Certification Practice Statement
certSIGN SSL EV CA Class 3

for SSL EV Certificates

Version 1.3

Date: 26 November 2018

Important
Notice

This document is property of CERTSIGN SA

Distribution and reproduction prohibited without authorization by CERTSIGN SA

Address: 29 A Tudor Vladimirescu Avenue,

AFI Tech Park 1, Bucharest, Romania

Phone: 004-021-31.19.901

Fax: 004-021-31.19.905

Web: www.certsign.ro

Document History

Version	Date	Reason	The person who made the change
1.0	January 2018	First version publishing	Information Security Officer
1.1	May 2018	CPS compliance with GDPR recommendations	PKI Policies Manager
1.2	July 2018	CPS compliance with CA-Browser Forum, about validating the Applicant's ownership or control of the domain	PKI Policies Manager
1.3	November 2018	Update change headquarters	PKI Policies Manager

This document was created and is the property of:

Owner	Author	Date created
Information Security Officer	Information Security Officer	December 2018

Distribution List

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

This document was approved by:

Version	Name	Date
1.0	Policies and Procedures Management Body	January 2018
1.1	Policies and Procedures Management Body	May 2018
1.2	Policies and Procedures Management Body	July 2018
1.3	Policies and Procedures Management Body	November 2018

Content

1 Introduction

The **Certification Practice Statement for certSIGN SSL EV CA Class 3 G2** (further referred in this document as **CPS EV CA** or **CPS**) describes in detail the certification policy applied by CERTSIGN for issuance of digital certificates by the certSIGN SSL EV CA Class 3 G2 subordinate certification authority.

The structure and content of the CPS are in compliance with RFC 3647 recommendations, current version of CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and current version of CA/B Forum Guidelines For The Issuance And Management Of Extended Validation Certificates published at http://www.cabforum.org.

1.1 Overview of Certificate Practice Statements

The CPS is the ground for **CERTSIGN** and **Certification Authority**, **Registration Authority and associated Relying Parties'** functioning regarding issuance of qualified certificates for website authentication. As well, this document describes the general rules of certification services delivery such as Subject's registration, public key certification, certificates rekey and certificate revocation.

1.2 Document name and identification

The document represents the **Certification Practice Statement for certSIGN SSL EV CA Class 3 G2**. The following OID 1.3.6.1.4.1.25017.1.1.6.1 is registered by CERTSIGN for inclusion in all SSL EV certificates:

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

1.3 PKI Participants

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

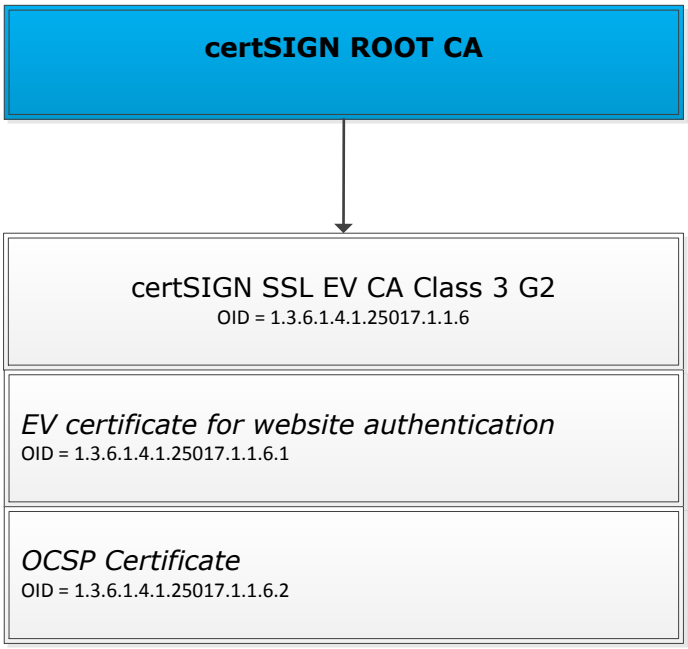
- Certification Authorities:
  - certSIGN SSL EV CA Class 3 G2
- Registration Authority,
- The Repository,
- Online certificate status protocol (OCSP),
- Subjects,
- Subscribers,
- Relying Parties,
- Relevant suppliers for CERTSIGN regarding issuance and management of digital certificates
- Policies and Procedures Management Body

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

1.3.1 Certification Authorities

The Certification Authority **certSIGN SSL EV CA Class 3 G2** is a Certification Authority for the CERTSIGN domain, subordinated to the certSIGN ROOT CA.

certSIGN SSL EV CA Class 3 G2 is identified by the following **OID: 1.3.6.1.4.1.25017.1.1.6.**



The **certSIGN SSL EV CA Class 3 G2** Certification Authority can register and issue certificates only to web servers.

1.3.2 Registration Authority

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

The Registration Authority is operated by CERTSIGN or a delegated third party, if the legislation allows this. Before CERTSIGN authorizes a Delegated Third Party to perform a delegated function, CERTSIGN contractually requires the Delegated Third Party to fulfill the conditions specified in the document "Requirements for Delegated Registration Authority for certSIGN SSL EV CA Class 3 G2 for SSL EVEV SSL certificates".

1.3.3 Subscribers

Subscriber

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

Subject

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

The subject can be:

- The Subscriber in case of requesting the certificate for himself,
- A legal entity for whom the Subscriber requests the certificate

A Subject is also responsible for:

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

1.3.4 Relying Parties

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

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

1.3.5 Other Participants

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

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

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

1.4 Certificate Usage

The purpose of SSL EV Certificate is specified by the key usage and extended key usage fields found within the EV Certificate: keyEncipherment, digitalsignature, serverAuthentication and clientAuthentication.

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

- The first defines the certificate applicability
- The other is a list or a description of the allowed and prohibited applications.

SSL EV Certificates issued under this CPS are used to identify web servers accessed via the TLS or SSL protocol.

1.4.1 Usage Purposes

The primary purposes of an SSL EV are to:

1. Identify the legal entity that controls a website: Provide a reasonable assurance to the user of an Internet browser that the website the user is accessing is controlled by a specific legal entity identified in the SSL EV by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information; and
2. Enable encrypted communications with a website: Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a website.

The secondary purposes of an SSL EV are to help establish the legitimacy of a business claiming to operate a website, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the owner of the business, SSL EV may help to:

1. Make it more difficult to mount phishing and other online identity fraud attacks using certificates;
2. Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and
3. Assist law enforcement organizations in investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

1.4.2 Excluded purposes

SSL EV focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, an SSL EV is not intended to provide any assurances, or otherwise represent or warrant:

1. That the Subject named in the SSL EV is actively engaged in doing business;
2. That the Subject named in the SSL EV complies with applicable laws;
3. That the Subject named in the SSL EV is trustworthy, honest, or reputable in its business dealings; or
4. That it is "safe" to do business with the Subject named in the SSL EV.

1.5 Policy Administration

1.5.1 Organization administering the document

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

Name S.C. CERTSIGN S.A.

Office: 29 A Tudor Vladimirescu Avenue, AFI Tech Park 1, Bucharest, Romania

Register Number: J40/484/2006

Tax registration code: RO 18288250

Registered office: 107A Oltenitei Street. building C1, ground floor, Sector 4, Bucharest, Romania, PC 041303

Phone	(+4021)3119901
Fax	(+4021)3119905
e-mail	office@certsign.ro
Web	www.certsign.ro

Table: 1.5.1 Organization administering the document

1.5.2 Contact person

Name	Policies and Procedures Management Body (PPMB)
Phone	(+4021)3119901
Fax	(+4021)3119905
e-mail	office@certsign.ro
Web	www.certsign.ro

Table: 1.5.2 Contact person

1.5.3 Person determining CPS suitability for the policy

Name	Policies and Procedures Management Body
Phone	(+4021)3119901
Fax	(+4021)3119905
e-mail	office@certsign.ro
Web	www.certsign.ro

Table: 1.5.3 Person determining CPS suitability for the policy

1.5.4 CPS Approval Procedures

Every version of this CPS is in force (has a valid status) up to the moment of publication and approval of its new version. A new version is developed by the Policies and Procedures Management Body and published for comments with the status to be approved (if applicable). Upon reception and inclusion of the remarks the CPS is supplied for internal approval. After completion of the approval procedure a new version of CPS it is published and labeled as valid. Rules and requirements concerning CPS management also govern Certification Policy management.

Subjects have to comply only with the currently applicable CPS.

If within 30 days from the publication of changes proposals to CPS, CERTSIGN does not receive significant remarks concerning these changes, a new version of CPS, with the status **under approval**, becomes a governing document of the certification policy, respected by all Subjects of CERTSIGN, and the status of the version is changed into **valid**.

Subjects/ Subscribers who do not accept new, modified terms and regulations of CPS are obligated to make a suitable statement within 15 days of the date of the new version of CPS approval. This thing results in termination of the contract related to certification services providing and the revocation of the certificated issued on its ground.

1.6 Definitions and acronyms

Access – ability to use and employ any information system resource.

Access control – the process of granting access to information system resources only to authorized users, applications, processes and other systems.
Audit – execution of an independent system review and assessment with the aim to test adequacy of implemented system management controls, to verify whether an operation of the system is performed in accordance with accepted Certification Policy and the resulting operational regulations, to discover possible security gaps, and to recommend suitable modification of control measures, the certification policy and related procedures.
Audit data – chronological records of the system activities, allowing reconstruction and analysis of the event sequence and modification to the system, associated with the recorded event.
Authenticate – to confirm the declared identity of an entity.

Authentication – security controls aimed at providing reliability of transferred data, messages or their sender, or controls of authenticity verification of a person, prior to delivery of a classified type of information.
Certificate activity period – period between the starting and ending date of the certificate validity or the period between the starting date of the certificate validity period and the moment of its revocation
Certification path – ordered path of certificates, leading from a certificate being a point of trust chosen by a verifier up to a certificate subjected to verification. A certification path fulfills the following conditions:

- For all certificates cert(x) included in the certification path {cert(1), cert(2), ..., cert(n-1)} the subject of the certificate cert(x) is the issuer of the certificate cert(x+1),
- The certificate cert(1) is issued by a Certification Authority (point of trust) trusted by the verifier,
- cert(n) is a certificate being verified.

Every certification path may be bounded with one or more certification policies or such a policy may not exist. Policies assigned to a certification path are the intersection of policies whose identifiers are included in every certificate, incorporated in the certification path and defined in the extension certificatePolicies.

Certification Policy – document formed as a set of the rules that are strictly obeyed by an issuing authority during provision of certificate services.
Certificate revocation – defines procedures concerning revocation of a valid key pair (certificate revocation) in the case when an access to the key pair has to be restricted to prevent possible usage in encryption or electronic signature creation. A revoked certificate is placed on Certificate Revocation List (CRL).
Certificate Revocation List (CRL) – periodically or immediately issued list, signed electronically by an authority, allowing identification of the certificates subjected to revocation before expiration of validity period. CRL contains the name of the CRL issuer, date of publication, date of the next update, serial numbers of revoked certificates and dates and reasons for their revocation.
Certificate and Certificate Revocation List publication – Procedures of distribution of issued certificates and revoked certificates.
Certification services provider – trusted institution (including hardware devices under its control) part of the third trusted parties which provides services able to create, sign and issue certificates or non-repudiation services.

