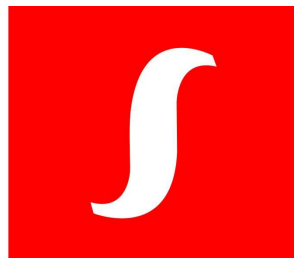


Certification Practice Statement



certSIGN®

Version 1.3

Date: February, 2009

Document History

Versiune	Data	Motiv	Persoana care a facut modificarea
1.0	April 2006	First version publishing	Electronic Services Manager
1.1	July 2006	1 year term for reviewing the classification	Electronic Services Manager
1.2	August 2008	The function responsible for administering the CPS and his contact data	Electronic Services Manager
		Detaills about protecting and backup of customers encryption private keys	Electronic Services Manager
		certSIGN position regarding the use of trademarks in the digital certificates issued	Electronic Services Manager
		For the moment certSIGN does not use external Ras	Electronic Services Manager
		certSIGN does not provide certificate suspension services	Electronic Services Manager
		The error messages in response to OCSP validation requests are not digitally signed	Electronic Services Manager
		certSIGN does not implement tokens/smartcards lifecycle management processes	Electronic Services Manager
		More details provided about the disaster recovery site	Electronic Services Manager
		certSIGN does not provide subscriber key management services	Electronic Services Manager
		certSIGN does not provide certificate rekey services	Electronic Services Manager
1.3	February 2009	Description of the process at RA to verify the owner of the domain for ssl certificates.	Electronic Services Manager
		Description of the process at RA to verify that the email account associated with the email address in the cert is owned by the subscriber	Electronic Services Manager

This document was created and is owned by:

Proprietar	Autor	Data crearii
Electronic Services Manager	Electronic Services Manager	27 January 2006

Distribution List

Destinatar	Data distribuirii
Public-Internet	13 February 2009

This document was approved by:

Versiune	Nume	Data
1.0	Policies and Procedures Management Body	April 2006

1.1	Policies and Procedures Management Body	July 2006
1.2	Policies and Procedures Management Body	August 2008
1.3	Policies and Procedures Management Body	February 2009

Content

- 1 Introduction..... 9
 - 1.1 Certification Process Overview 9
 - 1.2 CPS Identification 12
 - 1.3 CPS Parties..... 12
 - 1.3.1 Certification Authorities 13
 - 1.3.2 Registration Authority 15
 - 1.3.3 Repository 16
 - 1.3.4 End users 16
 - 1.4 Certificate Applicability Area..... 17
 - 1.4.1 Recommended Applicability Area 18
 - 1.4.2 Prohibited applications 19
 - 1.5 Contact address 20
- 2 General provisions..... 21
 - 2.1 Obligations 22
 - 2.1.1 certSIGN’s Obligations..... 22
 - 2.1.2 Registration Authority Obligations..... 24
 - 2.1.3 Subscriber Obligations 26
 - 2.1.4 Relying Parties Obligations..... 28
 - 2.1.5 Repository Obligations 30
 - 2.2 Liability 31
 - 2.2.1 Certification Authority Liability 31
 - 2.2.2 Registration Authority Liability 33
 - 2.2.3 Subscriber Liability 33
 - 2.2.4 Relying Parties Liability..... 33
 - 2.2.5 Repository Liability 34
 - 2.3 Financial Liability 34
 - 2.4 Applicable Law. Period. Applicability. Other resolutions..... 34
 - 2.4.1 Applicable Law..... 34
 - 2.4.2 Enforcement. Period 34
 - 2.4.3 Applicability..... 35
 - 2.4.4 Clause Independence 35
 - 2.4.5 Referrals 36
 - 2.4.6 Notifications 36
 - 2.4.7 Litigations Resolution 36
 - 2.5 Services fees. Payment..... 37
 - 2.5.1 Digital certificate issuance and renewal fees..... 38
 - 2.5.2 Certificate access fees 38
 - 2.5.3 Revocation or Status Information Access Fees 38
 - 2.5.4 Other fees..... 39
 - 2.5.5 Fees refund..... 39
 - 2.6 Repository and information publication 39

2.6.1	Information published by certSIGN.....	39
2.6.2	Frequency of publication.....	40
2.6.3	Access to Information Published by certSIGN.....	41
2.7	Audit	41
2.7.1	Audit Frequency	42
2.7.2	Identity / Qualifications of Auditor	42
2.7.3	Auditor’s Relation with the Audited Party	42
2.7.4	Topics Covered by Audit.....	42
2.7.5	Actions Taken as a Result of Deficiency	43
2.8	Information Confidentiality and Privacy	43
2.8.1	Types of Information Considered Confidential and Private.....	44
2.8.2	Types of Information Not Considered Confidential and Private.....	45
2.8.3	Disclosure of Certificate Revocation Reason	46
2.8.4	Disclosure of Non-Public Information to Law Enforcement Officials	46
2.8.5	Release of Confidential Information upon Owner’s Request	46
2.8.6	Other Circumstances of Information Release	46
2.9	Intellectual Property Rights.....	46
3	Identification and authentication	48
3.1	Initial Registration	48
3.1.1	Types of Names	49
3.1.2	Need for Names to be Meaningful.....	50
3.1.3	Rules for Interpreting Various Name Forms	51
3.1.4	Names Uniqueness.....	51
3.1.5	Name Claim Dispute Resolution Procedure	52
3.1.6	Prove of Private Key Possession.....	52
3.1.7	Authentication of Legal Entity’s Identity.....	53
3.1.8	Authentication of Natural Entity’s Identity.....	56
3.1.9	Devices Origin Authentication	57
3.1.10	Authorizations’ Authentication	58
3.1.11	Trade marks.....	59
3.2	Subscriber’s Identity Authentication in Certificate Renewal or Modification.....	60
3.2.1	Certificate Renewal	60
3.2.2	Certificate Modification	61
3.3	Subscriber’s Identity Authentication in Certificate Revocation.....	61
4	Operational Requirements.....	63
4.1	Application Submission	63
4.1.1	Registration request.....	64
4.1.2	Certificate Renewal, Rekey or Modification Request	65
4.1.3	Certificate Revocation Request.....	65
4.2	Request Processing	66
4.2.1	Request Processing in Registration Authority.....	67
4.2.2	Request Processing in the Certification Authority.....	67
4.3	Certificate Issuance	67
4.3.1	Certificate Issuance Awaiting	68
4.3.2	Certificate Issuance Rejection	69

4.4	Certificate Acceptance	70
4.5	Certificate and Key Usage	70
4.6	Recertification	71
4.7	Key Certification and Certificate Rekey.....	71
4.8	Rekey	72
4.9	Certificate Modification	72
4.10	Certificate Revocation	74
4.10.1	Circumstances for certificate revocation	74
4.10.2	Who can request certificate revocation.....	76
4.10.3	Procedure for certificate revocation.....	77
4.10.4	Certificate Revocation Maximum Period	78
4.10.5	CRL issuance frequency.....	79
4.10.6	Certificate Revocation List Checking	80
4.10.7	On-line Certificate Status Verification.....	80
4.10.8	Revocation of CA certificate	81
4.10.9	Circumstances for certificates suspension.....	82
4.10.10	Who can request the suspension of a certificate	82
4.10.11	The procedure for certificates suspension.....	82
4.10.12	Limitation of the suspension period of a certificate	82
4.11	Tokens or smartcards management	82
4.12	Events recording and auditing procedures	82
4.12.1	Types of Recorded Events	83
4.12.2	Frequency of Logs Processing	84
4.12.3	Event Journals Retention Period	84
4.12.4	Protection of event journals	85
4.12.5	Procedures for logs backup.....	85
4.12.6	Notification to entities responsible for responding to events.....	85
4.12.7	Vulnerability Assessment	86
4.11	Token/Smartcard management	86
4.12	Events and Audit Procedures Recording.....	86
4.13	Backup and recovery procedure	87
4.14	Records archival	88
4.14.1	Types of data archived	88
4.14.2	Frequency of data archive.....	89
4.14.3	Archive retention period	89
4.14.4	Requirements for time stamping of the records	90
4.14.5	Access procedures and archived information verification	90
4.14.6	Responsible entities notification for events treatment.....	90
4.15	Key Change over of a Certification Authority	91
4.16	Key Security Violation and Disaster Recovery.....	92
4.16.1	IT&C systems applications and data security violation.....	92
4.16.2	Key compromise or suspicion of Certification Authority private key compromise	93
4.16.3	Security coherence after disaster	93
4.17	Certification Authority termination or service transition	94

