associated to a public key from the certificate was compromised or there is a serious reason to suspect it was compromised,
- employment relationship or the legal agreements between the Subscriber and the Subject are concluded,
- The Subject, holder of the private key associated with the public key from the certificate, requests the revocation,
- The Subscriber requests the revocation of an end-entity certificates for Subjects,
- Subjects/ Subscribers do not accept the new, modified terms and regulations of the CPS,

- Subjects/ Subscribers do not accept the new, modified terms and regulations of CPS
- The Certification Authority terminates its activity; in this case all certificates issued by this Certification Authority before the stated period for service termination shall be revoked along with the certificate of the Certification Authority,
- The Subscriber delays or is not paying the value of the services provided by CADef CA,
- The private key or the security of the certSIGN certificate have been compromised in a way that threatens the credibility of the certificates,
- Loss of QSCD status for the device on which the certificate is placed, before the end of the certificate validity period.
- In other cases where the Subject does not comply with the rules of this CPS, the Subscriber Agreement, Terms and Conditions or other agreements concluded between the parties in connection with the services provided by CADef CA.

The compromised private key means:
(1) unauthorized access to the private key or a strong reason to suspect such a thing,
(2) loss of private key or the appearance of a reason to suspect such loss,
(3) theft of the private key or the appearance of a reason to suspect such theft,
(4) accidental deletion of the private key.

4.9.2 Who can request certificate revocation

The following entities can send certificate revocation requests:

- The Subject, who is the holder of the private key associated with the public key from the certificate,
- The Subscriber, who enters into a contractual agreement with certSIGN for certification services to Subjects,
- The Registration Authority that can request the revocation either on behalf of a Subject or if it has information that justifies the certificate revocation,
- Trusted roles associate to CADef CA, under the supervision of PPMB.

The revocation request may target more certificates.

4.9.3 Procedure for certificate revocation

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

The processing of the certificate revocation request takes place as follows:

- CERTSIGN verifies the revocation request, including that it is submitted by a legitimate entity. If the request is successfully verified, CADef CA places the information concerning the certificate revocation on the Certificate Revocation List (CRL);
- certSIGN notifies the Subject about the revocation or about the decision to revoke or cancel the request, along with the reasons for these cancellations.

Whenever a certificate or a private key corresponding to a certificate to be revoked are stored on a QSCD, following the certificate revocation, the QSCD is deleted in highly secure

conditions. This action is performed by the owner of the QSCD – a natural or legal entity (a representative of such an entity). The owner of the QSCD shall keep it secure, to prevent the theft or unauthorized usage until the deletion of the private key.

4.9.4 Grace period for the revocation request

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

4.9.5 Timeframe for the CA to process the revocation request

certSIGN guarantees a maximum timeframe of 24 hours for processing a certificate revocation request**.** In this situation, the certificate is revoked after Certsign receives the request**.** When an authenticated request is sent using the revocation code received from certSIGN, the certificate is automatically revoked.
The information concerning the certificate revocation is stored in CERTSIGN database. The revoked certificates are placed on the Certificate Revocation List (CRL) in compliance with the CRL release frequency.
As an exception, in case of disaster, if the revocation request cannot be confirmed within 24 hours, certSIGN will re-schedule as soon as possible the analysis of the request and will announce all the affected parties on the reasons of the delay.

4.9.6 Verification of revocation requirements for Relying Parties

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

4.9.7 Frequency of CRLs issuance

Every Certification Authority part of CERTSIGN issues Certificate Revocation Lists. A new CRL is published in the Repository immediately after every certificate revocation, or within one day. The CRL's availability period is 48 hours and it is updated daily.
The Certificate Revocation List (CRL) for certSIGN Root CA G3 Authority is issued at least once a year, unless certificates of one of the authorities subordinated to the certSIGN CA authority have been revoked.
In case of certificate revocation of an authority affiliated to CERTSIGN this certificate is immediately published in the Certificate Revocation List.

4.9.8 Maximum latency for CRLs

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

4.9.9 Availability of online revocation/status check

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

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

4.9.10 On-line verification of revocation requirements

See chapter 4.9.6 of the current document.

4.9.11 Other forms available for the announcement of revocation

Not applicable.

4.9.12 Special requirements re key compromise

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

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

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

4.9.13 Circumstances for suspension

Certificates issued by CADef CA CANNOT be suspended.

4.9.14 Who can request the suspension

Not applicable.

4.9.15 Procedure for requesting the suspension

Not applicable.

4.9.16 Limitations of the suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

The certSIGN certificate status verification services are CRL and OCSP. Access to these services is made via the websites "www.certsign.ro" and "ocsp.certsign.ro". Certificate status services provide information on the status of valid certificates. The integrity and authenticity of status related information is protected by an electronic signature of the respective CA.

4.10.2 Availability of services

Certificate status services are available 24/7.

4.10.3 Optional features

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

4.11 End of subscription

The subscription ends after:

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

For legal compliance reasons, certSIGN and all registration authorities preserve all data and documentation for at least 10 years from the end of subscription.

4.12 Key escrow and recovery

certSIGN does NOT allow key escrow for qualified certificates.