Certificate Approver - A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve SSL EV Requests submitted by other Certificate Requesters.
Certificate Requester - A natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an SSL EV Request on behalf of the Applicant.
Confirmation Request - An appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue.
Confirming Person - A position within an Applicant's organization that confirms the particular fact at issue**.**
Contract Signer - A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements**.**
Cross-certificate –– public key certificate issued to a Certification Authority, containing different names of the issuer and the subject; a public key of this certificate may be used solely for electronic signature verification. It is clearly indicated that the certificate belongs to the Certification Authority.
Cross-certification – procedure of issuance of a certificate by a Certification Authority to another Certification Authority, not directly or indirectly affiliated with the issuing authority. Usually a cross-certificate is issued to simplify the building and verification of certification paths containing certificates issued by various CA's. Issuance of a cross-certification may be performed on the basis of a mutual agreement, between two Certification Authorities which issue cross-certification to each other.
Cryptographic module – set consisting of hardware, software, microcode or their combination, performing cryptographic operations (including encryption and decryption), executed within the area of this cryptographic module.
Distinguished name (DN) – set of attributes forming a distinguished name of a legal/private entity and distinguishing it (i.e. the entity) from other entities of the same type.
Electronic signature – cryptographic transformation of data allowing the data recipient to verify the origin and the integrity of the data, as well as protection of the sender and recipient against forgery by the recipient; asymmetric electronic signatures may be generated by an entity by means of a private key and an asymmetric algorithm, e.g. RSA.
End entity – authorized entity using the certificate as a Subject or a Relying Party (not applicable to the Certification Authorities).
Information system – entire infrastructure, personnel and components used for assembly, processing, storage, transmission, publication, distribution and management of information.
Key state transformations – state of a key may be changed only when one of the following transformations occurs (according to ISO/IEC 11770-1):

- Generation – key generation process; key generation should be performed in accordance with accepted key generation procedures; the process may include test procedure, aimed at enforcement of key generation rules,
- Activation – results in key becoming valid and available for cryptographic operation performance,

- Deactivation – constraint of a key; the situation may occur due to expiry of the validity period of a key,
- Reactivation – allows further usage of the key in the state of unavailability for cryptographic operation,
- Destruction – results in termination of key life cycle; this notion means logical key destruction but may also apply to physical key destruction.

Object – object with controlled access, for example a file, an application, the area of the main memory, assembly and retained personal data.

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

Procedure for emergency situation operations - procedure being the alternative of a standard procedure path and executed upon the occurrence of emergency situation.

Point of trust – the most trusted Certification Authority, which a Subject or a Relying Party trusts. A certificate of this authority is the first certificate in each certification path created by a Subject or a Relying Party. The choice of point of trust is usually enforced by the certification policy governing the operation of the entity issuing a given certificate.

Proof of possession of private key – information submitted by a Subject in a manner allowing the recipient to verify validity of the binding between the sender and the private key, accessible by the sender; the method to prove possession of private key usually depends on the type of employed keys, e.g. in the case of signing keys it is enough to present signed text (successful verification of the signature is the proof of private key possession), while in the case of encrypting keys, the Subject has to be able to decrypt information encrypted with a public key in his/her/its possession. certSIGN carries out verification of associations between key pairs used for signing and encrypting only on the level of Registration and Certification Authority.

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

Public key certificate – a data structure containing at least the name or identifier of a Certification Authority, a Subject's identifier, his/her/its public key, the validity period, serial number, and the assigned one by the Certification Authority. A certificate may be in one of the three basic states: waiting for activation, active and inactive.

Public Key Infrastructure (PKI) – architecture, techniques, practices and procedures that collectively support implementation and operation of certificate-based public key cryEptography systems; PKI consists of hardware, software, databases, network resources, security procedures and legal obligation bonded 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 meets the requirements laid down in Annex I of the Regulation (EU) 910/2014;

Qualified Certificate for Electronic Seal - a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III of the Regulation (EU) 910/2014;
Qualified Electronic Signature Creation Device means an electronic signature creation device that meets the requirements laid down in Annex II of the Regulation (EU) 910/2014
Qualified Certificate for Website Authentication means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;

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 repealing Directive 1999/93/EC
Revoked certificate – public key certificate placed on Certificate Revocation List.
Requester – Subject in the period between submission of a request to a Certification Authority and the completion of certificate issuance procedure
Relying Party – the recipient who has received information containing a certificate or an associated electronic signature verified with a public key included in the certificate and who has to decide whether to accept or reject the signature on the basis of the trust for the certificate.
Secret key - key applied in symmetric cryptography techniques and used only by a group of authorized Subjects.
Shared secret holder – authorized holder of an electronic card, used for storage of the shared secret.
Subject - The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber
Subject Identity Information - Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field**.**
Subscriber – A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use
Subscriber Agreement - An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
Signature Policy – detailed solutions, including technical and organizational solutions, defining the methods, scope and requirements of confirmation and verification of an electronic signature, whose execution allows verification of signature validity.
Shared secret – part of a cryptographic secret, e.g. a key distributed among n trusted individuals (cryptographic tokens, e.g. electronic cards,) in a manner, requiring m parts of the secret (where m<n) to restore the distributed key.
States of private key – private keys may have one of the three basic states (according to ISO/IEC 11770-1 standard):

- **Waiting for activation (ready)** – the key has been already generated but is not accessible for usage;
- **Active** – the key may be used in cryptographic operations (e.g. for creation of electronic signatures)
- **Inactive** – the key may be used solely for decryption and its public pair for electronic signature verification.

Token – element of data used for exchange between parties and containing information transformed by means of cryptographic techniques. The token is signed by a Registration Authority operator and may be used for authentication of its holder in the contact with a Certification Authority.
Trusted third party (TTP) – institution or its representative trusted by an authenticated entity, an entity performing verification and other entities in the area of operations associated with security and authentication.
Validation of public key certificates – verification of certificate status, allowing validation whether the certificate is revoked or not. This problem may be solved by the sole interested entity on the basis of CRL or by a request, directed to OCSP server.
Valid certificate – public key certificate is valid only when (1) it has been issued by a Certification Authority, (2) it has been accepted by the Subject and (3) it has not been revoked.

CA	certification Authority
CP	certification Policy
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CPS	certification Practice Statement
CRL	certificate Revocation List
DN	Distinguished Name
DNS	Domain Name System
EV	Extended Validation
gTLD	generic Top Level Domain
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
LRA	Local Registration Authority
OSCP	On-line certificate Status Protocol
OV	Organization Validated
PKI	Public Key Infrastructure
PPMB	Policies and Procedures Management Body
PRA	Primary Registration Authority
PSE	Personal Security Environment
QSCD	Qualified Electronic Signature Creation Device
QCP-w	Qualified Certificate Policy for Website Authentication
SSL EV	Qualified Certificate for Website Authentication
RSA	Rivest, Shamir, Adleman asymmetric cryptographic algorithm
TLD	Top Level Domain
TLS	Transporty Layer Security
TSP	Trust Services Provider
TTP	Trusted Third Party

2 Publication and Repository Responsibilities

2.1 Repositories

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

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

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

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

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

2.2 Publication of Certification Information

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

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

For all issued certificates, the certificate status information is available through CRLs and OCSP service provided by CERTSIGN 24*7*365.

CERTSIGN conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.
CERTSIGN hosts 3 web pages that allow Application Software Suppliers to test software with Subscriber Certificates issued by certSIGN SSL EV CA Class 3 G2:

http://testssl-valid-sslev.certsign.ro/

http://testssl-expired-sslev.certsign.ro/

http://testssl-revoked-sslev.certsign.ro/

CERTSIGN makes available to relying parties the terms and conditions regarding the use of the EV SSL certificates.

2.3 Time or frequency of publication

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

- Certification Policy and CPS – see Chapter 1.5,
- Certificate of the Certification Authorities – after issuing a new certificate;
- Subjects' certificates – when the consent has been obtained, after every issue of a new certificate;
- Certificate Revocation List – see Chapter 7;
- Audit reports performed by authorized institutions – when certSIGN receives them;
- Additional information – after every update.

2.4 Access control on repositories

All information published by certSIGN in the Repository accessible via http://www.certsign.ro/repository . The repository is publicly and internationally available, 24*7*365

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

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

3 Identification and authentication

The chapter hereby describes general rules for identification of the Subscriber, rules that apply when issuing a SSL EV by CERTSIGN.

The verification is mandatory performed in the stage of Subscriber registration and modification as well as upon CERTSIGN's request in case of any other certification service.

3.1 Naming

The Subject names in an SSL EV is compliant with naming convention as set in the EV Guidelines and the Baseline Requirements published by the CA/Browser Forum.

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

The Distinguished Name attribute is unique to the Subject to which it is issued. For each SSL EV, a unique serial number within the name space of the certSIGN SSL EV CA Class 3 G2 is issued.

3.1.1. Types of names

Certificates issued by certSIGN are in compliance with X.509 v3 standard. This means that the certificate issuer and the Registration Authority that acts on behalf of the issuer approve the Subject's name in compliance with X.509 standard (with referring to X.500 series' recommendations). Basic names of the Subjects and of the certificate issuers placed in certSIGN's certificates are in compliance with the Distinctive Names – DN – (also known as directory names), created following X.500 and X.520 recommendations. Within DN, it is possible to define attributes of Domain Name Service (DNS). This allows the Subjects to use two types of names: DN and DNS simultaneous. This is a very important option in case of issuing certificates to servers administrated by the Subject.

3.1.2. Need for Names to be Meaningful

For SSL certificates, FQDN name may be placed in the Common Name (CN) attribute of the Subject field. If is present in CN, it must be also copied in the Subject Alternative Name extension, in DNS Name. Subject Alternative Name are marked as non-critical, in accordance with RFC5280.

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

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

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

- Field Organization Identifier - An official unique identifier of the Subscriber as legal entity

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

Not applicable.

3.1.4. Rules for Interpreting Various Name Forms

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

3.1.5. Uniqueness of names

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

3.1.6. Recognition, authentication and role of trademarks

Not applicable.

3.2 Initial Identity Validation

Before issuing a SSL EV, the CA ensure that all Subject organization information in the Certificate conforms to the requirements of, and has been verified in accordance with, the procedures prescribed in this CPS, the EV Guidelines published by the CA/Browser Forum and matches the information confirmed and documented by the RA pursuant to its verification processes. Such verification processes are intended accomplish the following:

1. Verify the Applicant's existence and identity, including;
   a. Verify the Applicant's legal existence and identity (as stipulated in the EV Guidelines),
   b. Verify the Applicant's physical existence (business presence at a physical address) , and
   c. Verify the Applicant's operational existence (business activity).
2. Verify the Applicant's authorization for the SSL EV, including;
   a. Verify the name, title, and authority of the Contract Signer, Certificate Approver, and
3. Certificate Requester;
   a. Verify that Contract Signer signed the Subscription Agreement; and
   b. Verify that a Certificate Approver has signed or otherwise approved the SSL EV Request.
4. Verify the Applicant is a registered holder or has exclusive control of the domain name to be included in the SSL EV.

3.2.1 Method to prove Possession of Private Key

RA performs proof of possession tests for CSRs created using reversible asymmetric algorithms (such as RSA) by validating the signature on the CSR submitted by the Applicant with the SSL EV Application. .

3.2.2 Authentication of Legal Entity's Identity

RA operating under the certSIGN SSL EV CA Class 3 G2 shall perform a verification of any organizational identities that are submitted by an Applicant or Subscriber. It determines whether the organizational identity, legal existence, physical existence, operational existence, and domain name provided with an SSL EV Application are consistent with the requirements set forth in the EV Guidelines published by the CA/Browser Forum. The information and sources used for the verification of SSL EV Applications may vary depending on the jurisdiction of the Applicant or Subscriber. Under present CPS, CERTSIGN will only accept SSL EV applications from entities for which existence can be confirmed in Romania.

certSIGN PPMB may, in its discretion, update verification practices to improve the organization identity verification process. Any changes to verification practices shall be published pursuant to the standard procedures for updating the CPS.

3.2.2.1 Organization status

CERTSIGN verifies that the subscriber is an existing and legitimate organization.