4.17.1	Requirements associated to duty transition.....	94
4.17.2	Certificate issuance by the successor of terminated Certification Authority.....	95
5	Physical, Organizational and Personnel Security Controls.....	96
5.1	Physical Security Controls	96
5.1.1	certSIGN physical security controls.....	96
5.1.2	Physical security controls within the Registration Authority.....	99
5.1.3	Subscriber's physical security.....	100
5.2	Organizational security control.....	100
5.2.1	Trusted roles.....	100
5.2.2	Number of persons required per task.....	103
5.2.3	Identification and authentication for each role.....	103
5.3	Personnel control	104
5.3.1	Personal background, qualifications and required confidentiality clauses	105
5.3.2	Personnel training requirements	105
5.3.3	Training frequency	106
5.3.4	Job rotation	106
5.3.5	Sanctions for unauthorized actions	106
5.3.6	Contract personnel.....	106
5.3.7	Documentation supplied to personnel	106
6	Technical information security controls.....	107
6.1	Key pair generation and usage.....	107
6.1.1	Key pair generation	108
6.1.2	Private Key Delivery to Entities	112
6.1.3	Public key delivery to the Certification Authority.....	112
6.1.4	Certification Authority public key delivery to Relying Parties	112
6.1.5	Key sizes	113
6.1.6	Public Keys parameters generation and parameter quality checking.....	113
6.1.7	Hardware and/or software key generation	114
6.1.8	Key usage.....	114
6.2	Private key protection	115
6.2.1	Standards for cryptographic modules.....	115
6.2.2	Private key dual access control	116
6.2.3	Private Key custody	118
6.2.4	Private Key backup	119
6.2.5	Private Key archival	119
6.2.6	Private Key entry into cryptographic module	119
6.2.7	Method of activating the private key.....	120
6.2.8	Method of deactivating private key.....	121
6.2.9	Method of destroying the private key	122
6.3	Other aspects of key pair management.....	122
6.3.1	Public key archival	122
6.3.2	Usage period of public and private keys	123
6.4	Activation data	125
6.4.1	Activation data generation and installation.....	125
6.4.2	Activation data protection	125

6.4.3	Other aspects of activation data	126
6.5	Computer security controls.....	126
6.5.1	Specific computer security technical requirements	126
6.5.2	Computer security rating	127
6.6	Technical controls specific for life cycle.....	127
6.6.1	System development specific controls	127
6.6.2	Security management controls	128
6.7	Network security controls.....	128
6.8	Cryptographic modules specific controls.....	128
7	Certificate, CRL and OCSP profile	130
7.1	Certificate profile	130
7.1.1	Contents of the certificate	130
7.1.2	Certificate extensions.....	139
7.1.3	Electronic signature algorithm identifier	143
7.1.4	Electronic signature field.....	143
7.2	CRL profile	143
7.2.1	Supported CRL entry extension.....	144
7.2.2	Revoked certificate and CRL.....	145
7.3	OCSP confirmation response profile	145
7.3.1	Version number	146
7.3.2	Certificate status information	146
7.3.3	Supported standard extensions	146
8	CPS Management	147
8.1	CPS changes procedure	147
8.2	Publication and notification procedures.....	148
8.3	CPS Approval Procedures	148

1 Introduction

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

The CPS describes four certification policies applied by certSIGN to issue the certificates for authorities and end users. These policies represent four different levels of credibility (**Class 1, Class 2, Class 3, and Class 4**) corresponding to public key certificates. The applicability ranges of certificates issued in compliance with these policies might be the same. However, the responsibilities (also from legal point of view) of the Certification Authority and of the certificate users are different. The structure and content of the CPS are in compliance with RFC 3647 recommendations. The CPS assumes that the reader is familiar with the notions regarding the certificates, electronic signature and Public Key Infrastructure (PKI).

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

1.1 Certification Process Overview

The CPS is the ground for **certSIGN** and **Certification Authority, Registration Authority and associated Relying Partys'** functioning. As well, this document describes the general rules of

certification services delivery such as Subscriber's registration, public key certification, key and certificates renewal and certificate revocation.

The Public Key Infrastructure (PKI) architecture of **certSIGN** is divided into two levels (see Figure 1.1). Level 1 contains the **certSIGN ROOT CA**. The Certification Authorities on Level 2 are directly signed by **certSIGN ROOT CA**. **certSIGN ROOT CA** operates only off-line. In case of compromising of **certSIGN CA 2, 3, or 4**, **certSIGN ROOT CA** will be used to revoke their certificates and to issue new certificates.

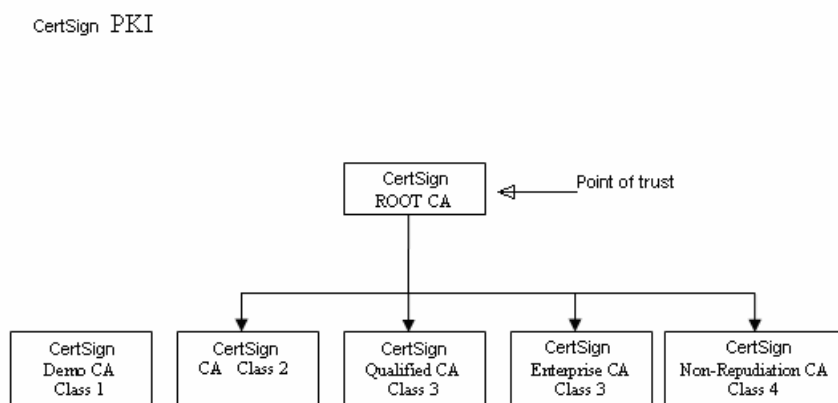


Figure 1.1. The certificates issuing Certificates operate inside certSIGN

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

- certSIGN CA Class 2
- certSIGN Qualified CA Class 3
- certSIGN Enterprise CA Class 3
- certSIGN Non-Repudiation CA Class 4

all issuing certificates with different levels of credibility.

certSIGN Demo CA Class 1 is a selfsigned authority which issue only demo certificates.

For the time being, certSIGN does not have a mutual agreement with another certificate issuing authority. If this situation will change the users will be informed by publishing the new version of the Certification Policy (CP) and of the Certification Practice Statement (CPS).

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

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

Class	Type	Subtype
Class 1 (Demo)	Simple demonstrative certificate	
	Code signing demonstrative certificate	
	Web servers demonstrative certificate	
	VPN gateways demonstrative certificate	
	CA servers demonstrative certificate	
	TSA server demonstrative certificate	
	Validation servers (OCSP) demonstrative certificate	
Class 2	Simple certificate	Simple certificate for authentication and signing <ul style="list-style-type: none"> ▪ without SS-CD and key generated by the Subscriber ▪ with SS-CD and key generated by the Subscriber ▪ with SS-CD and key generated by certSIGN
		Simple certificate for encryption <ul style="list-style-type: none"> ▪ without SS-CD and key generated by the Subscriber ▪ with SS-CD and key generated by the Subscriber ▪ with SS-CD and key generated by certSIGN
Qualified CA Class 3	Qualified certificate	Qualified certificate <ul style="list-style-type: none"> ▪ with SS-CD and key generated by the Subscriber ▪ with SS-CD and key generated by certSIGN
Enterprise CA Class 3	Trusted encryption certificate	Trust encryption certificate <ul style="list-style-type: none"> ▪ with SS-CD and key generated by the Subscriber ▪ with SS-CD and key generated by certSIGN
	Code signing certificate	
	Web servers certificate	

	VPN gateways certificate	
Class 4	CA servers certificate	
	TSA server certificate	
	Validation servers (OCSP) certificate	

Table 1.1. Types of certificates

1.2 CPS Identification

The name of this document is: the CPS of certSIGN. The document is available:

- Electronic version at the Repository on address <http://www.certsign.ro/Repository> or on request sent to office@certsign.ro;
- Printed version on request sent to certSIGN (see Chapter 1.5).

1.3 CPS Parties

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

- Certification Authorities:
 - CERTSIGN ROOT CA,
 - CERTSIGN Demo CA Class 1,
 - CERTSIGN CA Class 2,
 - CERTSIGN Qualified CA Class 3,
 - CERTSIGN Enterprise CA Class 3,
 - CERTSIGN Non-Repudiation CA Class 4,
- Registration Authority,
- The Repository,
- Online certificate status protocol (OCSP)
- Subscribers,
- Relying Parties.

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

1.3.1 Certification Authorities

The Certification Authority **CERTSIGN ROOT CA** is a Primary Certification Authority for the CERTSIGN domain. All the other Certification Authorities in this domain are subordinated to the CERTSIGN ROOT CA (see Figure 1.3).

- Currently, there are four Certification Authorities subordinated to the certSIGN ROOT CA: **CERTSIGN CA Class 2, CERTSIGN Qualified CA Class 3, CERTSIGN Enterprise CA Class 3, CERTSIGN Non-Repudiation CA Class 4** and CERTSIGN Demo CA Class 1, a selfsigned one.