5 Facility, Management and Operational Controls

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

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

- ETSI EN 319 401, General Policy Requirements for Trust Service Providers,
- ETSI EN 319 411-1, Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements,
- ETSI EN 319 411-2, Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;

5.1 Physical Controls

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

5.1.1 Site location and construction

All certSIGN CA and RA operations are conducted within a physically protected environment with controls based on the risk assessment that are meant to deter, prevent, detect and counteract the materialization of risks on its assets. We also maintain disaster recovery facilities for our CA and RA operations, facilities that are protected by physical security controls similar to those implemented at our primary facility. All physical security controls implemented by certSIGN are in accordance with ISO 27001 and 27002 standards and are described in detail in the security policies and procedures. Some of the most important security controls are:

- A clearly defined and protected perimeter through which all entries and exits are monitored;
- Critical components are protected with several perimeters
- An access control system configured to allow access only to those individuals appropriately cleared and specifically authorized to enter the area;
- Manned and electronic monitoring for unauthorized intrusion at all times;
- Personnel not on the access list are properly escorted and supervised;
- A site access log is maintained and inspected periodically;
- Every piece of equipment is correctly maintained to ensure its continuous availability and integrity.

5.1.2 Physical access

The physical access within certSIGN is controlled and monitored by an integrated alarm system. certSIGN has fire prevention systems, intruder detection systems and power supply systems in case of emergency.

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

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

certSIGN premises are divided into:

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

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

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

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

5.1.3 Power and air conditioning

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

5.1.4 Water exposure

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

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

When no longer required, HSMs will be factory reset to prevent any possibility of reusing CA private keys and will be returned to cryptographic inventory.

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

Secure deletion is made in accordance with the Information Security policy of certSIGN.

5.1.8 Offsite backup

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

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

5.2 Procedural controls

5.2.1 Trusted roles

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

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

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

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

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

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

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

Employees are formally appointed to trusted roles by PPMB. The "least privilege" principle is applied when configuring access privileges to trust roles.

5.2.2 Number of people required per task

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

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

5.2.3 Identification and authentication for each role

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

Each assigned account:

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

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

5.2.4 Roles requiring separation of duties

certSIGN implements and enforces a separation of roles and duties for the roles of Administrator, Operator, and Auditor to ensure that the same person cannot hold multiple roles. All those roles have job descriptions, with specific skills and experience requirements, defined from the viewpoint of roles fulfilled. The following principles are implemented: the segregation of roles and the assignment of the minimum necessary rights in the systems. Depending on how sensitive the positions are as a result of the attributions associated with them, the following are established: the access levels, as well as the procedure for verifying the previous activity of the persons who are to occupy those positions, as well as the level of training and awareness required for them.

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

5.3 Personnel control

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

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

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

5.3.2 Background check procedures

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

5.3.3 Staff training requirements

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

- CPS requirements,

- Procedures and security controls used by the Certification Authority and the Registration Authority
- Responsibilities arising from roles and tasks performed in the system,

After completion of the training, participants sign a document confirming to have become acquainted with the Certification Practice Statement, the Certification Policy and to have accepted the restrictions and obligations imposed.

5.3.4 Frequency and requirements of traineeships

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

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Requirements for independent contractors

Contract personnel (external service, developers of subsystems or applications, etc.) are subjected to the same verification procedure as employees of certSIGN (see Chapters 5.3.1, 5.3.2 și 5.3.3). In addition, the personnel employed on a contract basis, while working in the certSIGN premises, must be permanently accompanied by a CERTSIGN employee, except for those who have received approval from the security administrator and who can access classified information internally or in accordance with the legal norms in force.

5.3.8 Documentation provided to the personnel

certSIGN staff has access to the following documents:

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

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

5.4 Audit logging procedures

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

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

5.4.1 Logged events

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

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

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

Every automatic or manual log contains the following information:

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

All events about the life-cycle of CA keys are logged.

All events about the life-cycle of certificates are logged.

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

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

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

All registration information, including the following, is recorded:

- The type of document(s) submitted by the applicant upon registration;
- Registration of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable;
- Storage location of copies of applications and identification documents, including the agreement signed by the Subject/Subscriber;
- Any specific option within the agreement (i.e., consent to the certificate publication)

- Identity of the entity accepting the application;
- Method employed to validate identification documents,

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

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

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

Access to logs is allowed exclusively for the security officer, the administrators of the Certification Authorities and auditors by request sent by email or in paper format to CISO.

The privacy of subject information is kept.

5.4.2 Frequency of processing event logs

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

5.4.3 Retention period of audit logs

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

Archived logs are kept for at least 7 years.

5.4.4 Protection of audit logs

Log files shall be adequately protected by an access control mechanism. A system of adequate protection against changes and deletion of audit logs is implemented so that no one can modify or delete audit records except for transfer to a long-term preservation environment for archiving purposes. Only the security officer, administrators or an auditor may review an event log. Access to the event log is configured in such a way that:

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

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

5.4.5 Backup Procedure for Audit Logs

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

5.4.6 Audit Data Collection System (internal vs external)

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

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

5.4.7 Notification of the generating source

Not applicable.

5.4.8 Vulnerability assessments

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

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

5.5 Logs archiving

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

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

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

Backup copies are created and retained outside certSIGN location.

5.5.1 Types of archived data

The following data are included in a trustworthy archive:

- All certificates for a period of at least 7 years after their expiration
- Archived logs are kept for at least 7 years
- Logs for issuing and revoking certificates for a period of at least 7 years from the date of issue / revocation
- CRLs are retained for at least 7 years from publication
- • The following, for at least 7 years after the expiration of all certificates based on these records:
    - log of all events relating to the life cycle of keys managed by the CA
    - (signed) terms and conditions regarding use of the certificate

5.5.2 Archive retention timeframe

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

5.5.3 Archive protection

certSIGN ensures:

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

Archives are accessible only to authorized personnel.