As proof that it is an existing and legitimate organization CERTSIGN requires and verifies at least the following documents:

- For public/governmental organizations, a recent certified extract (up to 1 month old) in the government of the Trade the Chamber of Commerce or any law, deed or a governmental decree which states the competent representative (or representatives).;
- For private organizations a recently certified extract (up to 1 month old) from the National Trade Register.

As proof that it is a lawful organization, the TSP determines whether the latest EU to list of banned terrorist people and prevents organizations, published by the European Council.

These lists can be found on the web:

http://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX:32017D1426

CERTSIGN will not issue SSL EV certificate to an organization that is on this list.

3.2.2.2 Organization name

CERTSIGN verifies that the organization name that is included in the certificate, is accurate and complete, and corresponds to the subscriber registered organization name

As proof of the correctness of the declared official organization name CERTSIGN will at least obtain and verify the following documents:

Private organizations: A recently certified extract (up to 1 month old) from the Trade Register of the Chamber of Commerce. Further, in the supplied evidence organizational entity should be distinguished from any other organizations with the same name. An extract from the National Trade Register contains this information

Government Entities: The foregoing information concerning the legal existence and identity of a Government Entity may also be provided by a superior governing Government Entity in the same political subdivision as Applicant (e.g. a Secretary of State may verify the legal existence of a specific state department),

International Organization Entities: Legal existence and identity may be confirmed:

(a) With reference to the constituent document under which the International Organization was formed; or
(b) Directly with a signatory country's government (i.e. from an appropriate government agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization); or
(c) Directly against any current list of qualified entities that the CAB Forum may maintain at www.cabforum.org. In cases where the International Organization applying for the SSL EV is an organ or agency - including a non-governmental organization (NGO) of a verified International Organization, then CERTSIGN may verify the International Organization applicant directly with the verified umbrella International Organization of which the applicant is an organ or agency.

3.2.2.3 Organization address

CERTSIGN verifies that the data supplied by the subscriber regarding address of the organization is accurate and complete and that it is the address where the organization is operating.

Address will contain at least country, locality, street name, building number and postcode.

As proof of the correctness and existence of the organization operations at the specified address CERTSIGN requires and verifies at least the following documents:

- For public/governmental verification is performed against the public service of online verification on mfinante.ro (Ministry of Finance);
- For private organizations and unincorporated a recently certified extract (up to 1 month old) from the National Trade Register.

If the address in the supporting documents correspond thing to the address of the request CERTSIGN will consider it sufficient is evidence that this is the address where the organization carries out its work.

If the address does not match the evidence then CERTSIGN must perform a site visit at the specified location of the subscriber and capture its findings in a report. The report must include at least the following:

- Verify that the Applicant’s business is located at the exact address stated in the SSL EV Request (e.g., via permanent signage, employee confirmation, etc.);;
- Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location;;
- Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant;
- Indicate whether there is evidence that Applicant is conducting ongoing business activities at the site (e.g., that it is not just a mail drop, P.O. box, etc.), and
- Include one or more photos of (i) the exterior of the site (showing signage indicating the Applicant’s name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace..

Alternatively CERTSIGN will accept a statement by a notary that the specified address

is the address where the organization carries out its work

3.2.2.4 Organization phone verification

CERTSIGN verifies that the phone number of the organization specified by the subscriber is correct and complete.

As proof of correctness and existence of the specified general telephone number of the organization CERTSIGN:

- Calls the telephone number and obtains an affirmative response sufficient to enable a reasonable person to conclude that the Applicant is reachable by telephone at the number dialed; and
- Confirms the general telephone number of the organization as listed in the most recent version of the (online) "Pagini Aurii" - https://www.paginiaurii.ro/;

Alternatively, during a site visit, the person who is conducting the site visit could call the telephone number provided and conclude by talking to the person present at Applicant's site during the visit—who is also on the phone with the person calling—that the Applicant is reachable by telephone at the number dialed; provided that the number confirmed is not a mobile phone.

3.2.2.5 Operational existence

Subscribers of SSL EV s must satisfy the requirement of "operational existence," which is presumed if the Applicant has been in operation for three (3) years or more. If they have been in existence for less than three years, as indicated by the records of the Government Agency, then they must be listed in the current information provided by a Qualified Independent Information Source, or they must have an active current Demand Deposit Account with a Regulated Financial Institution, which may be established with authenticated documentation received directly from a Regulated Financial Institution verifying that Applicant has an active current Demand Deposit Account with the institution.

3.2.2.6 Validation of domain authorization or control

The Guidelines require that the Applicant:

a. Is the registered holder of the domain name; or

b. Has been granted the exclusive right to use the domain name by the registered holder of the domain name; and that the Applicant is aware of its registration or exclusive control of the domain name.

Verification of the authorization and identity of the representative of the legal person submitting the application on behalf of this entity is made in accordance with Chapter. 3.2.2.4.4, CA / Browser Forum BR:

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

The Random Value remain valid for use in a confirming response for 30 days from its creation.

The response e-mail must be sent using the e-mail account used for initial sending, and CERTSIGN verifies if Random Value is the same.

3.2.3 Authentication of Natural Entity's Identity

RA operating under the certSIGN SSL EV CA Class 3 G2 shall perform a verification of the identity and authority of the Contract Signer, the Certificate Approver, and the Certificate Requestor associated with SSL EV Applications that are submitted by an Applicant or Subscriber. In order to establish the accuracy of an individual identity, the RA shall perform identity and authority verification consistent with the requirements set forth in the EV Guidelines published by the CA/Browser Forum.

certSIGN PPMB may, in its discretion, update verification practices to improve the organization identity verification process. Any changes to verification practices shall be published pursuant to the standard procedures for updating the CPS.

3.2.4 Non-verified Subscriber information

CERTSIGN does not include unconfirmed subscriber information in Certificates. CERTSIGN is not responsible for non-verified Subscriber information submitted to CERTSIGN or otherwise submitted with the intention to be included in a certificate.

3.2.5 Validation of authority

For certificates issued at the request of a Subscriber's agent, both the agent and the Subscriber shall jointly and severally indemnify and hold harmless CERTSIGN, and its parent companies, subsidiaries, directors, officers, employees, agents, and contractors.

The Subscriber shall control and be responsible for the data that an agent of Subscriber supplies to CERTSIGN. The Subscriber must promptly notify CERTSIGN of any misrepresentations and omissions made by an agent of Subscriber. The duty of this article is continuous.

The authority of individuals—Contract Signers, Certificate Approvers and Certificate Requesters—to act asthe Subscriber's agents is confirmed by receipt of an SSL EV Authority Letter / Master Agreement from the Subscriber signed by a person with authority (i.e., a "Confirming Person").

(1) Confirmation Request. Persons who have such authority are contacted by CERTSIGN through an appropriate out-of-band communication requesting verification or confirmation of the particular fact in issue, i.e., the individual's authorization as a Contract Signer, Certificate Approver or Certificate Requester.

(A) Addressee. The request for the SSL EV Authority Letter / Master Agreement is directed to:

a. A position within Applicant's organization who qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) and who is identified by name and title in a current extract of the National Trade Register, a Verified Legal Opinion, a Verified Accountant Letter, or by contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for Applicant's Place of Business, verified in accordance with the Guidelines); or
b. Applicant's Registered Agent, registered Principal Individual, or Registered Office in the Jurisdiction of Incorporation or Registration as listed in the official records of the Government Agency, with instructions that it be forwarded to an appropriate Confirming Person; or

c. A named individual verified to be in the direct line of management above the Contract

Signer or Certificate Approver by contacting Applicant's Human Resources Department by phone or mail (at the phone number or address for Applicant's Place of Business, verified in accordance with the EV Guidelines).

(B) Means of Communication. Based on (A) above, the Confirmation Request is directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:

(i) If the request for the EV Authority Letter / Master Agreement is sent by paper mail, it is addressed to:

(a) The verified address of Applicant's Place of Business;

(b) The business address for such Confirming Person specified in a current extract from the National Trade Register, a Verified Legal Opinion, or a Verified Accountant Letter; or

(c) The address of Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation or Registration.

(ii) If the request for the SSL EV Authority Letter / Master Agreement is sent by e-mail, it is addressed to the Confirming Person's business e-mail address provided by Applicant's Human Resources Department pursuant to (A) above, or as listed in the extract from the National Trade Register, a Verified Legal Opinion, or a Verified Accountant Letter.

(iii) If the request for the SSL EV Authority Letter / Master Agreement is made by telephone call, then the Confirming Person is contacted by calling the verified main phone number of Applicant's Place of Business, asking to speak to such person, and the person taking the call identifies himself or herself as such person.

(iv) When a request for the SSL EV Authority Letter / Master Agreement is sent by facsimile, then it is sent to the facsimile number listed in a current Qualified Government Information Source, a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant Letter with the fax cover page clearly addressed to the Confirming Person.

(2) Confirmation Response. CERTSIGN's receipt of the SSL EV Authority Letter / Master Agreement from the Confirming Person is verified by telephone, e-mail or other written communication between CERTSIGN and the Confirming Person.

(3) Verification of Name, Title, and Authority of Contract Signer and Certificate Approver. The Guidelines require that CERTSIGN verify the name, title and authority of Contract Signers and Certificate Approvers. The SSL EV Authority Letter / Master Agreement accomplishes these objectives by providing independent confirmation from the Applicant of such name, title, and authority as outlined above. The attestations in the SSL EV Authority Letter / Master Agreement include the employment and signing authority of the Contract Signer and the employment and approval authority of the Certificate Approver.

(4) In accordance with Section 22(d)(3) of the Guidelines, CERTSIGN may rely on a verified Confirming Person to confirm their own contact information: email address, telephone

number, and facsimile number. CERTSIGN may also rely on this verified contact information for future correspondence with the Confirming Person if:

(i) The domain of the e-mail address is owned by the Applicant and is the Confirming Person's own e-mail address and not a group e-mail alias.

(ii) The Confirming Person's telephone/fax number is verified by the CA to be a telephone number that is part of the organization's telephone system, and is not the personal phone number for the person.

New gTLD domains

Before issuing a certificate containing an Internal Server Name with a gTLD that ICANN announced is at issue in view of making it operational, the CA will announce the applicant that that gTLD may become operational and that, in that moment, the CA will revoke the certificate, except in the situation when the applicant registers that domain on his/her name.

Within maximum 30 days after ICANN approves a new gTLD for operation – fact proven by posting a contract with the gTLD's operator on the www.ICANN.org website – the CA operated by certSIGN will (1) compare the new gTLD with all its valid certificate entries and (2) will stop issuing certificates containing a Domain Name that includes the new gTLD immediately after the CA has first verified the subscriber's control over the Domain Name or the exclusive right to use it.

Within maximum 120 days after posting a contract for a gTLD on the www.icann.org, the CA must revoke every certificate containing a Domain Name including the new gTLD, except in the situation when the subscriber either registered the domain on his/her name or he/she can demonstrate the control over the Domain Name.

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 the present document describe the process.

3.3.2 Identification and authentication for re-key after revocation

See Sections 4.9.1 through 4.9.3 for information about Certificate revocation procedures.

3.4 Identification and Authentication for Revocation Request

A Subscriber may request revocation of their SSL EV at any time provided that the Subscriber can validate to the RA that processed the Subscriber's SSL EV Application that the Subscriber is the organization to whom the SSL EV was issued. The RA shall authenticate a request from a Subscriber for revocation of their SSL EV by requiring the revocation code received by the Subscriber at the SSL EV Application and/or some subset of the information provided by the Subscriber with the SSL EV Application. Upon receipt and confirmation of such information, the RA shall then process the revocation request as stipulated in 4.9.