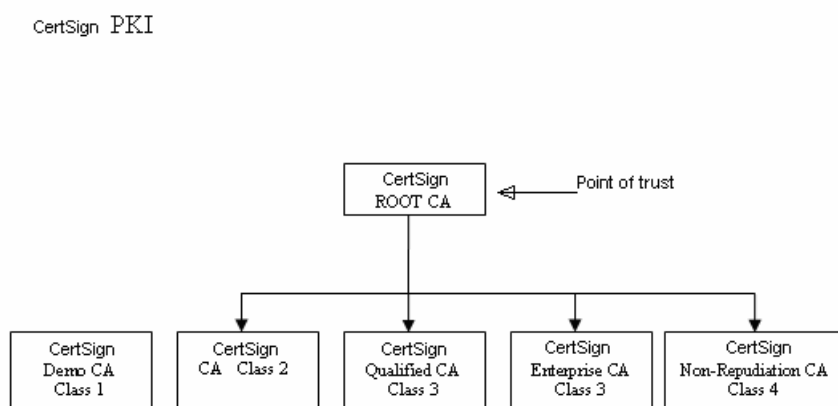


Figure 1.3. Structure of certification domain certSIGN

The Primary Certification Authority, **CERTSIGN ROOT CA**, can register and issue certificates only to Certification Authorities and authorities that issue electronic confirmations of non-repudiation that belong to the CERTSIGN domain. Before beginning the activity, every subordinate Certification Authority must send a request to the Primary Certification Authority,

CERTSIGN ROOT CA for registration and public key certificate issuance (see also the procedures described in chapter 6.1 of the *present CPS*). **CERTSIGN ROOT CA** authority operates based on a *self signed* certificate issued by itself. In such a certificate the **certificatePolicies** extension is missing (see Chapter 7.1.1), which means that there are no limitations for the set of **certification paths** to which certSIGN ROOT CA certificate can be attached.

CERTSIGN ROOT CA Certification Authority is a **point of trust** for certSIGN's customers. Thus, every certification path must start with the certSIGN ROOT CA authority's certificate.

CERTSIGN ROOT CA Certification Authority renders certification services to:

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

The subordinate certification authorities **CERTSIGN Demo CA Class 1**, **CERTSIGN CA Class 2**, **CERTSIGN Qualified CA Class 3**, **CERTSIGN Enterprise CA Class 3** and **CERTSIGN Non-Repudiation CA Class 4** issue certificates to Subscribers in compliance with the policies with the identifiers from Table 1.3.

Certification Authority	Certification Policy
CERTSIGN Demo CA Class 1	{CERTSIGN}* id-policy(1) id-cp(1)id-Class-1(1)
CERTSIGN CA Class 2	{CERTSIGN} id-policy(1) id-cp(1)id-Class-2(2)
CERTSIGN Qualified CA Class 3	{CERTSIGN} id-policy(1) id-cp(1)id-Class-3(3) si itu-t(0).identified-organization(4).etsi(0).qualified-certificate- policies(1456).policy-identifiers(1). qcp-public-with-sscd (1)
CERTSIGN Enterprise CA Class 3	{CERTSIGN} id-policy(1) id-cp(1)id-Class-3(3)
CERTSIGN Non-Repudiation CA Class 4	{CERTSIGN} id-policy(1) id-cp(1)id-Class-4(4)

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

Subordinate Certification Authorities are configured to issue certificates to:

* {certSIGN}=1.3.6.1.4.1.25017= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). certSIGN's IANNA assigned number (25017)

- users who wish to insure the electronic mail or other services' security and credibility (such as, electronic commerce, software and information libraries) by means of certificates,
- entities that provide non-repudiation services (time stamp authority),
- suppliers of services connected with mobile telecommunications,
- network devices providing encrypted connections over VPN,
- hardware devices owned by private or legal entities to provide services based on public key certificates such as on-line certificate status verification (OCSP),
- other Certification Authorities.

1.3.2 Registration Authority

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

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

Registration Authority functions on the basis of the authorization obtained from a Certification Authority corresponding to the CERTSIGN domain and can operate only within CERTSIGN. Now, external Registration Authorities are not allowed.

1.3.3 Repository

See 2.6 Repository and data publishing

1.3.4 End users

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

Subscribers

Any natural or legal entities, as well as hardware devices owned by them can be Subscribers of certSIGN – CA, provided that they fulfill the terms of the Subscriber's definition (see Chapter 1.3.4). In particular, the Registration Authority's operators, CERTSIGN's employees and indispensable equipments to insure the quality of CERTSIGN's security (firewalls, routers, and authentication servers) represent as well the Subscribers.

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

certSIGN issues different types of certificates and of different credibility levels. Subscribers must decide what type of certificate is the most suitable for their needs (see Chapter 1.4).

Relying Partys

A Relying Party, using certSIGN's services, can be any entity that takes decisions based on the correctness of the connection between a Subscriber's identity and the public key (connection confirmed by one of the Certification Authorities subordinated to CERTSIGN ROOT CA).

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

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

1.4 Certificate Applicability Area

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

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

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

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

		compromising are very high and where the consequences of a security incident are very serious. These certificates might be used to protect transactions of unlimited value (unless it is stated differently in a certificate) and transactions with high level of fraud occurrence.
--	--	---

Table 1.4. Sensitivity level of information and policy name

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

1.4.1 Recommended Applicability Area

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

1. **certificates for Certification Authorities** – their usage is not restricted to a definite area; the applicability area might result from the extension in the certificate that settles how the private key may be used (see the field **keyUsage**, Chapter 7), or its role (for example, Subscriber, Certification Authority or other authority that provides PKI services); this type also contains operational certificates of the Certification Authorities;
2. **certificates for server authentication confirmation** – are used by services that operate based on SSL/TLS/WTLS protocols;
3. **simple certificates for signing and authentication** – allow to sign emails and files or to authenticate a subscriber (for example by SSL protocol);
4. **qualified certificates** – allow documents' signing with legal value;
5. **certificates confirming certificate status** – they are issued for servers that function in compliance with OCSP protocol and provide information regarding the certificates' status;
6. **certificates for Time Stamp Authorities** – are issued to servers which, as a response to a Subscriber's request, issue time stamps binding some data (documents, messages,

electronic signatures etc.) to a moment of time based on which it can be determined the data sequence in time;

7. **encrypting certificates** – used to insure the security of e-mails, files and folders;
8. **certificates to secure the code** – used by programmers to protect the software against forgery.

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

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

The list of recommended applications (by CERTSIGN) is published on site at address: <http://www.certsign.ro/>.

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

1.4.2 Prohibited applications

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

1.5 Contact address

Address: 133 Șerban Vodă Ave., C1, 2nd floor, Poste Code 040205

E-mail: office@certsign.ro

Telephone: 00 40 311 99 04

Fax: 00 40 311 99 05

2 General provisions

This chapter describes the obligations / warranties and liabilities of the Certification Services Provider certSIGN, Registration Authority, Subscribers and certificates users (Relying Parties). The obligations and liabilities are governed by mutual agreements between the above mentioned parties (see Figure. 2).

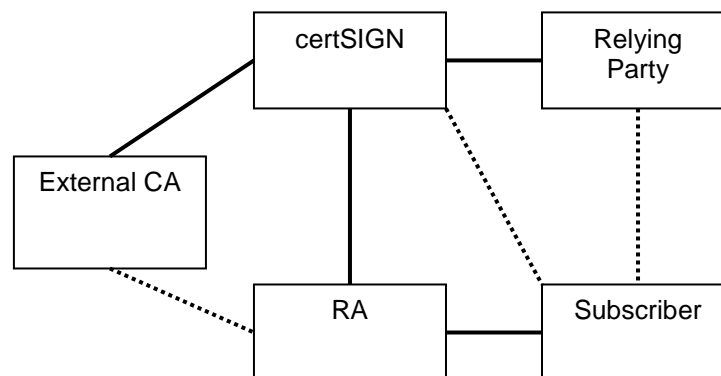


Figure 2 Agreement between parties

Contracts concluded by CERTSIGN with Relying Parties and Subscribers describe types of services provided by CERTSIGN, their mutual obligations and liabilities.

Between CERTSIGN and local authorities there are concluded contracts when these parties play the role of a Certification Authority's agent that operates within CERTSIGN's domain. Based on such an agreement a Registration Authority may conclude contracts of certification service providing with Subscribers on behalf of CERTSIGN. In well-founded cases the Registration Authorities may conclude contracts on their own behalf with Subscribers for services provided by the Registration Authorities.

certSIGN Certification Authority can register and issue a certificate to any external entity that plays the role of subordinate Certification Authority, provided that the registration and issuance of the certificate are based on an agreement concluded between the two parties.

The CPS and the Certification Policy are part of the contracts concluded between CERTSIGN and Subscribers, Relying Parties or other entities that provide services of public key infrastructure, such as time stamp, certificate status verification etc.

Contracts concluded between a Relying Party and a Subscriber will dully follow the provisions of the CPS hereby, its provisions prevailing in case of doubt or noncompliance.