5.5.4 Archive back-up procedures

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

5.5.5 Requirements for timestamping of logs

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

5.5.6 Archive collection system (internal or external)

Archive collection systems of certSIGN are internal.

5.5.7 Procedures to obtain and verify archived information

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

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

5.6 Key changeover

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key life, certSIGN ceases to use the expiring CA Private Key to sign Certificates (at least three years before the expiration) and

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

5.7 Compromise and disaster recovery

This chapter describes the procedures used by certSIGN in abnormal situations (including natural disasters) to restore services to the guaranteed level. These procedures are executed in accordance with the Business Continuity and Disaster Recovery Plan.

5.7.1 Incident and compromise handling procedures

certSIGN has a process for crisis management implemented as a security incident management procedure in order to respond quickly and in a coordinated manner to incidents and to limit the impact of security breaches. Employees are assigned trusted roles to track alerts of potential critical security events and to ensure that relevant incidents are reported in accordance with the procedure. In the case of critical failures, the same procedure shall be used.

The procedure for managing security incidents also specifies how the notification of the appropriate parties is made in accordance with the regulatory rules applicable to any security breach or loss of integrity that has a significant impact on the trust service provided and the personal data retained by it within 24 hours of the breach being identified.

In case of security incident, internal procedures are used. The procedures include the notification of the Supervisory body, the National CSIRT or other competent authorities.

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

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

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

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

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

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

- Physical corruption to the computer system of certSIGN, including network resources corruption – this threat addresses corruptions originating from emergency situations,
- Software and application malfunction, rendering data inaccessible – such corruptions address operating system, user applications and execution of malicious software, for example viruses, worms, Trojan horses,
- Loss of network services, important for certSIGN business. Its main site power failure and damages to the network connections.
- Corruption of part of the Intranet used by certSIGN to provide services – this can lead to customer obstruction and (unintentional) denial of services.

To prevent or limit the results of the above threats:

- The Security Policy of certSIGN includes a Business continuity and Disaster Recovery Plan.
- In the event of an event that blocks the operation of certSIGN, in maximum 48 hours, the auxiliary facility will be activated, which can substitute all the important functions of a Certification Authority until the restoration of the primary facility. The distance between the primary facility and the secondary location is large enough for the potential disaster affecting the primary facility not to affect the secondary location.
- Installation of new versions of software applications in production can only be done after their intensive testing in a test environment, in accordance with the procedures described. Any changes to the system require the approval of the Security Administrator of certSIGN.
- certSIGN systems use applications for data backup based on which the system can be restored and audited at any time. Backups include all security relevant data.
- All systems of which the IT infrastructure is composed for the provision of certification and timestamp services are continuously monitored and all security events are recorded and analysed. Abnormal system activities indicating a potential security breach, including intrusion into network systems, are detected and reported as alarms to enable certSIGN to detect, record and react in a timely manner to any unauthorized and/or unusual attempt to access its resources.
- The sensitivity of any information collected or analysed is taken into account, protecting it against unauthorized access.
- In order to detect any discontinuity in the monitoring operations, the start and stop of the logging functions is also monitored.
- The availability of all important components of the ICT infrastructure used for the provision of certification services as well as the availability of critical services are also monitored.
- certSIGN address any previously unaddressed critical vulnerability within 48 hours of its discovery. If this is cost-effective, given the impact, a plan to reduce vulnerability will be created and implemented or the decision that vulnerability does not require remediation will be documented.

5.7.2 Procedures upon compromise of an entity's private key

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

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

- Notification of compromise of all Subjects / Subscribers and other entities with which certSIGN has agreements or other forms of established relationships, among which Affiliated Entities and other Trust Service Providers. In addition, this information will be made available to other Affiliated Entities via the media system and by electronic mail.
- Notification of the general public through several channels, including a message on the certSIGN CA repository and web site, a press release in the media;
- A certificate corresponding to the compromised key is placed on Certificate Revocation List
- All the certificates signed by the corrupted CA are revoked and a suitable reason for revocation is submitted
- The Certification Authority generates a new key pair and a new certificate
- New certificates for Subject are generated
- The new certificates for Subjects are submitted to them free of charge
- If a Certificate is revoked because of CA key compromise, certSIGN Root CA G3 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.

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

5.7.3 Business continuity capabilities after a disaster

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

All system data required to resume CA operations are saved and stored in a remote and safe place to enable certification and time stamping services to resume their activities in a timely manner in the event of an incident / disaster.

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

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

The BCP & DRP plans 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 possible, steps will be taken to avoid a repeat of a disaster.

5.8 Termination of CA or RA activities

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

Requirements associated with the transfer of responsibility

Before a Certification Authority ceases its activity, it will:

- Inform (at least 30 days in advance) about the decision to terminate the services the following: all Subjects/Subscribers holding active certificates (not expired and not revoked) issued by this authority and other entities with which CertSIGN has agreements or other forms of collaboration, including Relying Parties, other trust service providers and relevant authorities, such as supervisory bodies. In addition, this information will be made available to other relying parties;
- Revoke the unexpired certificates that have been issued.
- Transfer its obligations to a trusted party to maintain all information necessary to provide evidence of the operation of the certification and timestamp services for a reasonable period of time, unless it can be demonstrated that certSIGN does not hold any such information; the information refers to registration information, to the revocation status of the unexpired certificates that were issued and to the archives of the event log for the respective period of time, as mentioned to the Subjects /Subscriber and the Relying Party;
- Destroy or withdraw from use the CA's private keys, including backups, in a manner that makes it impossible to retrieve the private keys;
- If possible, certain arrangements will be made to transfer the provision of certification services to existing customers to another certification service provider.