4 Certificate Life-Cycle Operational Requirements

This chapter describes the basic procedures that are common to all types of Subject certificates within the certification process.
The in depth procedures relating to PKI component services (CAs, RAs, CRLs signers, OCSP responder, Timestamping Authority, etc.) and the related personals/roles involved in the operational process of these components are described in internal confidential documentation. The following section provides a description of these documents that can be disclosed publicly.
In basic lines the certification process begins with the Subject: *indirectly* sending a request (after original confirmation of the request by the Registration Authority). Based on the request, the Certification Authority takes a decision concerning the provisioning / rejection of the service requested. The requests sent shall contain necessary information for correct identification of the Subject and Subscriber.
certSIGN provides access to the following basic services:

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

Work schedule

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

4.1 Certificate Application

To obtain an SSL EV, an Applicant must:

a. Generate a secure and cryptographically sound Key Pair,
b. Agree to all of the terms and conditions of the CPS and the Subscription Agreement, and
c. Complete and submit an SSL EV Application, providing all information requested by an RA.

The following Applicant roles (refer to the EV Guidelines for a definition of each role) are required for the issuance of a SSL EV:
Certificate Requester – The SSL EV request must be signed and submitted by an authorized Certificate Requester.
Certificate Approver – The SSL EV request must be reviewed and approved by an authorized Certificate Approver.
Contract Signer – A Subscription Agreement applicable to the requested SSL EV must be signed by an authorized Contract Signer.
One person MAY be authorized by the Applicant to fill one, two, or all three of these roles. An Applicant MAY also authorize more than one person to fill each of these roles.
Upon an Applicant's completion of the SSL EV Application and acceptance of the terms and conditions of this CPS and the Subscription Agreement, RA follows the procedures described in chapters 3.2.2, 3.2.3, 3.2.5 to perform verification of the information contained in the SSL EV Application. If the verification performed by a RA is successful, the RA may, in its sole discretion, request the issuance to the Applicant of an SSL EV from certSIGN SSL EV CA Class 3 G2. If a RA refuses to request the issuance of an SSL EV, the RA shall (i) use commercially reasonable efforts to notify the Applicant by email of any reasons for refusal, and (ii) promptly refund any amounts that have been paid in connection with the SSL EV Application.

In the event of successful verification of an SSL EV Application, the RA shall submit a request to an EV CA for the issuance of an SSL EV and shall notify the Applicant by email once an SSL EV has been issued by the EV CA. The Applicant will be provided with a URL that can be used to retrieve the SSL EV.

4.1.1 Certificate Authority Authorization

CERTSIGN checks certification authority authorization (CAA) records in accordance with RFC 6844 as part of the domain verification process.
If a CAA record exists that does not list CERTSIGN as an authorized CA, an RA will verify the use of the domain name despite the CAA record.

4.1.2 Who can submit a certificate application

certSIGN SSL EV CA Class 3 G2 maintains an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. This information is used to identify subsequent suspicious certificate requests.

4.1.3 Enrollment process and responsibilities

The enrolment process is handled by a specific entity that is referred to as the Registration Authority or RA under the responsibility of CERTSIGN.
CERTSIGN provides the infrastructure and the operational resources for the operation of the RA. CERTSIGN also provides supervision, support for and auditing for all the processes and services of the RA. The RA is responsible for the verification of the following items:

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

The enrolment process is performed in compliance with the rules and methods described in the present CPS and in the internal guidelines and procedures of the RA.
The following Applicant roles are required for the issuance of an SSL EV:

- Certificate Requester – The SSL EV Request Form MUST be submitted by an authorized Certificate Requester.
- Certificate Approver – The SSL EV Request Form MUST be approved by an authorized Certificate Approver.
- Contract Signer – A Subscriber Agreement applicable to the requested SSL EV MUST be signed by an authorized Contract Signer.

Prior to the issuance of a Certificate, the CA SHALL obtain the following documentation from the Applicant:

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

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

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

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

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

The information extracted from the PKCS#10 CSR, i.e., the company name from the Organizational name (e.g., O= CERTSIGN SA) and the domain name from the Common Name (CN=www.certsign.ro) contained in the PKCS#10 CSR is verified against the full legal name of the organization (and if applicable, any assumed name) in the application. If the common name does not match, the Certificate Requester must make the necessary corrections and generate and re-submit a new PKCS#10 to proceed. (If other information does not match, a new PKCS#10 may or may not be required, depending on the server platform.) CERTSIGN registration personnel compare the information submitted by the Requester to ensure that it is consistent with the information received under the heading cap. 3.2.2.4.4, CA/Browser Forum BR record before allowing the application process to continue.

4.2 Certificate Application Processing

During the certificate approval process, CERTSIGN Registration Personnel employ controls to validate the identity of the Subscriber and other information featured in the certificate application. CERTSIGN registration personnel review the application information provided by the Applicant to ensure compliance with the Guidelines.

The following steps describe the milestones in the Certificate Application Processing:

Steps 1: The Certificate Requester fills out the certificate request form, the PKCS#10 CSR, common name, organizational information, address, and billing information along with his or her electronic signature or physical format with handwritten signature. The Requester submits other required information to CERTSIGN, including contact names of personnel within the organization who have authority to approve the request and sign the Subscriber Agreement. The Requester provides a Purchase Order to verify the payment for processing the request and issuing the SSL EV.

Step 2: CERTSIGN verifies all information that is required to be verified by the Guidelines using a variety of sources, including National Trade Register, ICANN, Ministry of Finance, Verified Accountant Letters, Verified Legal Opinions, and the Applicant's Human Resources Department.

Steps 3: CERTSIGN requests and receives a signed SSL EV Authority Letter / Master Agreement from the Applicant (unless a valid SSL EV Authority Letter / Master Agreement from the Applicant is already in its possession).

Step 4: The Contract Signer accepts and signs Subscriber Agreement in electronic format or physical on paper and handwritten signature. After this the processing of the request

Step 5: The Certificate Approver is either contacted by telephone or directed to a web page whereby the Certificate Approver's approval of certificate issuance is obtained.

Step 6: All signatures by Certificate Requesters, Certificate Approvers and Contract

Signers are verified through follow-up procedures or telephone calls. Alternatively, if the signatures are performed using qualified certificates conforming to EU 910/2014 no further verifications are made.

Step 7: Two (2) CERTSIGN Operators (A Registration Officer and A Validation Specialist) are required to approve issuance of the Certificate (see Final Cross-Correlation and Due Diligence below).

Step 8: A secure system is used to send the certificate generation request to the certSIGN SSL EV CA Class 3 G2, and the Qualified Web Certificate is created.

Step 9: The Certificate Requester is notified that the Certificate has been created and

is ready for download (or is sent to the Requester zipped in an e-mail).

4.2.1 Performing identification and authentication functions

Identification and Authentication for a Subject certificate The Registration Authority Officers performs identification and authentication of the end-users according to procedure defined in chapter 3.2.
The RA collects and validates the Subject's and Subscriber's identity information and attributes information.

4.2.2 Approval or rejection of certificate applications

Prior to a determination of whether to approve or reject an application for a SSL EV, CERTSIGN conducts other verification checks required by the Guidelines, including the following:

1. Applications for SSL EV are screened for high-risk targets of phishing and other fraudulent schemes. CERTSIGN checks appropriate internal and external lists of organization names that are most commonly targeted in phishing and other fraudulent schemes, and automatically flags such SSL EV Requests for further scrutiny before issuance.
2. Individual names, applicant names, physical locations and jurisdictions of Applicants for SSL EV are reviewed to determine whether they are identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization as specified in 3.2.2.1.

Final Cross-Correlation and Due Diligence

Approval of certificate issuance by CERTSIGN requires two Operators (Registration Operator and Validation Specialist. (See Section 5.2.2, Number of Persons Required per Task, and Section 5.2.4, Roles Requiring Separation of Duties).

(a) CERTSIGN's procedures ensure that a Registration Operator who is not responsible for the collection and review of information reviews all of the information and documentation assembled in support of the SSL EV and looks for discrepancies or other details requiring further explanation.

(b) CERTSIGN requests, obtains and documents further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, Qualified Independent Information Sources, and/or other sources of information, as necessary to resolve the discrepancies or details requiring further explanation.
(c) CERTSIGN does not issue an SSL EV until the entire corpus of information and documentation assembled in support of the SSL EV is such that issuance of the Certificate will not communicate inaccurate factual information that CERTSIGN knows, or by the exercise of due diligence should discover, from the assembled information and documentation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, CERTSIGN will decline the SSL EV Request and notify the Applicant accordingly.
(d) CERTSIGN performs the requirements of Final Cross-Correlation and Due Diligence through employees under its control and having appropriate training, experience, and judgment in confirming organizational identification and authorization.
(e) In the case where some or all of the documentation used to support the application is in a language other than English or Romanian, a CERTSIGN employee skilled in such language having the appropriate training, experience, and judgment in confirming organizational identification and authorization performs the requirements of this Final Cross-Correlation and Due Diligence. When CERTSIGN employees do not possess the necessary language skills, CERTSIGN relies on language translations of the relevant portions of the documentation provided by a qualified Translator.

From time to time, CERTSIGN may modify the requirements related to application information requested, based on CERTSIGN requirements, business context of the usage of certificates, or as it may be required by law.

Following successful completion of all required validations of a certificate application, CERTSIGN will approve an application for an SSL EV.

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

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

4.2.3 Time to process certificate applications

CERTSIGN does not issue certificate immediately upon registration. Certificates have to be issued by the Certification Authority; by approving the certificate request received from the RA therefore the certificates are not immediately available to the Subscriber when the certificates are created by the CA.

Every form request is processed as it follows:

- Registration Authority's operator receives the Subscriber's request
- The operator verifies the data from the request regarding the Subject and the Subscriber

- Following the verification, the operator confirms the identity between the data stated and those included in the request; if the request contains non-compliant data it is rejected,
- The request confirmed is sent to the Certification Authority,
- The Registration Authority verifies also other data that are not specified in the request but they are also necessary for issuing the certificate.

Request Processing in the Certification Authority

The Certification Authority verifies if the Registration Authority confirmed the requests.

4.3 Certificate Issuance

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

4.3.1 CA actions during certificate issuance

The certificate is issued as part of the certificate enrolment process. The CA will only receive certificate requests from the RA. The CA, the RA and the personalization process are integrated systems and communicate over closed network connections. The CA only process requests that are originated from the trusted RA of CERTSIGN.
For every certificate request, the CA will perform the following verifies and actions:

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

4.3.2 Notification to Subject by the CA of issuance of certificate

The certificate is issued as part of the certificate enrollment process. The Subscriber receives a notification of certificate issuance.
One month before the certificate expiration, the Subscriber is informed that the certificate is about to expire.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

The RA and the Subscriber have the right to reject the certificate provided at least one of the following objections applies:

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

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

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

4.4.2 Publication of the certificate by the CA

See chapter "PUBLICATION AND REPOSITORY RESPONSIBILITIES"

4.4.3 Notification of certificate issuance by the CA to other entities

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

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

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

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

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

See Sections 1.4.1, 6.1.7 and 7.1.

4.5.2 Relying party public key and certificate usage

CERTSIGN assumes that all user software will be compliant with X.509, the SSL/TLS protocol, and other applicable standards that enforce the requirements and requirements set forth in this CPS. CERTSIGN does not warrant that any third party's software will support or enforce

such controls or requirements, and all relying parties are advised to seek appropriate technical or legal advice.

Parties relying on an SSL EV must adhere to the SSL/TLS protocol and verify a digital signature at all times by checking the validity of a digital certificate against the OCSP service at http://ocsp.certsign.ro or the relevant CRL published by 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 or the security of an SSL/TLS session is exclusively that of the relying party. Reliance on a digital signature or

SSL/TLS handshake should only occur if:

- The digital signature or SSL/TLS session 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 is accepted as reasonable under the provisions made for the relying party under this CPS and within the Relying Party Agreement. If the circumstances of reliance exceed the assurances delivered by CERTSIGN under the provisions made in this CPS, the relying party must obtain additional assurances.