2.1 Obligations

2.1.1 certSIGN's Obligations

certSIGN ensures that:

- Its commercial activity is based on reliable devices and trusted software applications,
- Its activity and services are in compliance with legal provisions, they do not violate author's rights nor the third parties' rights,
- Its services are in compliance with broadly accepted terms:
 - Certification services – in compliance with X.509, PKCS#10, PKCS#7, PKCS#12,
 - Time stamp services – in compliance with RFC 3161 standard,
 - Certificate status verification (OCSP) – in compliance with RFC 2560 standard.
- Follows and enforces the procedures described in the present CPS particularly concerning:
 - Checking the information regarding the identity of the Subscriber to whom it is issued a certificate belonging to the CERTSIGN domain; procedures of verifying the Subscriber's identity depend on the information included in a certificate and vary according to certification fees, nature and Subscriber's identity and certificate applicability area (see Chapters 3 and 4),
 - Certificates which are revoked in case of existing supposition or certainty that the certificate contents data that are not up to date or the private key corresponding to the certificate was compromised (revealed, lost etc.),
 - Informing a subscriber and other interested entities in case the Subscriber is the subject of a certificate issued, revoked or suspended,

- Publication of the lists of revoked or suspended certificates in places stated in the present CPS,
 - Generating and using private keys only for purposes stated in the present CPS; protecting the keys thus to not allow their use for any other purpose except that accepted,
 - Personalization and issuance of cryptographic devices, *on which there are stored the certificates and the key pair* (when the key is generated by a Certification Authority),
 - Publication of necessary information for the correct receiving, management and certificate revocation,
- Issued certificates do not contain false information neither known or coming from the persons who approve the certificate issuing request or those who issue certificates
 - Issued certificates do not contain any mistake resulting from negligence or procedure violation by the persons who approve the certificate issuing requests or those who issue certificates,
 - Subscriber's distinguished names that appear in certificates are unique for CERTSIGN domain,
 - Ensures protection for personal data in compliance with Law no. 677/2001 regarding personal data protection and with Law no. 506/2004 concerning the processing of personal data and the protection of privacy in the electronic communications sector;
 - If a key pair is generated with the Subscriber's authorization the key pair is delivered confidentially to the Subscriber and immediately afterwards it is deleted from the delivery support, excepting the case when the Subscriber requests to archive the key pair.

CERTSIGN commits itself to:

- Register and issue certificates only for the Certification Authorities whose certification policy and CPS were approved by CERTSIGN; CERTSIGN may request that at least one of

the four certification policies (mentioned in Table 1.3 and Chapter 7.1.1.2) should be applied by the registered Certification Authority,

- Concludes contracts with Subscribers, Relying Parties (if applicable), and Certification Authorities; the certification services are provided only based on contracts and only following the request of a Subscriber, Relying Parties, Certification Authority,
- To create and administrate a list of software applications and devices recommended for use in order to generate asymmetrical key pairs,
- To create and administrate a list of recommended applications that fulfill the requirements in Chapter 1.4.1,
- To carry out scheduled audits within Certification Authorities and Registration Authority that belong or are connected to certSIGN domain;
- To request some independent auditors to realize assessments for CERTSIGN domain, to make them available the necessary documents and information and to follow the auditor's recommendations.

2.1.2 Registration Authority Obligations

Registration Authority operating within CERTSIGN domain ensures that:

- Its commercial activity is based in reliable devices and software applications recommended by CERTSIGN,
- Its activity and services are in compliance with the law and do not violate neither the copyrights nor the third parties' rights,
- The subscriber's identification data filled in CERTSIGN's database correspond to those made available by the Subscriber and these information will be updated immediately they are aware of the modifications done,
- The information concerning the Subscriber validated and later sent to the Certification Authority to be included in the certificate, is precise,

- Does not contribute intentionally or unintentionally to the appearance of mistakes or inaccuracy regarding information contained in the certificate,
- The rendered services are in compliance with broadly accepted terms (de jure and de facto): X.509, PKCS#10, PKCS#7, PKCS#12,
- The rendered services are provided based on procedures compliant with the recommendations of the present CPS; particularly concerning:
 - procedures of Subscriber's identity verification,
 - procedure for demonstrating a private key's possession associated with the public key for which the certification is requested,
 - procedures of reception, processing and confirmation or rejection of client's requests for issuing, renewal,
 - procedures of sending requests to Certification Authorities based on a request accepted by a Subscriber for issuing, renewal, revocation;
 - procedures of archive of requests and information received from Subscribers, decisions taken and information sent to the Certification Authorities,
 - procedures of generating keys for Subscribers, provided that the agreement concluded with the Certification Authority and the Subscriber allows this; the keys cannot be stored by the Registration Authority unless the agreement concluded with the Subscriber states this very thing,
- it submits to scheduled internal and external audits, mainly to those carried out by certSIGN's personnel or those approved by it.

Besides those mentioned above, the Registration Authority commits itself to:

- submit CERTSIGN's recommendations, mainly those resulting from audits,
- secure the personal data protection in compliance with Law no. 677/2001 regarding personal data protection and with Law no. 506/2004 the processing of personal data and the protection of privacy in the electronic communications sector;

- protect operators' private keys in compliance with security requests mentioned in the CPS,
- not use operators' private keys for other purposes except those stated in the present CPS, unless it is approved by CERTSIGN,
- obtain from trusted sources and thoroughly verify the active public keys, certificates and CRLs of the Certification Authorities belonging to CERTSIGN.

2.1.3 Subscriber Obligations

The CPS and the Certification Policy are part of every contract concluded between a Subscriber and certSIGN. By applying for registration to Registration Authority and signing the registration confirmation the Subscriber agrees to enter the certification system on the conditions stated in the documents mentioned above.

Depending on the relations between CERTSIGN and a subscriber and on the credibility level of the certificate requested by a subscriber the obligations may be formulated as a contract between the subscriber and CERTSIGN.

According to the contract the end Subscriber commits itself to:

- Agree the terms of the contract;
- Approve every certificate issued for him / her; CERTSIGN's warranties and obligations related to a certain type of certificate are valid from the moment the certificate is approved by the Subscriber,
- Take all necessary precautions allowing to correspondingly generate (by himself, the Registration Authority or the Certification Authority) and to safely store the private key from a key pair (to prevent from loss, compromising, modification or unauthorized use);
- To use devices and software applications recommended by CERTSIGN in case the Subscribers generate themselves the keys;
- State true data in the applications sent to Registration Authority or to a Certification Authority and then stored in CERTSIGN's database and in issued public key certificates; a

Subscriber must be aware of the responsibilities for direct or indirect damages caused as following data forgery;

- Accept that every electronic signature created by means of a private key belonging to the Subscriber or associated to an approved certificate that contains the corresponding private key represents the Subscriber's signature and to acknowledge that the certificate was not invalid (beyond the expiry date) nor revoked or suspended when the signature was created;
- Get to know in general the notions concerning certificates, electronic signatures and PKI.

The end Subscriber also commits himself to:

- Comply with the rules of the present CPS and the Certification Policy,
- Generate cryptographic keys, manage the passwords, the public and private keys, to exchange information with the Registration Authority and Certification Authorities only via software applications recommended by CERTSIGN; the access to this software, the environments and devices on which there are stored the keys and passwords must be properly controlled,
- Regard the loss or revealing of the password (revealing of the password by an unauthorized person) as a loss or revealing of the private key (its revealing by an unauthorized person),
- Do not allow the access to its private keys to unauthorized persons,
- Do not use as end Subscriber a private key specially associated to a certificate issued by certSIGN, for signing CRLs or certificates,
- Make prove of possession of the private key to the Registration Authority or Certification Authority or to demonstrate its possession in other way,
- Do not reveal passwords to an unauthorized person,

- Send the Registration Authority the requested documents to confirm the information included in the application sent and the identity of the person who sent the request or of the entity that actions on behalf of the Subscriber,
- In case of security violation (or of suspicion of security violation) of private keys notify the certificate issuer,
- Use the public key certificates and the corresponding private keys only for the purposes stated and in compliance with applicability areas and prohibitions settled by the CPS
- Obtain the public key certificates of the Certification Authorities and Registration Authority as well as those corresponding to other services provided by CERTSIGN.

2.1.4 Relying Parties Obligations

The CPS and the Certification Policy are part of every contract concluded between certSIGN, a Relying Party and / or a Subscriber. The object of such a contract might be:

- Providing Repository services, time stamp services and certificate status verification services (OCSP) – in case of concluding contracts with CERTSIGN;
- Specifying the conditions that must be fulfilled by an electronic signature in order to be considered valid by a Relying Party – in case on concluding a contract with a Subscriber;

Depending on the relations between a Relying Party and CERTSIGN or a subscriber and on the levels of the certificates accepted by a Relying Party, the obligations of the Relying Parties are settled within a contract concluded between CERTSIGN and a Relying Party.