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

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

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

Issuance of certificates by the successor of the ceasing Certification Authority

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

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

The archive of the Certification Authority that ceases its activity must be handed over to the Primary Certification Authority – certSIGN root CA G3 in case the CADef CA authority ceases its activity.

5.9 Supply chain

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

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

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

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

6 Technical security controls

6.1 Key pair generation and installation

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

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

CADef CA owns at least one certificate signed by **certSIGN Root CA G3**. The private key corresponding to the public key contained in the certificate is used exclusively to sign the public keys of the Subjects and the Certificate Revocation List necessary for the functioning of the CA.

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

The private keys of a Subject shall be generated using a QSCD. An entity owns a QSCD when CERTSIGN is generating the key.

6.1.1 Key pair generation

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

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

After the key ceremony, certSIGN issues a key ceremony report proving that it was carried out according to the stated procedure and that the integrity and confidentiality of the key pair were secured by the trust role responsible for the security of the certSIGN key management ceremony (e.g. Security Officer), as a witness that the report accurately records the key management ceremony while it was performed.

In all cases, certSIGN:

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

CADef CA keys and the keys of other subordinated authorities and the subsequent certification of the public keys are undertaken in a physically secured environment by personnel in trusted roles under, at least, dual control:

- At least three employees in trusted roles
- The security officer
- At least one representative of the Policies and Procedures Management Body (PPMB)
- A Master of Key Ceremony
- At least one independent or external auditor

CADef CA key pairs are generated on designated workstations, authenticated and connected to security hardware modules, compliant with the requirements of FIPS 140-2 Level 3 or ISO/IEC 15408 EAL 4. They are always kept encrypted on these devices.
CADef CA key pair generation process is similar to the accepted procedure for generating keys in certSIGN, as described above. Actions performed during key pair generation are logged, dated and signed by each person present during generation. Logs are kept for the needs of joint system audits and reviews.

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

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

Prior to the expiration of its CA certificate, which is used to sign the Subject's keys, the CA will generate a new certificate to sign the Subject's key pairs and apply all necessary measures to avoid disruption of the operations of any entity relying on the CA certificate. The new CA certificate shall also be generated and distributed in accordance with this CPS. These operations must be carried out at an appropriate time interval between the expiry date of the certificate and the last signed certificate to allow all parties having relations with certSIGN (subjects, subscribers, relying parties, higher CAs in the CA hierarchy, etc.) acknowledge of this key change and implement the necessary operations to avoid creating inconveniences and malfunctions. This does not apply if we cease our operations before the expiry date of our own certificate of signature.

Subject Keys generated by the CA are generated using an algorithm recognized as suitable for future use, throughout the validity period of the certificate.

Subject keys are generated:

- By certSIGN, on behalf of the Subject, through software applications and cryptographic devices certified as QCSD in accordance with EU Regulation 910/2014. certSIGN uses only QSCD which is in a list of validated QSCDs, maintained by certSIGN through an internal procedure.

6.1.2 Delivering the private key to the Subscriber

The private key is generated by certSIGN and stored directly on the QSCD device under the exclusive control of the Subject (by PIN code known only to the Subject).

6.1.3 Delivering the public key to the certificate issuer

The distribution of a public key does not apply if a key pair is generated by certSIGN, which issues a certificate for the generated key pair directly on the Subject’s QSCD..

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

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

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

certSIGN certification Authorities publish their certificates in the repository publicly available at: https://www.certsign.ro/en/resources/

Certificates of certSIGN Certification Authorities are delivered to relying parties along with the software (operation systems, web browsers, e-mail clients etc.), which enables the use of certSIGN services.

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

6.1.5 Key size

certSIGN CA certificate uses a 4096 -bit key for certificates and CRL signing.

Digital certificates issued by CADef CA use RSA keys of 2048 bits.

Digital certificates are signed using RSA algorithm in combination with the SHA-2 algorithm.

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

6.1.6 Public Key Generation Parameters and Quality Check

certSIGN has a documented procedure for conducting CA key pair generation for all Cas, including certSIGN CADef CA.

The key pair of a subject is generated using a QSCD that meets the requirements set out in Annex II to Regulation (EU) 910/2014, with technical specifications that enable them to process key algorithms and lengths, as described in Chapter 7.

Subject keys are generated by certSIGN. Before generating the keys, the Subject has full responsibility for verifying that the hardware device used to generate the keys meets the QSCD requirements.

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

The purposes for which the keys can be used are described in the KeyUsage field (see Chapter 7.1.1.2) of the X.509 v3 standard extensions. This field must be checked by the application of the Subscriber administering the certificates.

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

a) digitalSignature: certificates for the electronic signature verification,
b) nonRepudiation: certificates for the provision of the non-repudiation service by natural persons, as well as for purposes other than those described in points f) and g). The Non-repudiation bit can only be set in a public key certificate with which it is intended

to verify electronic signatures and should not be combined with those described in points c) - e) and related to ensuring confidentiality,

c) keyEncipherment: used to encrypt keys of symmetric algorithms, providing data privacy,
d) dataEncipherment: used to encrypt Subject data other than those described in paragraphs c) and e),
e) keyAgreement: used for key exchange protocols,
f) keyCertSign: the public key is used for the verification of the electronic signature in certificates issued by entities providing certification services,
g) cRLSign: the public key is used for the verification of electronic signatures on the lists of revoked and suspended certificates issued by entities providing certification services,
h) encipherOnly: can only be used with the keyAgreement bit to indicate the purpose of encrypting data within key exchange protocols,
i) decipherOnly: can only be used with the keyAgreement bit to indicate the purpose of decrypting data within key exchange protocols.