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

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

By means of this CPS, CERTSIGN has adequately informed relying parties on the usage and validation of digital signatures and SSL/TLS sessions through this CPS and other documentation published in its public repository available at http://www.certsign.ro/repository or also due to CERTSIGN availability via the contact addresses specified in Sections 2.2 and 9.11 of this CPS.

4.6 Certificate Renewal

CERTSIGN does not perform certificate renewal.

4.7 Certificate Re-key

Pursuant to Section 25(b) (Validation of Re-issuance requests) of the EV Guidelines, CERTSIGN may rely on previously verified information to issue a Replacement Certificate where:

i. The expiration date of the Replacement Certificate is the same as the expiration date of the currently valid SSL EV being replaced, and

ii. The certificate subject of the Replacement Certificate is the same as the certificate subject contained in the currently valid SSL EV.

Re-keying, or replacing a certificate, means to request a new certificate with the same certificate contents except for a new Public Key. This might occur, for instance, if the subscriber accidentally deletes the corresponding private key. (Note that some device platforms, e.g. Apache, allow renewed use of the private key.) If the Subscriber's other contact information and private key have not changed, CERTSIGN can issue a Replacement Certificate using the same PKCS#10 CSR as was used for the previous certificate. Otherwise, a new PKCS#10 CSR must be submitted and a Replacement Certificate is issued, provided that the Subscriber otherwise qualifies, above. Other aspects of certificate re-key (e.g., who may request re-key, notification of issuance, conduct constituting acceptance, and publication of the certificate) are the same as they are for initial certificate issuance. See Sections 3.3.1, 4.1, 4.2, 4.3 and 4.4

4.7.1 Circumstance for certificate re-key

CERTSIGN performs rekeying of certificates which have not been revoked prior to their expiry.

CERTSIGN CA and RA work together to request or push re-keys of end entity certificates at a configurable time prior to the expiry of certificates.

The timeframe and methods for notification are configurable.

4.7.2 Who may request certification of a new public key

certSIGN allows the re-key process to be initiated by both the Subscriber of the certificate, or the CA / RA managing that appropriate certificate.

4.7.3 Processing certificate re-keying requests

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

- The identification of the requester and validation results from previous requests are considered valid while the validated information has not changed and those information are obtained from a source specified under Section 3.2 no more than thirty-six (36) months prior to issuing the Certificate.

Any data that has changed is to be validating as if this was a new request.

4.7.4 Notification of new certificate issuance to Subject

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

4.7.5 Conduct constituting acceptance of a re-keyed certificate

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

4.7.6 Publication of the re-keyed certificate by the CA

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

4.7.7 Notification of certificate issuance by the CA to other entities

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

Key certification and rekey is done when a Subscriber, in the name of a Subject (already registered) generates a new key pair (or orders a Certification Authority to generate such a key pair) and requests the issuance of a new certificate to confirm the possession of a new created public key.

Key certification or certificate rekey is performed only upon Subscriber's request and shall be preceded by the submission of a request on a corresponding form filled in by the Subscriber. Requests will be confirmed in case the Registration Authority's operator asks it.
Procedures for processing the rekey and certification request are equivalent to processing procedures for certificate requests described in Chapter 4.2 and certificate issuance procedures described in Chapter 4.3. Following this process:

- The Subscriber is informed about the issuance of the new certificate and its serial number.
- A new certificate is published in the Certification Authority's Repository.

Certification and certificate rekey procedure is as well applicable to certificates of a certain Certification Authority, although in such a situation all clients of the Certification Authority will be informed about the procedure execution.
certSIGN always informs Subscriber (with at least 30 days before) about the approach of the expiry period. This information is sent as well for Certification Authority's certificates.

4.8 Certificate Modification

CERTSIGN does not allow modification of certificate details during the lifetime of the certificate. If any information on the certificate changes, the Subscriber must request revocation of the original certificate and request that a new certificate be issued. CERTSIGN may, at its discretion, credit a portion of the cost of the new certificate to the Subscriber's account. See Sections 4.1, 4.2, 4.3 and 4.4.

4.9 Certificate Revocation

A certificate revocation has a significant influence on its usage and on Subscriber's obligations. Shortly after a Subject's certificate revocation, the certificate shall be considered invalid (under revocation). Similarly, in case of the Certification Authority's certificate – the cancellation of a certificate's validity means the withdrawal of the certificate issuance rights for its owner and the revocation of all certificates issued by him.
The revocation affects neither the transactions made before the revocation, nor the obligations resulting from the following of the present CPS.
This chapter states the conditions necessary for a Certification Authority to have reasons to revoke the certificate.

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

4.9.1 Circumstances for certificate revocation

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

- The information within the certificate has changed,
- A private key associated to a public key within the certificate or on the storage device was compromised or there is a serious reason to suspect it was compromised,
- The Subscriber requests the revocation,
- May be revoked by the issuer, certSIGN for instance, if a Subscriber does not follow the Certification Policy, CPS or the agreement, or other documents issued by the Certification Authority,

- The Certification Authority terminates its activity; in this case all certificates issued by this Certification Authority before the stated period for terminating the services shall be revoked along with the certificate of the Certification Authority,
- The Subscriber delays or does not pay the value of the services rendered by the Certification Authority,
- The private key or the security of a Certification Authority were compromised in a manner that endangers the certificates' credibility,
- CERTSIGN's right to issue and manage SSL EV certificates under the EV Guidelines, EU Regulation 910/2014 and Baseline Requirements
- In other cases when the Subscriber does not comply with the rules of this CPS, Certification Policy, or the agreement.
- CERTSIGN receives a lawful and binding order from a government or regulatory body to revoke the SSL EV;
- CERTSIGN receives notice or otherwise become aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the SSL EV, or that the Subscriber has failed to renew its domain name;
- CERTSIGN determines, in its sole discretion, that the SSL EV was not issued in accordance with the terms and conditions of the EV Guidelines and QCP-w;
- CERTSIGN determines that any of the information appearing in the SSL EV is not accurate;
- CERTSIGN receives notice or otherwise becomes aware that there has been some other modification of the information pertaining to the Subscriber that is contained within the SSL EV; or
- If CERTSIGN receives notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person as defined in EU list specified at 3.2.2.1

The private key compromised means: (1) unauthorized access to the private key or a strong reason that determine to believe such thing, (2) private key loss or occurrence of a reason to suspect such a loss, (3) private key stolen or occurrence of a reason to suspect such a robbery, (4) accidental deleting of the private key.
The revocation request can be sent through the Registration Authority (this implies the Subscriber to contact the authority), or directly to a Certification Authority (the request may be authenticated by signature). The revocation request shall contain information that allow the secure authentication of the Subscriber by the Registration Authority in compliance with provisions of Chapter 3.1.8. If the Subscriber's identity authentication is not successful, the Certification Authority rejects the revocation request.

4.9.2 Who can request certificate revocation

The Subscriber and its appropriately authorized parties can request revocation of an SSL EV (e.g., a Contract Signer, Certificate Approver or Certificate Requester identified by the Subscriber in SSL EV Authority Letter / Master Agreement). CERTSIGN may, if necessary, also request that the revocation request be made by either an organizational contact, billing contact or the domain registrant.

For a party who is not the Subscriber, the filing of a "Certificate Problem Report" is the first step in initiating a certificate revocation request. These persons include Relying Parties, Application Software Vendors, and other third parties who may make reports to CERTSIGN of

complaints or suspected Private Key compromise, SSL EV misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to SSL EV.

Registration Authority acts with extreme caution when processing revocation requests that were not sent by the Subscriber and accept only those requests in compliance with Chapter 4.9.1.

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

- Verifies if the respective party has the right to issue such a request
- Requests a justification for the respective request
- Sends a notification concerning the revocation or the starting of the revocation process to the Subscriber.

Every request shall be sent:

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

Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing CERTSIGN of reasonable cause to revoke the certificate. The revocation request may aim more certificates.

4.9.3 Procedure for certificate revocation

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

The certificate revocation may be performed as follows:

- The Subscriber sends to CERTSIGN an electronic revocation request authorized by the password received together with the certificate, or
- The Subscriber sends to CERTSIGN an electronic revocation request electronically signed by the Subscriber with a valid qualified certificate(not revoked or expired), or
- The Subscriber provides in person the revocation request on paper at one of the CERTSIGN Registration Authorities and the authenticity of the paper document is realized by the Registration Authority; after the successful verification of the request the Registration Authority prepares an electronic revocation request and submits it to the Certification Authority, or
- The Subscriber's representative submits a revocation request either electronically or on paper. CERTSIGN contacts the Subscriber via telephone in order to obtain confirmation; only after the confirmation is obtained the certificate may be revoked. The phone number of the company is the one identified in the initial registration process.

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

Every certificate revocation request shall provide means of univocal identification of the revoked certificate, shall contain reasons for which the revocation is requested and shall be authenticated.

A certificate revocation request takes place as it follows:

- CERTSIGN verifies the revocation request, including that it is submitted by a legitimate entity. If the request is successfully verified, the Certification Authority places the information concerning the certificate revocation in the Certificate Revocation List (CRL);
- The Certification Authority notifies the Subscriber about the revocation or about the decision of request cancellation along with the reasons for this cancellation.

If a certificate or a private key corresponding to a certificate to be revoked were stored on a hardware device as following the certificate revocation, the hardware device must be initialized in high security conditions.

4.9.4 Procedure for certificate problem reporting

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

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

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

4.9.5 Revocation request grace period

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

4.9.6 Time within which CA must process the revocation request

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

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

As it is described in Table 4.9.5.

Certification Policy	Allowable grace period
certSIGN	Within 24 hours

Table 4.9.5. The maximum period for processing a certificate revocation request

CA decides whether revocation or other appropriate action is warranted based on at least the following criteria:

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

The information concerning the certificate revocation is stored in CERTSIGN's database. The revoked certificates are placed in the Certificate Revocation List (CRL) in compliance with the publishing periods of CRL.
At the time of certificate revocation the operators of the Registration Authority and Subscriber involved are automatically informed about this revocation. Information about the current status of the certificate is available by means of the certificate status verification service immediately after the stated grace period. This service may be requested, for example, by a Relying Party that verifies the availability of an electronic signature applied to a document received from the Subscriber.

4.9.7 Revocation checking requirements for relying parties

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

4.9.8 CRL issuance frequency

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

4.9.9 Maximum latency for CRLs

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

4.9.10 On-line revocation/status checking availability

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

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

4.9.11 On-line revocation checking requirements

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

For the status of Subscriber Certificates, the CA updates information provided via an Online Certificate Status Protocol at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.

For the status of Subordinate CA Certificates:

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

(i) Every twelve months and
(ii) Within 24 hours after revoking a Subordinate CA Certificate.

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

4.9.12Other forms of revocation advertisements available

Currently, no other forms of revocation advertisements are available.

4.9.13 Special requirements re key compromise

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

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

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

4.9.14Circumstances for suspension

Not applicable

4.9.15Who can request suspension

Not applicable

4.9.16Procedure for suspension request

Not applicable

4.9.17Limits on suspension period

Not applicable

4.10 Certificate status services

Not applicable

4.10.1Operational characteristics

CERTSIGN's certificate status services are CRL and OCSP. Access to these services is made through the web site "certsign.ro" and the on line "ocsp.certsign.ro". The certificate status

services provide information on the status of valid certificates. The integrity and authenticity of the status information is protected by a digital signature of the respective CA.