By contract, a Relying Party commits itself to:

- Agree and follow the terms and conditions of the contract. The rights and obligations of the parties come into force when the contract is concluded.
- Thoroughly verify every electronic signature from a certificate or document received. To check the signature the Relying Party must:

- specify the certification path that contains every certificate of the Certification Authorities that make possible the verification of the signature from the signer's certificate,
- make sure that the chosen certification path is the best for creating the signature; in some cases it is possible to exist more than a path starting from a given certificate (by means of which the signature was created) and to a Certification Authority on which the signature verification is based.
- Make sure that none of the certificates from the certification path, belonging to certSIGN, is not on the revoked or suspended certificate lists;
- Check if all the certificates from the certification path belong to a Certification Authority and these are authorized to sign other certificates,
- (optionally) specify the date and time when a document or a message was signed. This thing is possible only if the document or message was time stamped (before its signing) with a time stamp issued by a Time Stamp Authority, or a time stamp was associated with an electronic signature just after the document's signing; such a verification allows the implementation of non-repudiation services or can be used to solve disputes,
- verify, using a defined certification path, the credibility of the signer's certificate, document or message and the authenticity of the signature,
- carry out accurately the cryptographic operations using software applications and devices with a security level corresponding to the sensitivity level of certificates processed and the credibility level of the used certificates,
- consider an electronic signature as being invalid if by means of applied software and devices is not possible to determine if the electronic signature is valid or if the verification result is negative,
- electronic signature verification aims at stating whether: (1) an electronic signature was created by means of a private key corresponding to a public key from a certificate issued

by certSIGN for a Subscriber and (2) the message (document) signed was not modified after signing.

- Trust only those certificates of public keys that:
 - Are used in compliance with the stated purpose and correspond to the applicability areas mentioned by the Relying Party, for example, by a signature policy (see Chapter 1.4),
 - Whose status was verified based on corresponding Certificate Revocation Lists or by means of certSIGN's OCSP service
- Specify the conditions that must be fulfilled by a public key certificate and an electronic signature in order to be considered valid; these conditions may be formulated, for example, as a certification policy accepted and then published.

Every document with a defective or questionable electronic signature should be rejected or subjected to other procedures that might allow determining its validity. Any person that approves such a document bears the responsibility for consequences resulting from this fact.

The Relying Party must be aware of the provisions of the CPS and Certification Policy (warranties and obligations).

2.1.5 Repository Obligations

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 Subscribers' registered in certificates, and Subscribers have given their written consent regarding these certificates in compliance with the requests mentioned in Chapters 2.1.3. and 4.3,
- Ensure that the certificates of the Certification Authorities, Registration Authority belonging to CERTSIGN domain as well as the Subscriber's certificates (after their approval) 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, Subscribers 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.

2.2 Liability

Liability of parties delivering or using services in the domain managed by CERTSIGN is settled by contracts mutually concluded. Parties' liability results from violating the terms and conditions specified in the contracts concluded and in other documents related to these contracts. In exceptional cases, if the contract states so, a part of legal liability of a party may be taken or delegated to other party. Such a situation occurs when a Certification Authority delegates the responsibility of verifying the Subscribers' identity to Registration Authority. The Registration Authority is responsible for its obligations specified in Chapter 2.1.2.

*From legal point of view certSIGN is responsible for the consequences of actions taken by the Certification Authorities **CERTSIGN Demo CA Class 1, CERTSIGN CA Class 2, CERTSIGN Qualified CA Class 3, CERTSIGN Enterprise CA Class 3 and CERTSIGN Non-Repudiation CA Class 4, Registration Authority, Repository and in case contracts state so, other Certification Authorities..***

The legal liability does not eliminate nor does a substitute the responsibility that results from the contracts conclude between parties or law regulations.

2.2.1 Certification Authority Liability

Certification Authorities belonging to CERTSIGN bear legal liability in case the direct or indirect damages caused to Subscribers or Relying Parties:

- Occur despite their obeying the terms and conditions settled in the Certification Policy and in the CPS,
- Occur due to CERTSIGN's errors as well as: discrepancies between the process of identity verification and stated procedures, improper protection of the Certification Authorities' private keys, impossibility of accessing the provided services (for example, CRLs), unless it is not demonstrated the CERTSIGN's guilt.
- Occur following violations of certSIGN's obligations, mentioned in Chapters 2.1.1, only in case CERTSIGN's guilt is proved.

The Subscriber states and is the only liable for the following:

- The data and documents provided to a Registration Authority are true and precise,
- By accepting a certificate accepts the fact that the certificate does not contain mistakes resulting from negligence or procedure violation from persons that process the certificate requests or those who issue certificates.

CERTSIGN will not conclude any contract with those Subscribers who do not accept these statements, in case it is aware of any of the above mentioned cases.

CERTSIGN does not assume any responsibility for the Relying Parties' actions, Subscribers or other parties that are not associated with CERTSIGN. CERTSIGN is not liable for:

- Damages caused by force majeure and / or fortuitous. Force majeure is defined as the unforeseeable and unavoidable event that takes place after the contract concluding, such as: fire, earthquake, any other natural disaster, as well as war. The relatively unpredictable and invincible event without any extraordinary character, such as: strikes, legal restrictions, other such events represent the fortuitous;
- Damages caused by installing and using applications or devices used to generate and manage cryptographic keys, encryption, creating of electronic signature that do not fulfill conditions specified in paragraph 1.4.1,
- Damages caused by improper usage of certificates issued („improper“ represents the usage of a revoked or suspended certificate or used not in compliance with its stated purpose, stated in the present CPS),

- Situation when a certificate was not approved by a Subscriber and this thing was confirmed by the respective Subscriber, the Subscriber bears the liability,
- Storage of false data in CERTSIGN's databases and their including in digital certificates issued to the Subscriber in case the Subscriber stated that these are false.

2.2.2 Registration Authority Liability

Liabilities of the Registration Authority are automatically taken by certSIGN as resulting from the liabilities stated in Chapters 2.1.1, 2.1.2, 2.1.5. The conditions in which these responsibilities are taken are settled by the contracts concluded by certSIGN with Subscribers and Relying Parties (if applicable).

In case the Registration Authority does not make the necessary verifications when a Subscriber stated those mentioned in Chapter 2.2.1, the full legal responsibility resulting from the violation of the obligations described in Chapter 2.1.2 belongs to the Registration Authority.

2.2.3 Subscriber Liability

The legal liability of the Subscribers results from obligations and warranties mentioned in Chapter 2.1.3. The liability conditions are stated in the contract concluded by the subscriber with certSIGN.

2.2.4 Relying Parties Liability

The legal liability of the Relying Parties results from the rights and obligations stated in Chapter 2.1.4. The liability conditions are stated in the contract concluded by the Relying Parties with certSIGN, or with a Subscriber.

The provisions of the contracts concluded by Relying Parties with Subscribers and certSIGN require that the Relying Party confirm that they have enough information to make a decision regarding the acceptance or rejection of an electronic signature while verifying it.

In contracts concluded the parties must specify the value of the financial accepted transactions only based on information included in a digital certificate and to submit a statement to confirm

that they are aware of the legal consequences that result from not following the obligations described in the present CPS.

2.2.5 Repository Liability

Liability for Repository service and its service consequences belong to certSIGN (see Chapter 2.2.1).

2.3 Financial Liability

certSIGN will cover the damages it might cause due to certification services for persons that build their moral on the legal effects of the qualified certificates up to the equivalent in lei of the amount of 10.000 euro for every risk insured. The insured risk represents every damages caused even if there are more such damages following the provider's no fulfilling of the liabilities mentioned by law.

2.4 Applicable Law. Period. Applicability. Other resolutions

2.4.1 Applicable Law

The present CPS is governed by the Romanian law. All activities developed based on this document will follow the provisions stated in normative documents in force in Romania concerning certification services.

certSIGN liabilities results from obligations assumed based on the present CPS.

2.4.2 Enforcement. Period

2.4.2.1 Enforcement. Period. Clause Modification

Provisions of the present CPS come into force on the notification date to the Regulation and Supervision Authority and are available until a new version is published.

Modifications made to the present CPS or the including of new provisions are done in compliance with procedures presented in Chapter 8.

2.4.2.2 Exceptions from the availability period

If the agreements concluded based on the present CPS contain confidentiality clauses regarding the content, clauses concerning the confidentiality of information owned by parties, clauses regarding the following of copyrights, these clauses are considered in force after the expiry of the availability period of the parties' agreement, too, for a period that will be defined when the respective agreement will be settled and following the legal provisions in force.

2.4.3 Applicability

The provisions of the present CPS are applicable to parties as they are mentioned in chapter 2.1 and to Subscribers that conclude contracts according to the provisions of the present CPS.

2.4.4 Clause Independence

In case one of the provisions of the present CPS or of the contracts concluded on its ground is considered by a legal court or by any other qualified authority as being null or inapplicable, the respective provision will be considered eliminated from the present CPS or contracts that were concluded on its ground, and the other provisions of the CPS or of the contracts concluded will remain valid and applicable and will be applied per se.