6.2 Private Key protection and Cryptographic Module Controls

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

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

The hardware and software mechanisms that protect the CA's private keys are adequately documented. HSMs are prepared, distributed and managed in accordance with the following technical standards:

- ETSI EN 319 401
- ETSI EN 319 411-1
- ETSI EN 319 411-2

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

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

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

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

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

6.2.1 Cryptographic module standards and controls

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

The Subject is using hardware key protection devices which are qualified electronic signature creation devices (QSCD).

The key pair generation may be carried out by the Subject within the QSCD, which is a trustworthy system.

When certSIGN generates the keys on behalf of the Subject it always uses QSCD.

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

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

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

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

Acceptance of shared secret by its holders

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

Protection of the shared secret

The keepers of the shared secret must protect their part against disclosure:

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

Availability and deletion (transfer) of shared secret

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

In the event of natural disasters, the holder of the secret shall report to the CERTSIGN emergency recovery site as directed by the issuer of the shared secret. The shared secret

must be delivered personally by the holder to the emergency recovery facility, in a way that allows it to be used for certSIGN business recovery to its normal state.

Responsibilities of the shared secret holder

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

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

6.2.3 Private key escrow

Private keys of Certification Authorities are not placed in escrow.

Private keys of the Subjects are not placed in escrow.

6.2.4 Private key back-up

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

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

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

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

The existence of a backup copy of the private key does not apply to the private key of the Subjects.

6.2.5 Private key archival

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

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

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

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

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

Inserting a private key in a security hardware module of the CADef certification authority requires restoring the key on the cards in the presence of an appropriate number of holders of shared secret that protects the module containing the private keys. As every Certification Authority can retain an encrypted copy of its private key, the keys may also be transferred between modules.

The private key of the Subject is not transferred into or from a cryptographic module.

6.2.7 Storage of private keys on cryptographic module

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

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

HSMs never leave the secure environment of the CA.

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

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

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

The subjects' private keys are stored in the secured memory of the QSCD. Built-in microchip protects private keys and other security-related information against attacks.

6.2.8 Private key activating method

All **CADef CA** private keys are inserted in a module after their generation, imported in an encrypted form from another module or restored from a shared secret. Activation of private keys is always proceeded by the operator's authentication. Authentication is based on a cryptographic card held by the operator.

The private key is stored on the QSCD, under the control of the subject. The key can only be accessed using secret activation data (e.g. PIN code).

6.2.9 Private key deactivation method

CADef CA private key deactivation methods refer to the key deactivation after its use or following the completion of a session where the key was used (application logoff).

The Subject's private key is deactivated by disconnecting the QSCD from the computer or from any other device.

6.2.10 Private key destruction method

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

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

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

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

The subject is responsible for the destruction of the private key. This can be achieved either by using the middleware initialization functions of the device or by physically destroying the device.

6.2.11 Cryptographic module rating

See above.

6.3 Other Key Pair Management Aspects

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

The CA signing keys used to generate certificates and the certificate revocation will 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 AC private signing keys are destroyed at the end of their life cycle.

CADef CA certificate attributes shall be compatible with the defined key usage as set out in Recommendation ITU-T X Recommendation.

6.3.1 Public key archival

certSIGN archives its own CA public keys and all CADef certified CA public keys in the form of X509 certificates containing the key.

See chapter 5.5 for archiving conditions.

6.3.2 Operational timeframes of certificates and private key usage period

The public key usage period is defined by the value of the validity field of every public key certificate. This is also the validity applied to the private key. The maximum period of use of the Subject's keys cannot exceed the validity of a certificate.

CADef CA certificate validity period is 10 years.

The period of validity of a Subject certificate is up to 3 years.

Certificate usage periods and related private keys may be reduced in case of revocation of a certificate.

Generally, the validity start date of a certificate matches the date of its issuance. It is not allowed to set this date in the future or in the past

6.4 Activation data

6.4.1 Generating and Installing Activation Data

Activation data are used in two main situations:

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

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

The shared secrets used to protect the Certification Authority's private key are generated in accordance with the requirements set out in Chapter 6.2 and kept on cryptographic cards. Cards are protected by a PIN code. Shared secrets become activation data after their activation, for example, by correctly entering the PIN code that protects the card. certSIGN ensures that the activation data of the keys and the activation operations of the private keys of the CA, are generated, managed, stored and archived as described in the relevant subsection of sections 6.1 and 6.2. Installing and retrieving CA key pairs in a secure cryptographic device requires simultaneous control of at least two employees with trusted roles.

CERTSIGN generates private keys using The Subject’s QSCD. It is Subject’s responsibility to generate activation data (e.g. PIN code).

6.4.2 Protecting activation data

The protection of activation data includes methods of controlling the activation data by which its disclosure is prevented. The methods of controlling activation data depend on the nature of the activation data: whether they are authentication phrases or whether this control is based on the private key or on the distribution of activation information in shared secrets.

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

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

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

This chapter describes the security controls of certSIGN computers.

The subject is responsible for his own computer security controls. These aspects are not covered in the subchapters below.

6.5.1 Specific technical requirements for computer security

Security measures protecting computing systems are applied at the level of the operating system, applications as well as physically.