4.10.2 Service availability

Certificate status services are available 24 hours per day, 7 days per week.
The CA maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Optional features

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

4.11 End of subscription

End of subscription occurs after:

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

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

4.12 Key escrow and recovery

CERTSIGN does not perform escrow or recovery of the subscriber private keys..

5 Facility, Management and Operational Controls

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

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

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

- ETSI EN 319 401, General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1, Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2, Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 421, Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

5.1 Physical Controls

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

5.1.1 Site location and construction

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

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

- A clearly defined and protected perimeter through which all entry and exit is controlled;
- Critical components are protected with several perimeters
- An entry control system which admits only those individuals appropriately cleared and specifically authorised to enter the area;

- Manned and electronic monitoring for unauthorized intrusion at all times;
- Personnel not on the access list are properly escorted and supervised;
- A site access log is maintained and inspected periodically;
- Equipment is correctly maintained to ensure its continued availability and integrity.

5.1.2 Physical access

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

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

Areas occupied by CERTSIGN are divided into:

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

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

Access to the *operators' area* is enforced through the use of an electronic card and their appropriate reader. Since all sensitive information is protected by the use of safes, while access to operator's or administrator's terminal requires prior authorization, the employed physical security is assumed as adequate. Keys to the area are accessible only to authorized personnel. The area may be occupied solely by CERTSIGN personnel and authorized individuals, the latter being granted access only if accompanied.

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

5.1.3 Power and air conditioning

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

5.1.4 Water exposure

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

Paper and electronic media containing information significant for CERTSIGN security after expiration of the retention period are destroyed. Security hardware modules are reset and deleted in compliance with the manufacturer's recommendations. These devices are, as well, reset and securely deleted when sent to service or repaired.

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

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

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

5.1.8 Waste disposal

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

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

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

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

5.1.9 Offsite backup storage

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

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

5.2 Procedural controls

5.2.1 Trusted roles

All the roles involved in the the provision of CERTSIGN's certification services are filled with employees of CERTSIGN.

All employees of CERTSIGN committed under signature to not having conflicting interests with CERTSIGN, maintaining confidentiality of information and protecting personal data.

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

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

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

- **Security officer** – Overall responsibility for the implementation of the security practices and policies.
- **System administrator** – Authorized to install, configure and maintain the Certification Authority's trustworthy systems for registration, certificate generation, subject device provision and revocation management. Installs hardware and operating systems; installs and configures the network equipment.
- **System operator** – Responsible for operating the Certification Authority's trustworthy systems on a day to day basis. Authorized to perform system backup and recovery. Has access to Subjects' certificates; revokes Subjects' certificates; provides continuity of backup copies and archives of database and system logs creation; manages databases; has access to confidential information about Subjects/ Subscribers but is not allowed to physically access any other system resources; transfers archive copies and current backup copies outside certSIGN seat.
- **Registration Officers**: Responsible for verifying information that is necessary for certificate issuance and approval of certification requests;
- **Revocation Officers:** Responsible for operating certificate status changes;
- **Validation specialist**: enforcing rigorous control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an SSL EV . One Validation Specialist MAY review and verify all the Applicant information and a second Validation Specialist MAY approve issuance of the SSL EV .
- **System Auditor** – Authorized to access archives and audit logs of the Certification Authority's trustworthy systems. Responsible for performance of internal audit, compliance of a Certification Authority with this CPS; this responsibility extends also on Registration Authority, operating within CERTSIGN.

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

Employee are formally appointed to Trusted roles by senior management responsible for security requiring the principle of "least privilege" when accessing or when configuring access privileges and are accepted by the management and the person to fulfil the role.

5.2.2 Number of persons required per task

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

For tasks related to critical CA functions such as but not limited to key management and in particular CA key generation, more than two persons are required for extended security and control reasons. Certificate issuance by the ROOT CA G2 is under at least dual control by authorized, trusted personnel such that one person cannot sign subordinate certificates on his/her own.

5.2.3 Identification and authentication for each role

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

- Placement on the list of persons allowed to access CERTSIGN locations,
- Placement on the list of persons allowed to physically access system and network resources of CERTSIGN,
- Issuance of confirmation authorizing to perform the assigned role,
- Assignation of an account and a password in CERTSIGN information system.
- Every assigned account:
- Has to be unique and directly assigned to a specific person,
- Cannot be shared with any other person,
- Has to be restricted according to function (arising from the role performed by a specific person) based on the CERTSIGN software system, of operating system and application controls.

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

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

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

5.2.4 Roles requiring separation of duties

CERTSIGN implements and enforces a separation of roles and duties for the roles of Administrator, Operator, and Auditor to ensure that the same person cannot hold multiple roles. All those roles have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. These include skills and experience requirements.

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

5.3 Personnel control

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

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

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

5.3.1 Qualifications, experience and clearance requirements

CERTSIGN ensures that all employees acting for the provision of certSIGN's certification services are checked prior to employment regarding qualifications, expert knowledge, experiences and clearance needed and as appropriate to fill trusted roles and to perform the related specific job function. Managerial personnel possess expertise and training in PKI technology and experience in information security management and risk management sufficient to carry out management functions.

5.3.2 Background check procedures

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

5.3.3 Training requirements

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

- Requirements of Certification Practice Statement,
- Requirements of Certification Policy,
- Procedures and security controls employed by a Certification Authority and a Registration Authority
- Common threats to the information verification process (including phishing and other social engineering tactics), and CA/B Forum Baseline Requirements
- Responsibilities arising from roles and tasks performed in the system,

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

The CA ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. CA documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to

perform that task. CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the CPS and the CA/B Forum Baseline Requirements.

5.3.4 Re Training frequency and requirements

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

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

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

5.3.8 Documentation supplied to personnel

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

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

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

5.4 Audit logging procedures

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

Whenever possible the logs are created automatically. If this is not possible logs on paper will be used. Each record in a log be it automatically created or by hand is preserved and disclosed during an audit, if required. The time accuracy of logs is ensured by three time servers. Two

of them use as a reference time source GPS satellites and one is synchronized with the system that provides the official time of Romania.

5.4.1 Types of Recorded Events

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

- **System entries** – contain information about customer's requests and server's responses (or vice versa) at the level of the network protocol (for example http, https); the data to record are: IP address of the station or server, performed operations (for example: searching, editing, writing etc.) and their results (for example the successful entry of a record in the database),
- **Errors** – contain information about errors at the network protocols level and at the applications' modules level;
- **Audit** – contain information specific for the certification services, for example: registration and certification request, rekey request, certificate acceptance, certificate issuing and CRL etc.

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

Every automatic or manual recording contains the following information:

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

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

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

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

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

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

All registration information including the following is recorded:

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

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

- Changes to the security policy
- Start and stop of systems;
- Outages;
- System crashes and hardware failures
- Firewall and router activities
- PKI system access attempts
- Physical access of personnel and other persons to sensitive parts of any secure site or area;
- Back-up and restore;
- Report of disaster recovery tests;
- Audit inspections;
- Upgrades and changes to systems, software and infrastructure;

Security intrusions and attempts at intrusion. Access to logs is exclusively allowed for the security officer, the administrators of the Certification Authorities and auditors

The privacy of subject information is maintained.

5.4.2 Frequency of Processing Log

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

5.4.3 Retention period for audit log

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

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

5.4.4 Protection of audit log

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

- Only the above entities have the right to read the journal's records,
- Only the security officer can archive or delete files (after their archiving) that contain recorded events,
- It is possible to identify any integrity violation; this thing insures that the records do not contain gaps or forgeries,
- No entity has the right to modify the content of a log.

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

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

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

5.4.7 Notification to event-causing subject

Not applicable.

5.4.8 Vulnerability assessments

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

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

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

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

5.5 Records archiving

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

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

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

Backup copies are created and retained outside CERTSIGN location.

5.5.1 Types of data archived

The following data are subjected to a trustworthy archive:

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

5.5.1.1 Certificate Issuance

All certificate issuance records (copies of certificates are held, regardless of their status as expired or revoked) are retained as records in electronic and/or in paper-based archives for the period detailed below in Section 5.5.2. CERTSIGN may require Applicants to submit appropriate documentation in support of a certificate application. In such circumstances, CERTSIGN retains such records as stated in this CPS.

CERTSIGN records the following information related to certificate issuance as part of its certificate approval checklist process:

- the subscriber's PKCS#10 CSR;
- Documentation of organizational existence for organizational applicants as listed in Section 3.2.2;
- Documentation of individual identity for individual applicants as listed in Section 3.2.3;
- Verification of organizational existence and status received from third party databases and government entities (including screen shots of web sites reporting such information);
- Mailing address validation (if different than those identified through the resources listed above);
- Letter of authorization for web sites managed by third party agents of Applicants (if applicable);
- Submission of the certificate application, including acceptance of the Subscriber Agreement;
- Name, e-mail, and IP address of person acknowledging authority of the Applicant/Subscriber collected pursuant to Section 3.2.5;
- Screen shot of web site;

- Other relevant contact information for the Applicant/Subscriber; and
- Copy of Digital Certificates issued.

5.5.1.2 Certificate Revocation

Requests for certificate revocation are recorded and archived, including the name of the person requesting revocation, the reason for the request and the CERTSIGN personnel involved in authorizing revocation. This information and all resulting CRLs are retained as records in electronic archives for the period detailed in Section 5.5.2 below.

5.5.1.3 Other Information

CERTSIGN also archives the following information concerning its CA operations:

- Versions of this CPS
- Contractual obligations
- Records of CA System equipment configuration and CA Private Key access and usage
- Security and compliance audit data (see Section 5.4); and
- Any other data or applications necessary to verify the contents of the archive.

5.5.2 Archive retention period

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

5.5.3 Protection of archive

CERTSIGN ensures:

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

Archives are accessible only to the authorized personnel.

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

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

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

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

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

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

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

5.5.6 Archive collection system (internal or external)

CERTSIGN archive collection systems are internal.

5.5.7 Procedures to obtain and verify archive information

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

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

5.6 Key Changeover

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

5.7 Compromise and Disaster Recovery

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

5.7.1 Incident and compromise handling procedures

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

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

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

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

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

5.7.2 Computing resources, software and/or data are corrupted

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

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

To prevent or limit results of the above threats:

- The Security Policy of CERTSIGN includes a Business continuity and Disaster Recovery Plan,
- In the case of corruption restraining certSIGN functionality, within 48 hours an emergency facility will be activated, which should substitute all significant function of a Certification Authority until the primary facility is restored to service. The distance between the primary and the emergency facilities is enough to avoid that the potential disasters occurring at the primary site could also affect the emergency site.
- Installation of updated software version in production is possible only after carrying out intensive tests on a testing environment, performed in strict accordance with disclosed procedures. Every modification in the system requires CERTSIGN security administrator's acceptance.
- CERTSIGN systems use application creating backup copy from data, allowing system recovery at any moment and performance of an audit. Backup copies include all the relevant data from security point of view.

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

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

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

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

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

5.7.3 Certification Authority private key compromise procedures

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

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

- Notification of the compromise to all Subjects/ subscribers and other entities with which certSIGN has agreements or other form of established relations, among which relying parties and other trust services providers. In addition, this information will be made available to other relying parties by means of mass media system and electronic mail
- Notification of the public through several channels, including a message on the certSIGN's CA repository and web site, a press release in media
- A certificate corresponding to the compromised key is placed on Certificate Revocation List
- All the certificates signed by the corrupted CA are revoked and a suitable reason for revocation is submitted
- The Certification Authority generates a new key pair and a new certificate
- New certificates for Subject are generated
- The new certificates for Subjects are submitted to them without charging any fees.