2.4.5 Referrals

The present CPS and contracts concluded on its ground may contain references to other provisions on condition that:

- This thing should be mentioned as a clause within the Code or in contract
- The respective provisions that are referred to in the Code or in contracts should be in written.

2.4.6 Notifications

The parties mentioned in the present CPS may define, based on agreements, the mutual notification methods. If these methods are not defined the present Code allows the information exchange using electronic mail, fax, telephone, network protocols (TCP/IP, HTTP) etc.

The communication means may be chosen depending on the exchanged information type. For example, almost all services provided by certSIGN require the usage of one or more network protocols allowed. Certain information and notifications must be delivered in compliance with a defined schedule. This thing is applied mainly to CRLs' publishing, to the new certificates belonging to the Registration Authority and Certification Authorities and to inform Subscribers or Relying Parties (if specified in contracts) about this, as well as notification concerning the endangering of the private key of any Certification Authority operated by certSIGN.

Any communication between parties concerning the fulfilling of the present contract must be submitted in written. Any document written must be registered both at the sending moment and when receiving it. Communications between parties can be done also by phone, telegram, telex, fax, or email, on the condition of a written confirmation for its receiving.

2.4.7 Litigations Resolution

The parties of a contract will try to find a friendly solution for the possible litigations occurred.

In case the parties dispute over a non fulfilled obligation that was previously assumed, the parties will try to solve it by direct conciliation. In case of direct conciliation each party will use a defending method admitted by the law in force to support the points of view.

Any dispute regarding the coming in force, interpretation, execution and termination of the present CPS and not friendly solved will be referred to law courts of common right to be solved by qualified authorities according to the Romanian legal provisions in force.

The governing language of the present CPS is Romanian language and the document will be interpreted according to the Romanian laws.

2.5 Services fees. Payment

The certification services fees and the types of services for which there are charged fees are published in the list of fees published on the address <http://www.certsign.ro>.

Services provided by certSIGN are settled as it follows:

- **Individual certification services** – the price is settled for every service in part, for example, for every certificate sold or a smaller number of certificates,
- **Certification services packages** – the price is settled for packages of services rendered to a single entity,
- **Subscription services** – the price is settled 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 stamp and certificate status verification services by means of OCSP protocols,
- **Indirect services** – the price is settled 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, than certSIGN will charge a fee for every certificate issued by the respective Certification Authority.

Payments will be done cash, by payment order, and also bank cards along with the invoice in compliance with the legal provisions in force.

2.5.1 Digital certificate issuance and renewal fees

Taking into consideration the difference between the procedures of issuing and renewing a certificate the value of the digital certificate issuing or renewing services (see 2.5), corresponding to models previously presented can be divided in three components: (1) the value of identification and authentication services rendered by the Registration Authority (2) the value of digital certificates issuing services and (3) the value of cryptographic devices' (token) personalization and issuing. These components may be quoted apart in a list of fees used also in case of certificate renewal (the identification costs, Subscriber's authentication and those of token personalization and issuing might be omitted in case of renewal).

2.5.2 Certificate access fees

The certificate access fees in certain special conditions requested by the Relying Parties is settled according to the ways applicable to rendered services based on a subscription and to indirect services.

The value of these services is settled in the contracts concluded with Relying Parties and depends on the type of certificate issued.

2.5.3 Revocation or Status Information Access Fees

The certificate revocation services, the certificate publication in CRL, or the access to the CRL's published in the Repository (or in other locations) are free of charge.

certSIGN can settle fees for certificate status verification services by means of OCSP protocol or other systems. In this case, the prices will be calculated according to the prices settled for individual certification services or to the services rendered based on a subscription.

Without certSIGN's written consent it is forbidden that third parties providing certificate verification services should use the information from CRLs or information regarding the certificate status. The usage of this information is allowed only after signing a contract with certSIGN. In this case, the value of service will be calculated according to the indirect selling

service (for example, it is settled an amount for every confirmation issued by a third party regarding a certificate's status).

2.5.4 Other fees

certSIGN can charge fees for other services rendered (see 2.5) such as:

- Generating keys for Certification Authorities or Subscribers,
- Testing of applications and including them in the list of recommended applications,
- Selling licenses,
- Design, implementation and installation activities,
- Sale of CPS, of Certification policy, handbooks, guides etc.
- Training courses.

2.5.5 Fees refund

certSIGN makes efforts to insure the highest security level for the provided services. If a Subscriber or a Relying Party is not content of the services rendered he might request the certificate revocation and the refund of the amounts paid within 30 days from the certificate's issuing date. After this period the Subscriber is entitled to request the certificate's revocation and the refund of the amounts corresponding to the elapsed period until the certificate's expiry if certSIGN does not fulfill the obligations and liabilities assumed and mentioned in the CPS.

The refund requests must be sent on the address mentioned in Chapter 1.5.

2.6 Repository and information publication

2.6.1 Information published by certSIGN

The Repository is a public interface to the following information:

- The current and previous version of the CPS and the Certification Policy
- Templates for contracts with the Subscribers and Relying Parties,

- certSIGN's statement regarding the insuring of confidentiality of the information received and processed
- the register (as in the electronic signature law)
- the certificates certSIGN ROOT CA, certSIGN Demo CA Class 1, certSIGN CA Class 2, certSIGN Qualified CA Class3, certSIGN Enterprise CA Class 3 and certSIGN Non-Repudiation Class 4 as well as the certificates of all Certification Authorities that belong or are connected to the certSIGN domain (for example, certificates of the Certification Authorities newly registered by RA),
- end subscribers' certificates (natural and legal entities, including certSIGN's employees and machines / software applications owned by them and which are indispensable for PKI services) in compliance with the electronic signature law.

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

- The CRLs are available in the so called CRL distribution points which addresses are specified in each certificate issued by certSIGN; the main CRLs distribution point is in the Repository at the url <http://crl.certsign.ro>,
- The list of Local Registration Authorities that were certified by the Registration Authority
- Other information that change in real time,

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

2.6.2 Frequency of publication

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

- Certification Policy and CPS – see Chapter 8,
- Certificate of the Certification Authorities – after issuing a new certificate;

- Certificate of the Registration Authority – after issuing a new certificate;
- Subscribers' certificates – after every issue of a new certificate;
- Certificate Revocation List – see Chapter 4.9.4;
- Audit reports performed by authorized institutions – when certSIGN receives them;
- Additional information – after every update.

2.6.3 Access to Information Published by certSIGN

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

certSIGN implemented logical and physical protection mechanisms against 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.

2.7 Audit

Audits intend to control the consistency of certSIGN's actions or of its delegated entities with their statements and procedures (including the Certification policy and the CPS).

certSIGN's audits mainly regard the data processing centers and the key management procedures. As well, these audits regard the Certification Authorities belonging to the certification path of **certSIGN ROOT CA**, Registration Authority or other elements of the public key infrastructure, such as OCSP servers.

certSIGN's audits may be carried out by internal teams (internal audit) or by independent organizations (external audit). In both cases the audit is done on the request and under the supervision of the security administrator (see Chapter 5.2.1).

2.7.1 Audit Frequency

The external audit checking the compatibility with the legal and procedure regulations (particularly with the Certification Policy and the CPS) is occurring once at four years, while an internal audit occurs at least once a year.

2.7.2 Identity / Qualifications of Auditor

The external audit is carried out by an authorized Romanian institution independent from certSIGN or from any international institution with a representative or any secondary headquarters in Romania. Such an institution should:

- Hire personnel with relevant technical background and experience (have documents to certify this thing) concerning public key infrastructure, technologies and information security techniques and audit for system security.
- Be a well known organization or registered company.

The internal audit is carried out by the quality and audit department of certSIGN.

2.7.3 Auditor's Relation with the Audited Party

See 2.7.2.

2.7.4 Topics Covered by Audit

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

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

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

2.7.5 Actions Taken as a Result of Deficiency

The results of the internal and external audits are sent to certSIGN's management. Within 14 days of the results sending this must draft a written opinion concerning the noticed deficiencies and to propose an action plan and deadlines to remove the deficiencies. Information regarding the solving method will be sent to the auditor.

*In deficiencies posing a direct threat for the certification process of **certSIGN Qualified CA Class 3**, **certSIGN Enterprise CA Class 3** and **certSIGN Non-Repudiation CA Class 4** the security administrator might make a decision of temporary suspending their activities. All certSIGN's customers will be notified of the decision taken and of the estimated time of the resuming time for the authority's activity. The notification might be done by means of Repository, via e-mail and –if absolutely necessary – by press publishing.*

2.8 Information Confidentiality and Privacy

All certSIGN's information was gathered, stored and processed in compliance with applicable laws, mainly with Romanian law regarding personal data protection (Law 677/2001) and Law no. 506/2004 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Relations between a Subscriber, a Relying Party and certSIGN are based on trust.