Computers are configured with the following security mechanisms:

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

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

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

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

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

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

6.5.2 Assessing computer security

The certSIGN information system meets the requirements described in ETSI Standards: ETSI EN 319 411 2 (Policy and security requirements for trust service providers issuing certificates, Part 2: Requirements for trust service providers issuing EU qualified certificates) and CEN CWA 14167 (Security requirements for trust systems managing certificates for electronic signatures).

6.6 Lifecycle specific security controls

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

6.6.1 System specific development controls

An analysis os security requirements is carried out at the design stage along with a definition of requirements of any system development project undertaken by or on behalf of certSIGN, to ensure that security is built into IT systems.

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

Similar rules apply when replacing hardware, such as:

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

6.6.2 Security management specific controls

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

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

6.6.3 Lifecycle security controls

Change control policies and procedures are applied to releases, modifications and emergency remediations of any operational software, as well as configuration changes that apply through the Security Policy of certSIGN.

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

Configurations of Issuing Systems, Certificate Management Systems, Security Support Systems and Front End Systems/Internal Support Systems are checked at least weekly to determine any changes that would violate the CA's security policies.

certSIGN implements internal security procedures to ensure that:

- security patches are applied within a reasonable time after they become available;
- security patches do not apply if they bring additional vulnerabilities or instabilities that outweigh the benefits of their application;

The reasons why no security patch is applied are documented.

certSIGN implements an internal capacity management procedure that ensures that for ITC infrastructure dedicated to certification services, capacity requests are monitored and projections of future capacity requirements are made to ensure that adequate processing power and storage is available.

6.7 Network security controls

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

a) Systems are segmented into networks or zones based on the functional, logical, and physical (including location) relationship between trustworthy systems and services. certSIGN applies the same security controls to all systems co-located in the same zone.
b) Access and communications between zones are restricted to those necessary for the operation of certification services. Unnecessary connections and services are explicitly forbidden or deactivated. The established set of rules is reviewed on a regular basis.
c) All systems that are critical to the certification services operation are kept in one or more secured zone(s))
d) Dedicated network for administration of IT systems and operational network are separated. Systems used for the administration of security policy implementation are not used for other purposes. The production systems for the certification services are separated from systems used in development and testing (e.g. development, test and staging systems).
e) Communication between distinct trustworthy systems are established only through trusted channels that are logically distinct from other communication channels and provide secured identification of its end points and protection of channel data from modification or disclosure.
f) If a high level of availability of external access to a specific certification service is required, the external network connection is redundant in order to ensure availability of the services in case of a single failure.
g) Regular vulnerability scan on public and private IP addresses identified by certSIGN is performed and evidence is recorded that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a trustworthy report.
h) certSIGN certification services undergo a penetration test on the related systems upon set up and after infrastructure or application upgrades or modifications that certSIGN considers to be significant. Evidence is recorded that each penetration test was

performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

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

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

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

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

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

certSIGN provides access to safe and high-security areas exclusively to trusted roles.

The **CADef CA** system is in highly secured area.

6.8 Timestamping

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

7 Certificate, CRL and OCSP profile

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

The profile of basic fields for CADef CA certificates is described Table 7.1.

Field name	Value or value constraints	
Version	3	
Serial Number	10056604df023b455abe	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Department (OU)=	certSIGN Root CA G3
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
Not before (validity period beginning date)	Oct 26 15:11:23 2022	
Not after (validity period end date)	Oct 26 15:11:23 2032	
Subject (Distinguished Name)	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-18288250
	Common Name (CN) =	CADef CA
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
Subject Public Key Info	4096 bits RSA key	
Signature	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	

Table 7.1. Profile of the basic fields for CADef CA

Profile of basic fields for certificates issued by CADef CA is described in Table 7.2.

Field name	Value and value constraints
Version	Version 3
Serial Number	Single value greater than zero (0) for all certificates issued by the certifying authorities under the CERTSIGN. It contains a random value of 8 bytes. A hardware cryptographic module is used to generate this value.
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)

Field name	Value and value constraints	
Issuer (Distinguished Name)	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-18288250
	Common Name (CN) =	CADef CA
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
Not before (validity period beginning date)	Universal Time Coordinated based.	
Not after (validity period end date)	Universal Time Coordinated based.	
Subject (Distinguished Name)	Encoded according to RFC 5280, may contain the fields shown in chapter 3.1.2.	
Subject Public Key Info	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and public key value); RSA key size is shown in chapter 6.1.5.	
Signature	Signature of the certificate, generated and coded in accordance with the requirements described in RFC 5280.	

Table 7.2. Profile of basic fields of certificates issued by CADef CA

7.1.1 Version numbers

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

7.1.2 Certificate extensions

Certificate extensions for CADef CA are described in Table 7.3.

Extension	Value or value constraints	Extension status
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.certsign.ro/certcrl/certsign-rootg3.crt	Non-critical
Basic Constraints	Subject type=CA, Path length constraint=0	Critical
Key Usage	keyCertSign (bit 5), cRLSign (bit 6)	Critical
Authority Key Identifier	2c66c503d80d4e9cfba3d81e05d4ba88e9bf1d95	Non-critical
Subject Key Identifier	f4c88f5ad7ff7318eb986c8202a81a26981f13a8	Non-critical

Extension	Value or value constraints	Extension status
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution Points	http://crl.certsign.ro/certsign-rootg3.crl	Non-critical

Table 7.3. Extensions of certified CADef CA

The extensions included in the qualified certificates for electronic signature with QSCD issued to natural persons are described in Table 7.4.