5.7.4 Business continuity capabilities after a disaster

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

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

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

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

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

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

5.8 Certification Authority or RA termination

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

5.8.1 Requirements associated to duty transition

Before a Certification Authority ceases its activity, it shall:

- Inform (at least 30 days in advance) the following about the decision to terminate its services: all Subjects/ Subscribers who hold active (unexpired and unrevoked) certificates issued by this authority and other entities with which the certSIGN has agreements or other form of established relations, among which relying parties, other trust service providers and relevant authorities such as supervisory bodies. In addition, this information will be made available to other relying parties;
- Handling of the revocation status for unexpired certificates that have been issued.
- Transfer its obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the certification and timestamping services for a reasonable period, unless it can be demonstrated that we do not hold any such information; The information refers to registration information, revocation status for unexpired certificates that have been issued. and event log archives for their respective period of time as indicated to the Subjects/ Subscriber and relying party
- CA private keys, including backup copies, will be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved;
- Where possible arrangements should be made to transfer provision of certification services for the existing customers to another certification service provider

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

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

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

5.8.2 Certificate issuance by the successor of terminated Certification Authority

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

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

The archive of the Certification Authority ceasing its service has to be turned over to the primary Certification Authority – certSIGN ROOT CA (in the case of termination of services of certSIGN SSL EV CA Class 3 G2).

6 Technical information security controls

6.1 Key pair generation and installation

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

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

certSIGN SSL EV CA Class 3 G2 owns at least one certificate signed by certSIGN ROOT CA. The private key corresponding to the public key contained in the certificate is used exclusively to sign the public keys of the Subjects and the Certificate Revocation List necessary for the functioning of the CA.

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

6.1.1 Key pair generation

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

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

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

The CA:

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

The keys of CertSIGN SSL EV CA Class 3 G2 are undertaken in a physically secured environment by personnel in trusted roles under, at least, dual control :

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

- at least one independent and external auditor

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

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

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

CA-generated subject keys are generated using an algorithm recognized as being fit for the uses, during the validity time of the certificate. CA key pair generation is performed using the RSA algorithm with a 4096 bits key length.

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

The Subjects' keys are generated by the Subject, by means of software applications or cryptographic devices. The CA rejects a certificate request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key.

6.1.2 Private Key Delivery to subscriber

Not applicable...

6.1.3 Public key delivery to the Certification Authority

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

6.1.4 Certification Authority public key delivery to Relying Parties

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

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

CA publishes its certificates by placing them in the publicly available repository of CERTSIGN: http://www.certsign.ro/repository.

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

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

6.1.5 Key sizes

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

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

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

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

6.1.6 Public Keys parameters generation and parameter quality checking

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

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

Allowed key usage purposes are described in KeyUsage field (see Chapter 7.1.1.) of standard extension of a certificate complying with X.509 v3. This field has to be obligatorily verified by the Subjects' application managing the certificates.

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

a) digitalSignature: certificate intended for verification of electronic signature,

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

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

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

e) keyAgreement: intended for protocols of key exchange,

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

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

h) encipherOnly: may be used solely with keyAgreement bit to indicate its purpose of data encryption in key exchange protocols,

i) decipherOnly: may be used solely with keyAgreement bit to indicate its purpose of data decryption in key exchange protocols.

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

- Self-signed Certificates to represent the Root CA itself;

- Certificates for Subordinate CAs and Cross Certificates.

6.2 Private key protection and Cryptographic Module Engineering Controls

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

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

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

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

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

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

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

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

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

6.2.1 Cryptographic module standards and controls

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

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

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

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

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

Acceptance of secret shared by its holders

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

Protection of shared secret

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

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

Availability and erasure (transfer) of the shared secret

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

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

Responsibilities of shared secret holder

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

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

6.2.3 Private Key escrow

Private keys of Certification Authorities are not subject to custody.

Subject's private keys are not subject to custody.

6.2.4 Private Key backup

CA creates a backup copy of their private key. Copies are used in case of execution of standard or emergency key recovery procedure (e.g. after disaster). When outside the secure cryptographic device the CA private key is protected in a way that ensures the same level of protection as provided by the secure cryptographic device. The copies of the private keys are protected by shared secrets. CERTSIGN does not retain copies of Certification Authority operator private keys. The CA private signing key are backed up, stored and recovered only

by personnel in trusted roles using, at least, dual control in a physically secured environment. The number of personnel authorized to carry out this function is kept to a minimum and consistent with the CA's practices. Copies of the CA private signing keys are subject to the same or to a greater level of security controls as keys currently in use.

6.2.5 Private Key archival

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

6.2.6 Private Key transfer into or form a cryptographic module

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

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

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

Introducing a private key into a security hardware module of the CA requires the restoration of the key on HSM in the presence of a corresponding number of shared secret owners that protect the module containing the private keys. Due to the fact that the CA can retain an encrypted copy of its private key, the keys may also be transferred between modules.

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

6.2.7 Private key storage on cryptographic module

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

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

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

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

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

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

6.2.8 Method of activating the private key

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

6.2.9 Method of deactivating private key

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

6.2.10 Method of destroying private key

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

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

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

Every private key destruction is recorded in the event journal.

The Subject is responsible to destroy the private key.

6.2.11 Cryptographic Module Rating

See above.

6.3 Other aspects of key pair management

CERTSIGN uses appropriately the CA private signing keys and does not use them beyond the end of their life cycle.

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

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

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

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

6.3.1 Public key archival

CERTSIGN archives its own CA public keys and all the public keys certified by certSIGN SSL EV CA Class 3 G2 in the form of X509 certificate containing the key.

See chapter 5.5 for archival conditions.

6.3.2 Certificate operational periods and key pair usage periods

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

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

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

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

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

Table 6.3.2.1 Maximum usage period of CA certificates

Key owner	Certification Policy	Main key usage
Legal entities	SSL EV	1 year;

Table 6.3.2.2. Maximum usage periods of Subject's certificates

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data are used in two basic cases:

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

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

protected by such participants through applicable internal procedures made available to these participants.

Shared secrets used for Certification Authority private key protection are generated in accordance with the requirements presented in Chapter 6.2 and retained inside cryptographic cards. The cards are protected by a PIN number, created in accordance with the requirements of FIPS-112. Shared secrets become activation data after their activation, i.e. providing the correct PIN number protecting the card. certSIGN ensures that activation data associated to CAs private keys and operations are securely generated, managed, stored and archived as described in the relevant sub-section of sections 6.1 and 6.2. The installation and recovery of the CA's key pairs in a secure cryptographic device shall require simultaneous control of at least two employees in trusted roles.

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

6.4.2 Activation data protection

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

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

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

6.4.3 Other aspects of activation data

Not applicable

6.5 Computer security controls

This chapter describes CERTSIGN’s computer security controls.

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

6.5.1 Specific computer security technical requirements

Technical requirements, presented in this Chapter, apply to single computer security control and installed software control, used for certSIGN. Security means protecting computer systems are executed on the level of operating system, application and physical protections.

Computers located in Certification Authorities and in their associated components (e.g. Registration Authority) are equipped with the following security means:

- Mandatory authenticated registration on the level of operating system and applications,
- Discretionary access control,
- Possibility of conducting security audit,

- The computer is accessible only to authorized personnel, performing trusted roles in certSIGN,
- Enforcement of duty segregation, arising from the role performed in the system,
- Identification and authentication of roles and personnel performing these roles,
- Prevention of re-usage of an object by another processes after the object release by an authorized process,
- Cryptographic protection of information exchange and protection of databases,
- Archive of history of operation carried out on the computer and data required by audits,
- A secure path allowing credible identification and authentication of roles and personnel performing these roles,
- Key restoration methods (only in the case of hardware security modules) and application and operating system,
- Monitoring and alerting means in the case of unauthorized compute resource access.

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

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

Media management procedures are implemented to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

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

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

6.5.2 Computer security rating

CERTSIGN computer system complies with requirements described in ETSI Standards: ETSI EN 319 411-1 and CEN CWA 14167 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures).

6.6 Life cycle security controls

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

6.6.1 System development controls

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

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

Similar rules apply to hardware components replacement, as follows:

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

6.6.2 Security management controls

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

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

6.6.3 Life cycle security controls

Change control policies and procedures are applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies CERTSIGN's security policy.

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

CERTSIGN implement internal security procedures for ensuring that:

- Security patches are applied within a reasonable time after they come available;
- Security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh
- The benefits of applying them;
- The reasons for not applying any security patches are documented

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

6.7 Network security controls

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

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

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

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

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

e) Communication between distinct trustworthy systems are only established through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.
f) If a high level of availability of external access to a specific certification service is required, the external network connection is redundant to ensure availability of the services in case of a single failure.
g) a regular vulnerability scan on public and private IP addresses identified by certSIGN is performed and evidence is recorded that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.
h) certSIGN certification services undergo a penetration test on the related systems at set up and after infrastructure or application upgrades or modifications that certSIGN determines are significant. Evidence is recorded that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

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

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

Means of protection of the network security accept only messages submitted with the usage of http, https, NTP, POP3 and SMTP protocols. Events (logs) are recorded in the system journals and allow supervision of correctness of the usage of services provided by CERTSIGN. Local network components (e.g. routers) shall be kept in a physically and logically secure environment and their configurations shall be periodically checked for compliance with the requirements specified by CERTSIGN.

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

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

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

The Root CA system is in a high security zone.

6.8 Time-stamping

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

6.9 Cryptographic modules specific controls

Cryptographic modules controls include requirements enforced on development, production and delivery of the modules. CERTSIGN does not define proprietary requirements in this area. However, CERTSIGN accepts and uses only cryptographic modules complying with the requirements in Chapter 6.2.

7 Certificate, CRL and OCSP profile

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

7.1 Certificate profile

Profile of basic fields for certSIGN SSL EV CA Class 3 G2 certificate in described in Table 7.1.

Field name	Value or value's constraint	
Version	3	
Serial Number	2006051670031857926 01acb75e127	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Department (OU)=	certSIGN ROOT CA
	Organization (O) =	CERTSIGN
	Country (C) =	RO
Not before (validity period beginning date)	Jan 30 09:46:55 2018 GMT	
Not after (validity period end date)	Jan 30 09:46:55 2028 GMT	
Subject (Distinguished Name)	Common Name (CN)	certSIGN SSL EV CA Class 3 G2
	Organisation Unit (OU) =	certSIGN SSL EV CA Class 3 G2
	Organization (O) =	certSIGN
	Country (C) =	RO
Subject Public Key Info	2048 bits RSA key	
Signature	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	

Table 7.1. Profile of the basic fields for certSIGN SSL EV CA Class 3 G2

Profile of basic fields for certificates issued by certSIGN SSL EV CA Class 3 G2 is described in Table 7.2.

Field name	Value or value's constraint
Version	Version 3
Serial Number	Unique value greater than zero (0) for all certificate issued by Certification Authorities within CERTSIGN. It contains a random value of 8 bytes. A hardware cryptographic module is

Field name	Value or value's constraint	
	used for generating this value.	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Common Name (CN) =	certSIGN SSL EV CA Class 3 G2
	Organisational Unit =	certSIGN SSL EV CA Class 3 G2
	Organization (O) =	certSIGN
	Country (C) =	RO
Not before (validity period beginning date)	Universal Time Coordinated based.	
Not after (validity period end date)	Universal Time Coordinated based.	
Subject (Distinguished Name)	Encoded in accordance with RFC 5280, may contain fields presented in Chapter 7.1.4.	
Subject Public Key Info	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key).	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.	

Table 7.2. Profile of the basic fields of certificates issued by certSIGN SSL EV CA Class 3 G2

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

Certificate extensions for certSIGN SSL EV CA Class 3 G2 are described in Table 7.3.