A third party might have access only to information public available in certificates. Other data delivered in applications sent to certSIGN will not be willingly disclosed to a third party under

any circumstance (except the legal situations). certSIGN may have access to Subscriber's private keys only in the following cases:

1. generation requests and key archiving, sent by the Subscriber,
2. submission of locally generated key for archive in the database of certSIGN.

Encryption keys archive is carried out only by customer's express request. Signature keys are never archived by certSIGN.

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 information to the parties involved in fulfilling the obligations will be confidentially done and will extend only to that information necessary to fulfill the obligations.

2.8.1 Types of Information Considered Confidential and Private

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

- Information provided by Subscribers in addition to information that must be sent reevaluated to perform the certification services; in those situations disclosing the information received require a previous written consent from the owner of the information or in others conditions according to the law.
- Information supplied by/to Subscribers (for example, the content of the contracts concluded with Subscribers or Relying Parties, bank accounts, registration applications, issuing, renewal, certificate revocation – except information included in certificates or

from the Repository in compliance with the present CPS); part of the information mentioned above can be disclosed only with the approval and for the purpose specified by the owner of the information (for example the Subscriber),

- Records of system transaction (all types of transactions, as well as data for transactions' control, the so called system transactions logs)
- Record of events (logs) connected with certification services, kept by certSIGN,
- Results of internal and external audits, if they are a threat for certSIGN's security,
- Emergency plans,
- Information about steps taken to protect the 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 criminal liability according to laws in force.

2.8.2 Types of Information Not Considered Confidential and Private

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

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

The following information categories sent to the Certification Authorities and the Registration Authority are available for the public in the Repository:

- Certification Policy and CPS,
- The pricelist for services provided,

- Guides for users,
- Certificates of the Registration Authority and Certification Authorities,
- Subscriber's certificates (after obtaining their approval),
- Certificates Revocation List (CRL),
- Information concerning trainings carried out by certSIGN.

2.8.3 Disclosure of Certificate Revocation Reason

If a certificate was revoked upon the request of an authorized party (not the party whose certificate is being revoked), information about the revocation and the related reasons are disclosed to both parties.

2.8.4 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.

2.8.5 Release of Confidential Information upon Owner's Request

The present CPS does not mention any condition in this respect.

2.8.6 Other Circumstances of Information Release

The present CPS does not mention any condition in this respect.

2.9 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 previous agreement in writing of certSIGN.

Every key pair associated to a certificate issued by certSIGN is the property of the subject of the certificate, described in the field *Subject* of the certificate (see Chapter 7.1), except professional certificates, in which case the owner is a legal entity.

3 Identification and authentication

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

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

3.1 Initial Registration

Subscriber's registration is performed when a Subscriber that requests the registration does not own a valid certificate issued by any other Certification Authority affiliated to certSIGN.

The registration presupposes a number of procedures that allow a Certification Authority – before issuing a certificate to a Subscriber – to gather the valid data concerning a certain entity in order to identify it.

Every Subscriber undergoes the registration process only once. After checking the data made available by a Subscriber this is included in the list of authorized users of certSIGN's services and is granted a public key certificate.

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

- Fill in an on-line registration form or a document that may be downloaded from certSIGN's Web site,
- Generate a RSA asymmetric key pair and provide the Registration Authority the proof of owning a private key; optionally, the Subscriber may delegate a Certification Authority or the Registration Authority to generate this key pair,
- Suggest a distinctive name (ND, see Chapter 3.1.1),

- Fill in and send a registration form that contains a public key and the prove of owning its corresponding private key,
- Optionally, attend the Registration Authority and provide the required documents (if required by the certification policy based on which the certificate is issued),
- Conclude an agreement with an agent on behalf of the Registration Authority concerning the services provided by certSIGN; the present CPS is part of this agreement.

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

3.1.1 Types of Names

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

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

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

3.1.2 Need for Names to be Meaningful

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

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

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

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

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

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

3.1.3 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 ND it goes to recommendations mentioned in Chapter 3.1.2.

3.1.4 Names Uniqueness

The identification of every holder of certificates issued by certSIGN is performed based on the ND. *certSIGN ensures the uniqueness of the ND assigned to every Subscriber.*

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

If a suggested ND violates the rights of other entities to this name (see Chapter 3.1.5), certSIGN may add other attributes to the ND (for example, the serial number) that ensures the uniqueness of this name within certSIGN's domain. A Subscriber is entitled to refuse a ND suggested in the procedure mentioned in Chapter 4.4.

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

certSIGN.ro / issuer name /Subscriber name

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

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

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

3.1.5 Name Claim Dispute Resolution Procedure

Names that are not owned by a Subscriber cannot be used in his certificate requests. certSIGN does not check if a Subscriber is entitled to use the specified name in the registration request nor intends to assume the role of an arbiter resolving disputes related to owner rights over any Distinctive Name, trade mark or trade name.

In disputes related to name claims certSIGN is entitled to reject or suspend a Subscriber's request without taking any liability in this regard. certSIGN is also entitled to take decisions concerning the Subscriber's name syntax and to assign the Subscriber the name resulting as following this decision.

3.1.6 Prove of Private Key Possession

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

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

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

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

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

It is recommended that the private keys should be generated inside a cryptographic device (token) or, in case they are generated outside the token, by means of a software or hardware generator following to be imported on token. Any entity may have a token when generating and importing the key or the token may be provided to the entity after the process of key generation. In the latter case, certSIGN warrants that the token and the key will securely reach straight to the respective entity (see Chapter 6.1.2).

3.1.7 Authentication of Legal Entity's Identity

Authentication of legal entity's identity is realized to prove that when processing a request the legal entity mentioned in the request really exists; as well, it is necessary to prove that a natural person that requests a certificate from behalf of a company or that receives it is authorized by this legal entity to represent it.

The procedures of legal entity's identity authentication are initialized if the entity

- Acts as a Subscriber and charges a Certification Authority with any certification service,
- Demands the issuance of a certificate for a hardware device or for an application (software) owned by this entity,

- Acts as an entity that requests its inclusion in the list of accredited Certification Authorities subordinated to certSIGN,
- Wishes to render other certification services, such as: Time Stamp Authority, OCSP etc.

The authentication of a legal entity's identity is done either by personal attendance of the authorized representative of the legal entity to the Registration Authority, or, by personal attendance of the authorized representative of the Registration Authority at the legal entity's headquarters (mentioned in the request).

The authorized representatives of the institution regardless the certificate level they are requesting are bind to present upon the request of the Registration Authority the following documents:

- Certified copy „in compliance with the original” of the registration certificate of the company;
- Copy of utility invoice (phone, others) issued to the company;
- Documents to attest the solicitor's identity (identity card or passport) and the authorization attesting that he is representing the company;
- Purchasing request;
- Template statement of the domain's titular (in case of WEB certificates when the certificate solicitor is not the owner of the domain he wants to secure).

The procedure performed by RA of checking the legal entity's identity and its authorized representative's identity consists of (see as well Table 3.1.8):

- Checking the documents rendered by the Subscriber,
- Checking the request, that consists of:
 - Checking the compliance of the data mentioned in the request with those from the documents rendered,
 - (optional) checking the proof of private key possession (if the request supposes a key pair to create an electronic signature) and the fact that the Distinctive Name is the right one,

- Checking the authorization and identity of the representative of the legal entity that submits the request (including applications for certification as Certification Authority) on behalf of this entity.
- Checking for certificates to be used for SSL-enabled servers, that the domain referenced in the certificate is registered by the entity submitting the certificate request or by that that has authorized the usage of domain by the entity submitting the request. This is done by means of whois service provided by ROTLD at www.rotld.ro
- Verification that the email account associated with the email address in the certificate is controlled by the subscriber. The certificate request cannot be made/validated in the RA software application if the subscriber does not validate his email account.

The Registration Authority is committed to check the correctness and the authenticity of all data rendered in a request (see Table 3.1.8, Chapter 3.1.9).

If the checking is successfully concluded an authorized operator of the Registration Authority:

- Assigns a distinctive name to the legal entity or approves the name suggested by it by submitting the request,
- Issues a confirmation that certifies the compliance of the data from the processing request with the data provided and sends this confirmation to the Certification Authority,
- Copies all the documents and certificates used by the operator to check the legal entity's identity or the identity of its representative that acts in its behalf,
- On behalf of the Certification Authority concludes a contract with a legal entity concerning the rendering of certification services; the agreement is concluded if the legal entity acts as Subscriber, Certification Authority, or an entity that renders other certification services.

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

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

- The identity of the Registration Authority's operator that checks the solicitor's identity,
- Sending the operator's statement (hand signed) which attests the fact that he verified the solicitor's identity in compliance with the requests of the present CPS,
- Verification data,
- The identifier of the operator and the solicitor in case the latter is personally present at the Registration Authority (supposing that the solicitor was assigned with such an identifier),
- The solicitor's statement (hand signed) related to the correctness of the data included in the request in compliance with the requirements of the present CPS,

certSIGN rejects the registration request of a solicitor if finds out that the respective legal entity is already registered.