Extension	Value or value constraints	Extension status
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.certsign.ro/certcrl/certsign-cadef.crt	Non-critical
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1)	Critical
Authority Key Identifier	f4c88f5ad7ff7318eb986c8202a81a26981f13a8	Non-critical
Subject Key Identifier	KeyIdentifier is composed of the 160bits SHA-1 hash of the BIT STRING subjectPublicKey value (except for the label, length and number of unused bits).	Non-critical
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=0.4.0.194112.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.6.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical

Extension	Value or value constraints	Extension status
CRL Distribution Points	http://crl.certsign.ro/certsign-cadef.crl	Non-critical
Subject Alternative Name	Other Name: RFC822 Name and Principal Name (UPN) *This extension is optional*	Non-critical
Enhanced Key Usage	Document Signing (1.3.6.1.4.1.311.10.3.12) Client Authentication (1.3.6.1.5.5.7.3.2)	Non-critical
Qualified Certificate Statements	esi4-qcStatement-1: 0.4.0.1862.1.1 esi4-qcStatement-4: 0.4.0.1862.1.4 esi4-qcStatement-6: 0.4.0.1862.1.6 id-etsi-qcs-QcType 1: 0.4.0.1862.1.6.1 esi4-qcStatement-5: 0.4.0.1862.1.5 URL=https://www.certsign.ro/repository Language=en	Non-critical

Table 7.4. Qualified certificate for electronic signature with QSCD issued to natural persons

Certificate extensions for OCSP certificates are described in Table 7.6.

Extension	Value or value constraints	Extension status
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1)	Critical
Authority Key Identifier	f4c88f5ad7ff7318eb986c8202a81a26981f13a8	Non-critical
Subject Key Identifier	3c767c4a3c2d6c5a82c02d62f92e1789e555f0b6	Non-critical
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	Non-critical
OCSPNoCheck	-	Non-critical

Table 7.6. Certificate extensions for OCSP certificates

7.1.3 Electronic signature algorithm identifier

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

7.1.4 Name formats

See section 3.1.

7.1.5 Name constraints

Not applicable.

7.1.6 Object identifier for the identification policy

The Certificate policy object identifiers used at certSIGN Qualified CA level are described in Table 7.7 and Table 7.8.

Certification Policy Name	Policy identifier
CADef CA	**{certSIGN} .{id-policy}(6).{id-CADef-CA} (1). *subpolicy ID=1.3.6.1.4.1.25017.6.1.subpolicy ID*** See below *subpolicyID* values.

Table 7.7.Policies identifiers and their names

CA level	Type	OID
CADef CA 1.3.6.1.4.1.25017.6.1	**Qualified certificate**	***Qualified certificate for electronic signature*** ▪ With QSCD and key generated by certSIGN - **.1** ***OCSP certificate- .3***

Table 7.8 Object identifiers for certification policies

7.1.7 Use of „Policy Constraints" extensions

Not applicable.

7.1.1 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.

7.1.2 Processing semantics for the critical „Certificate Policies" extension

Not applicable.

7.2 CRL Profile

CRL profile is described in Table 7.9.

Field name	Value and value restrictions	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-18288250
	Common Name (CN) =	CADef CA
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
ThisUpdate	Date emiterii CRL	
NextUpdate	Data urmatorului update CRL	
Revoked Certificates	Revocation certificate list	

Table 7.9 CRL profile for CADef CA

7.2.1 Version numbers

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

7.2.2 CRL and CRL input extensions

CRL extensions for CADef CA are described in Table 7.10.

Extension	Value and value constraint	Extension status
Authority Key Identifier	f4c88f5ad7ff7318eb986c8202a81a26981f13a8	Non-critical
CRL Number	Number of sequence to be incremented	Non-critical
ExpiredCertsOnCRL	Generalized Time	Non-critical

Table 7.10. CRL extensions of CADef CA

7.3 OCSP profile

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

OCSP service is provided by CERTSIGN on behalf of all affiliated Certification Authorities. OCSP server, which issues certificate status confirmations, employs a special key pair for CADef CA and ROOT CA G3, generated exclusively for this purpose.

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

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

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

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

The certificate status information is included in the **certStatus** field of the **SingleResponse** structure. It can have one of the following three main values:

- GOOD – indicates that the certificate is in a valid status

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

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

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

7.3.1 Version

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

7.3.2 OCSP extensions

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

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

8 Compliance audit and other assessments

certSIGN is a qualified certification service provider under the EU Regulation 910/2014.

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

8.1 Frequency or circumstances of assessment

certSIGN business supporting the services presented in the CPS is audited at least once at every 24 months.

Th audit checks compliance with the CPS and ETSI 319401 and ETSI 319411 technical standards.

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

8.2 Auditor's identity/qualifications

The audit will be conducted by a Conformity assessment body, as defined by in the EU Regulation 910/2014.

8.3 Relation of the auditor with the assessed entity

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

8.4 Topics covered by the audit

Planned audits cover, but are not limited to, all the aspects of certSIGN operations and services certSIGN specified in the CPS CADef CA.

8.5 Action taken as a result of the deficiency

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

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

8.6 Communication of results

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

9 Other business and legal matters

9.1 Fees

Certification services fees and the types of services charged are published in the list of fees available at the address http://www.certsign.ro . Prices are set according to the internal price policy.

The services offered by certSIGN are established as follows:

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

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

9.1.1 Rates for issuance and renewal of digital certificates

Rates are set according to the internal price policy.

9.1.2 Rates for certificate access

Free of charge service.

9.1.3 Rates for revocation services or access to certificate status information

Fees are set according to the internal price policy.

9.1.4 Other rates

Fees are set according to the internal price policy.