Extension	Value or Value constraint	Extension status
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro	Non-critical

Extension	Value or Value constraint	Extension status
	[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/root.crt	
Basic Constraints	Subject type=CA, Path length constraint=0	Critical
Key Usage	keyCertSign (bit 5), cRLSign (bit 6)	Critical
Authority Key Identifier	e0 8c 9b db 25 49 b3 f1 7c 86 d6 b2 42 87 0b d0 6b a0 d9 e4	Non-critical
Subject Key Identifier	36 3b a2 9e 25 87 2a 0f fd 9a 4a 3c 27 da cb a7 79 c3 0c 7f	Non-critical
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier= 1.3.6.1.4.1.25017.1.1.6 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution Points	http://crl.certsign.ro/root.crl	Non-critical

Table 7.3. Extensions of certSIGN SSL EV CA Class 3 G2 certificate

SSL EV certificate contains extensions described in Table 7.4.

Extension	Value or Value constraint	Extension status
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro	Non-critical

	[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/root.crt	
Key Usage	digitalSignature (bit 0), Key Encipherment (bit 2)	Critical
Authority Key Identifier	36 3b a2 9e 25 87 2a 0f fd 9a 4a 3c 27 da cb a7 79 c3 0c 7f	Non-critical
Subject Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	Non-critical
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.1.1.6.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2]Certificate Policy: Policy Identifier=2.23.140.1.2.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution Points	http://crl.certsign.ro/certsign-sslev.crl	Non-critical
Subject Alternative Name	This extension MUST contain one or more host Domain Name(s) owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for	Non-critical

	SSL EV.	
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Non-critical

Table 7.4. Qualified SSL certificate extensions

OCSP certificate contains extensions described in Table 7.5.

Extension	Value or Value constraint	Extension status
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.certsign.ro/certcrl/certsign-sslev.crt	Non-critical
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1)	Critical
Authority Key Identifier	36 3b a2 9e 25 87 2a 0f fd 9a 4a 3c 27 da cb a7 79 c3 0c 7f	Non-critical
Subject Key Identifier	3c 76 7c 4a 3c 2d 6c 5a 82 c0 2d 62 f9 2e 17 89 e5 55 f0 b6	Non-critical
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=1.1.3.6.1.4.1.25017.1.1.6.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution	http://crl.certsign.ro/certsign-sslev.crl	Non-

Points		critical
Subject Alternative Name	Other Name: Principal Name=office@certsign.ro RFC822 Name=office@certsign.ro	Non-critical
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	Non-critical
OCSPNoCheck	-	Non-critical

Table 7.5. OCSP certificate extensions

7.1.3 Algorithm object identifiers

The field of signatureAlgorithm contains a cryptographic algorithm identifier used for electronic signature created by a Certification Authority on the certificate. In the case of CERTSIGN, algorithm used is sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

7.1.4 Name forms

The contents of the fields must meet the requirements in section 3.1 and the current CAB Forum EV Guidelines.

7.1.5 Name constraints

Not applicable.

7.1.6 Certificate policy object identifier

Certificates policy object identifiers used at certSIGN SSL EV CA Class 3 G2 level are described in Table 7.6 and Table 7.7.

Certification Policy Name	Policy identifier
certSIGN SSL EV CA Class 3 G2	{certSIGN} .{id-policy}(3). {id-cp}(1).{id-EV-CA}(4) . *subpolicy ID=1.3.6.1.4.1.25017.1.1.6. subpolicy ID* See below table for *subpolicyID* values. *{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines (1) }(2.23.140.1.1)*

Table 7.6.Policies identifiers and their names

CA Level	OID
certSIGN SSL EV CA Class 3 G2 1.3.6.1.4.1.25017.1.1.6	*SSL EV certificate .1* *OCSP certificate .2*

Table 7.7 Certificate policy object identifiers

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

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

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL profile

CRL profile is described in Table 7.8.

Field name	Value or value's constraint	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer	Common Name (CN)	certSIGN SSL EV CA Class 3 G2
	Organisational Unit (OU)=	certSIGN SSL EV CA Class 3 G2
	Organization (O) =	certSIGN
	Country (C) =	RO
ThisUpdate	Date of CRL issuance	
NextUpdate	Date of next expected CRL update	
Revoked Certificates	List of revoked certificates	

Table 7.8 CRL profile for certSIGN SSL EV CA Class 3 G2

7.2.1 Version numbers (s)

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

7.2.2 CRL and CRL entry extensions

CRL extensions for certSIGN SSL EV CA Class 3 G2 are described in Table 7.9.

Extension	Value or Value constraint	Extension status

Authority Key Identifier	36 3b a2 9e 25 87 2a 0f fd 9a 4a 3c 27 da cb a7 79 c3 0c 7f	Non-critical
CRL Number	monotonically increasing sequence number	Non-critical

Table 7.9. CRL extensions for certSIGN SSL EV CA Class 3 G2

7.3 OCSP profile

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

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

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

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

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

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

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

- GOOD – indicates the valid status of certificate

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

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

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

7.3.1 Version numbers (s)

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

7.3.2 OCSP extensions

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

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

8 Compliance Audit and Other Assessments

In respect to the conformity audits and the competence, consistent operation and impartiality of conformity of assessment bodies assessing and certifying CA conformity as certification services provider and the conformity of CA services towards the criteria from Regulation 910/2014 and its implementing acts and CA/B Forum Baseline Requirements, CA/B Forum EV Guidelines we follow the requirements from standard ETSI EN 319 403.

8.1 Frequency or circumstances of assessment

CERTSIGN activities supporting the delivery of the services presented by this CPS are audited at least every 12 months.

The audit verifies the compliance with the present CPS and ETSI 319401,ETSI 319411, CA/B Forum Baseline Requirements, CA/B Forum EV Guidelines technical standards.

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

8.2 Identity/qualifications of assessor

The assessment will be performed by an independent external auditor in compliance with WebTrust EV Program for CAs criteria.

8.3 Assessor's relationship to assessed entity

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

8.4 Topics covered by assessment

The planned audits cover, but are not limited to, all aspects of CERTSIGN operations and services specified in by CPS Web CA.

8.5 Actions taken as a result of deficiency

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

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

8.6 Communication of results

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

The Audit Report will states explicitly that it covers the relevant systems and processes used in the issuance of all certificates that assert the policy identifiers listed in Section 7.1.6.1. The CA makes the Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, the CA provides an explanatory letter signed by the Qualified Auditor.

8.7 Self-audits

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

9 Other Business and Legal Matters

9.1 Fees

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

Services provided by CERTSIGN are set as follows:

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

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

9.1.1 Digital certificate issuance and renewal fees

Prices are set according to the internal price policy.

9.1.2 Certificate access fees

Free service.

9.1.3 Revocation or Status Information Access Fees

Prices are set according to the internal price policy.

9.1.4 Other fees

Prices are set according to the internal price policy.

9.1.5 Fees refund

Refund policy is defined within the internal price policy.

9.2 Financial Responsibility

9.2.1 Insurance coverage

CERTSIGN complies with the mandatory requirements from Section 8.4.Insurance from CA/B Forum EV Guidelines.

9.2.2 Other assets

Not applicable.

9.2.3 Insurance or warranty coverage for end-entities

CERTSIGN complies with the mandatory requirements from Section 8.4.Insurance from CA/B Forum EV Guidelines.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

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

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

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

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

or

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

or

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

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

Types of Information Considered Confidential and Private

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

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

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

The confidentiality obligation does not apply to CERTSIGN for providing certification services to a third party. Persons responsible for keeping the confidentiality of information and who obey the rules regarding information management bear the liability according to laws in force.

Disclosure of Certificate Revocation Reason

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

Disclosure of Non-Public Information to Law Enforcement Officials

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

9.3.2 Information not within the scope of confidential information

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

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

9.3.3 Responsibility to protect confidential information

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

9.4 Privacy of personal information

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

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

9.4.1 Privacy Plan

- In the provision of certification services, certSIGN acts as a personal data controller according to paragraph 7 of art. 4 of the Regulation no. 679/2016.
- Security measures required by the Romanian National Supervisory Authority for Personal Data Processing are implemented to guarantee that:
- Appropriate technical and organizational measures are taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Access to CERTSIGN services concerns only the processing of those identification data which are adequate, relevant and not excessive to grant access to the respective service.
- Confidentiality protection and registration data integrity: when exchanged with the subscriber/subject, when exchanged between CERTSIGN system components as well as when stored.

9.4.2 Information Treated as Private

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

9.4.3 Information Treated as Private

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

9.4.4 Responsibility to Protect Private Information

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

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

9.4.5 Notice and Consent to use Private Information

In the process of issuing a digital certificate Subjects / Beneficiaries are informed about the need to use their personal data for the service and the need for consent. The lack of consent entails the impossibility of providing the service.

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

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

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

9.4.7 Other Information Disclosure Circumstances

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

- disclosure of personal information to:

- auditors in the audits to which certSIGN is subject according to the provisions of Regulation (EU) no. 910/2014 under confidentiality;
- a third party who relies on the certification services provided by certSIGN in relation to which the Subject uses the certificate
- the courier companies with which certSIGN has a contract, with the agreement of the Subject / Beneficiary, if he has opted to transmit the certificate to his / her home

address or to another communicated address, respecting the same obligations regarding the security of personal data that he / has and certSIGN;

- an empowered person to whom I outsource certain services;
- affiliated companies certSIGN

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

9.5 Intellectual Property Rights

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

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

9.6 Representations and warranties

9.6.1 CA representations and warranties

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

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

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

The Certificate Warranties specifically include the those specified in the CA/B Forum Baseline Requirements, paragraph 9.6.1. and in CA/B Forum EV Guidelines paragraph 7.1.

9.6.2 RA representations and warranties

The RA has the obligation to comply scrupulously with the CPS, with the relevant section of the applicable CP, and with the CERTSIGN relevant internal procedures.

9.6.3 Subject representations and warranties

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

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

CA Terms and Conditions contains provisions imposing on the Subject itself the obligations and warranties specified in the CA/B Forum Baseline Requirements, paragraph 9.6.3.

9.6.4 Relying Party representations and warranties

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

- the successful performance of public key operations as a prerequisite for relying on a CERTSIGN Certificate
- the validation of a CERTSIGN Certificate by using the (CRLs) or certificate validation services provided by CERTSIGN
- the immediate termination of any reliance on a CERTSIGN Certificate if it has been revoked or when it has expired

9.6.5 Representations and warranties of other participants

No stipulation

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

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

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

9.9 Indemnities

CERTSIGN assumes no financial responsibility for improperly used Certificates, CRLs and related services specified in this CPS.

CERTSIGN acts as specified in paragraph "9.9.1 Indemnification by CAs" from CA/B Forum Baseline Requirements and in paragraph 18. Liability and Indemnification fromCA/B Forum EV Guidelines.

9.10 Term and termination

9.10.1Term

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

9.10.2Termination

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

9.10.3Effect of termination and survival

The conditions and effect resulting from termination of this CPS will be communicated via the CERTSIGN web site upon termination. That communication will outline the provisions that may survive termination of this CPS and remain in force. The responsibilities for protecting confidential information and private personal information shall survive termination, and the

terms and conditions for all existing Certificates shall remain valid for the remainder of the validity periods of such Certificates.

9.11 Individual notices and communications with participants

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

9.12 Amendments

9.12.1 Procedure for amendment

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

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

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

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

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

9.12.2 Notification mechanism and period

All changes to the present CPS under consideration by the PPMB shall be disseminated to interested parties for a period of minimum 10 days. The date of issuance and the effective date are indicated on the title page of the present CPS. The effective date will be at least 2 days later than the date of publication.

9.12.3 Circumstances under which OID must be changed

Not applicable.

9.13 Dispute Resolution Procedures

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

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement
No stipulation.

9.16.2 Assignment
No stipulation.

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

9.16.4 Enforcement
No stipulation.

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

9.17 Other Provisions
No stipulation.