9.1.5 Refunding

Payments may be reimbursed according to the applicable contractual conditions.

9.2 Financial liability

9.2.1 Warranty coverage

certSIGN has concluded the insurance policies in accordance with the applicable regulatory acts, i.e. Order no. 449/2017 issued by the MCSI to cover the damages it could cause due to the certification services for the persons who build their ethics based on the legal effects of the qualified certificates issued by CADef CA up to the Ron equivalent of the amount of EUR 10,000 for each insured risk.

9.2.2 Other assets

Not applicable.

9.2.3 Securing or covering the guarantee for the final entities

certSIGN benefits from insurance covering professional responsibilities, as shown before.

9.3 Confidentiality of Business Information

9.3.1 Purpose of Confidential Information

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

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

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

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

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

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

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

Types of information considered to be confidential or private

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

- Information provided by Subjects/ 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 other conditions according to the law;
- The content of the contracts concluded with the Subjects / Subscribers or Partner Entities, bank accounts, registration applications, issuance, renewal, revocation of certificates; this information may be disclosed only with the approval and for the purpose mentioned by the owner of the information (e.g., the Subject), except for the information included in the certificates or from the Repository, according to this CPS;
- The logs corresponding to the transactions in the system (all types of transactions, as well as the data for the control of transactions, the so-called transactions logs in the system);
- Event logs related to the certification services, retained by certSIGN;
- The results of internal and external audits, if they pose a threat to the security of the certSIGN;
- Emergency plans;

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

Persons who have access to confidential information are subject to the rules regarding the management of confidential information and are liable according to the legislation in force.

Disclosing the reason why a certificate has been revoked

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

Disclosing Confidential Information to the Representatives of Legal Authorities

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

9.3.2 Information not considered to be confidential

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

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

9.3.3 Responsibility to protect confidential information

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

9.4 Confidentiality of Personal Information

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

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

9.4.1 Plan to ensure the protection of personal data

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

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

- adequate technical and organizational measures are taken to ensure the security of the processed data, to protect the rights of the Subjects and to comply with the principles provided by Regulation no. 679/2016 and the provisions of Regulation (EU) no. 910/2014.

- access to certSIGN services refers to the processing of only those identification data, which are adequate, relevant and not excessive to grant access to that service
- the confidentiality and integrity of the registration data are ensured: when they are exchanged with the subscriber / subject, when they are exchanged between the components of the CERTSIGN system, as well as when they are stored.

9.4.2 Information considered as personal data

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

9.4.3 Information not considered as personal data

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

9.4.4 Responsibility to protect confidential information

certSIGN and its employees, undertake to maintain the confidentiality of personal information both during the provision of certification services and after the end of certificate validity.

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

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

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

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

9.4.6 Disclosure as a result of an administrative or legal process

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

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

9.4.7 Other circumstances for disclosure

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

✓ Disclosing personal information to:

- auditors during the audits to which CERTSIGN is subject according to the provisions of Regulation (EU) no. 910/2014 under confidentiality conditions;
- the courier companies with which certSIGN has a contract, with the consent of the Subject/Subscriber, if he has opted for sending the certificate to his home

address or to another address communicated, in compliance with the same obligations regarding the security of personal data that certSIGN has;

- proxies to whom certSIGN outsourced certain services;
- companies affiliated to certSIGN

✓ personal information appearing in certificates or in Public Directories (Repository), with the consent of the Subject/Subscriber;

✓ in any other justified situations with prior notification of the Subject/Subscriber.

9.5 Intellectual Property Rights

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

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

9.6 Representations and Warranties

9.6.1 CA representations and warranties

certSIGN issues X509 v3-compatible certificates.

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

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

9.6.2 RA representations and warranties

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

9.6.3 Subject's representations and warranties

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

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

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

9.6.4 Representations and warranties of Relying Parties

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

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

9.6.5 Representations and warranties of other participants

Not applicable.

9.7 Warranty waiver

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

9.8 Limitation of Liability

To the extent established by the Romanian law, in no case (except for fraud or willful misconduct by certSIGN) will certSIGN be liable for:

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

certSIGN shall not be liable to any person (beneficiary, subject, third party, partner entity, etc.) if the data submitted when issuing certificates are false, inaccurate, incomplete or outdated or if 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 case certSIGN's liability will be limited to 200 euro per certificate and will not exceed 10.000 euro in case of a claim, regardless of the number of certificates or the number of persons affected.

9.9 Indemnification

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

certSIGN responds and indemnifies only within the limits shown above.

9.10 Terms and termination

9.10.1 Terms

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

9.10.2 Termination

CPS remains in force until replaced by a new version.

9.10.3 Effect of termination and survival

The conditions and effect resulting from the termination of this CPS will be communicated through the website of certSIGN. This communication will highlight the provisions that may survive the termination of this CPS and will remain in force. The responsibilities for protecting Confidential Information and Personal Information must survive termination and the terms and conditions for all existing certificates will remain valid for the remainder of the validity periods of such certificates.

9.11 Individual notifications and communication with participants

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

9.12 Amendments

9.12.1 Procedure for amendment

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

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

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

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

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

9.12.2 Notification mechanism and timeframe

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

9.12.3 Circumstances in which the OID must be changed

Not applicable.

9.13 Dispute settlement procedures

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

9.14 Governing law

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

9.15 Compliance with applicable laws

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

9.16 Miscellaneous

certSIGN ensures unrestricted access to the services provided for persons with disabilities in accordance with the legislation and standards in force.

9.17 Other provisions

Not applicable.