3.1.8 Authentication of Natural Entity's Identity

The authentication of the natural entity's identity (private entities) has two purposes. The authentication must prove (1) that the data of a request refer to an existent private entity and (2) that the solicitor is really the private entity mentioned in the request.

The authentication of natural entities is realized on the basis of:

- documents (identity card or passport) that confirms the solicitor's identity,

and if the Subscriber wishes to include the data of an institution (legal entity) for which he works:

- written authorization with the company's explicit approval of including its data in the natural entity's certificate,
- valid excerpt from the Romanian Trade Register,
- other documents.

The procedure for natural entities realized in front of the Registration Authority consist of:

- verification of the documents rendered by the Subscriber (identity card or passport in original or notarized copy), including CA's or other institutions' databases,

- checking the submitted request:
 - verification of the consistency of the data from the request with those in the documents,
 - (optional) checking the proof of private key possession and of the compliance degree of the ND.
- Verification of the information set in the request using other sources (Romanian Trade Register, National Population Registry, etc.).
- Verification that the email account associated with the email address in the certificate is controlled by the subscriber. The certificate request cannot be made/validated in the RA software application if the subscriber does not validate his email account.

The requirements for verification of a private entity's identity depend on the certificate level (Table 3.1.8)

Certification policy	Requirements The Registration Authority's operators compare the received Subscriber's data using one of the possibilities:
certSIGN Class 1	A. In case of personal demonstrative certificates:
	<ul style="list-style-type: none"> • It is checked the e-mail address by sending installation instructions for certificates to the address mentioned in the request.
	B. In case of Enterprise demo certificates or Non-repudiation demo, the Registration Authority's operators compare the data received from the Subscriber using one of the following possibilities:
	<ul style="list-style-type: none"> • Via fax (recommended option), • Via electronic mail with attached file: gif, tif, jpg, bmp (optional), with the data sent to the Registration / Certification Authority by a Subscriber
certSIGN Clasa 2	<ul style="list-style-type: none"> • Via fax (recommended option), • By letter (optional) • By personal attendance (optional), • Via electronic mail with attached file: gif, tif, jpg, bmp (optional)
	<ul style="list-style-type: none"> • By personal attendance at the Registration Authority (recommended option) • By a letter that must contain copies of all original documents confirmed by a public notary (optional) • Electronic format that must contain copies of all original documents authenticated by a public notary under the prescriptions of the electronic notary law no 589/15.12.2004 (optional)
	<ul style="list-style-type: none"> • By personal attendance at the Registration Authority (recommended option) • By a letter containing copies of original documents confirmed by a public notary (optional), • In electronic format that must contain copies of the original documents authenticated under the prescriptions of the electronic notary law no 589/15.12.2004 (optional)
	<ul style="list-style-type: none"> • By personal attendance at the Registration Authority (recommended option) • By a letter containing copies of original documents confirmed by a public notary (optional), • In electronic format that must contain copies of the original documents authenticated under the prescriptions of the electronic notary law no 589/15.12.2004 (optional)

Table 3.1.8. Requirements imposed in the process of verification of the natural/legal entity's identity

3.1.9 Devices Origin Authentication

In many cases, a public key certificate is issued for physical devices (hardware), such as a router, a firewall, or a server. In these cases it is considered that every device is the property of

a natural or legal entity (has a sponsor). The sponsor is responsible of sending the data associated to the device:

- Device identifier;
- Device public key;
- Characteristics and authorizations of the device (in case these must be mentioned in the certificate),
- Contact data of the sponsor that allow the Registration Authority or Certification Authority to rapidly contact the sponsor.

The verification of the information that is registered depends on the certificate's credibility level. There are two methods to authenticate a devices and the integrity of the data rendered:

- Verification of the request electronically signed and sent by a sponsor (the request must be signed with a private key associated with a credibility level equal or higher than the certificate requested),
- During the personal registration by a sponsor of a device; the sponsor's identity is confirmed in compliance with the requests mentioned in Chapter 3.1.8.

3.1.10 Authorizations' Authentication

The certSIGN Registration Authority and Certification Authorities can confirm the authorization of a natural entity to act on behalf of other entities, usually legal entities. Such authorizations are frequently associated with a certain role in the institution.

The authentication of authorizations is part of the procedure preformed by the Registration Authority or by the Certification Authorities to process the certificate request for a legal person or for a device belonging to a legal or natural person. In both cases, the issuing of the certificate is a confirmation of the fact that a legal entity or a device has the right to use the private key on behalf of the legal entity.

The authorization is delegated by a legal entity either to its employees or to a third party empowered by it. The authorization's authentication procedure adopted by certSIGN contains

besides the authorization's authentication also the authentication of the natural entity to which these authorizations are delegated. This request may be omitted only if the entity is already a certSIGN Subscriber. The authentication of the natural entity's identity is performed as described in Chapter 3.1.8.

The authorizations' authentication procedure contents:

- Verification of the authenticity of the submitted request,
- Verification of compliance of legal entity's data filled in the request with those from the submitted documents,
- (optional) verification of the proof of private key possession (if the request refers to a key pair for signature creation) and the compliance degree of the legal and natural entity's ND that might act on behalf of this legal entity,
- Existence of a document issued by at least a member of the administration council and which confirms the natural person's authorization; the document must be notarized,
- Contact the direct superior of the natural entity to confirm the authorization.

3.1.11 Trade marks

Certsign doesn't verify if the Subscriber (the certificate user) is the person on whose name the trademark is registered at the Romanian State Office for Inventions and TradeMarks or if he benefits on the right of using it, right given by the trademark owner. The subscriber is the only one responsible for the information correctness provided for issuing the digital certificate. The Romanian State Office for Inventions and TradeMarks is the specialized body of the central public administration, the only authority that protects the trademarks and geographical indications in Romania. According to the Law 84/1998 regarding trademarks and geographical indications: "The right over the trademark is achieved and protected through registration at the Romanian State Office for Inventions and TradeMarks (Art 4)."

3.2 Subscriber's Identity Authentication in Certificate Renewal or Modification

To keep the continuity of the certificate, prior to its expiration, the user must request a new certificate. The new certificate may contain the same key (renewal). Upon users' request it is possible to keep the keys for a well determined period. More exactly, the key lifetime may not exceed a period twice as long than the maximum lifetime of a certificate. If this condition cannot be fulfilled another certificate has to be issued.

The renewal is allowed only before the certificate expiration. It can be done with maximum 30 days prior to the expiry and only once.

The identity of the subscribers that request the certificate renewal or its modification must be checked.

The procedures used aim to check whether the person or organization asking for a new certificate for a user is entitled to such claim.

Subscribers that send requests straight to a Certification Authority can be checked by this authority based on the electronic signature and on the public key certificate associated to this signature.

The certificate renewal or modification is not applied for certificates issued by certSIGN Class 1.

3.2.1 Certificate Renewal

A Subscriber or a Certification Authority uses the renewal if they already own a certificate and a private key associated to it and wishes to continue to use the same key pair. The new certificate created as result of the renewal consists of the same public key, same name and the rest of the information that are taken from the previous certificate, but the availability period, serial number and the issuer's signature are different from the data in the previous certificate. (see Chapter 4.6)

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

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

3.2.2 Certificate Modification

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

3.3 Subscriber's Identity Authentication in Certificate Revocation

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

- In first case, the Subscriber must submit an authenticated request for certificate revocation. The Subscriber authenticates the request by applying an electronic signature.
- The Subscriber that lost an active private key (or it was stolen) must use a second method. The revocation request must be certified by the Registration Authority.

In both cases, there must be a univocal identification of the Subscriber's identity. The revocation request may aim more certificates. The Subscriber's authentication and identification at the Registration Authority is realized analogically to the original registration (see Chapter 3.1). The Subscriber's authentication to the Certification Authority consists of

verifying the authenticity of the request. The detailed revocation procedure is described in Chapter 4.9.3.

4 Operational Requirements

There are further described the basic procedures of the certification process. Every procedure begins with sending a request by the Subscriber: *indirectly* (after original confirmation of the request by the Registration Authority) or *indirectly* to a Certification Authority. Based on the request, the Certification Authority takes a decision concerning the providing / rejection of the service requested. The requests sent must contain necessary information for correct identification of the Subscriber.

certSIGN provides access to the following basic services:

- a. registration, certification, renewal, rekey, certificate modification;
- 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 10 and 16. For all certificates classes excepting the test ones, the certificate revocation services are rendered in maximum 24 hours from the request.

If the request sent contains a public key the key must be prepared so that it could cryptographically connect the public key with other data specified in the request, especially with the Subscriber's identification data. A request may contain instead of public key the Subscriber's request to generate an asymmetric key on his name. This might be fulfilled by a Certification Authority or by the Registration Authority. Following the generation the keys are sent on secured path to the Subscriber so that they cannot be activated by an unauthorized person.

4.1 Application Submission

Requests for one of the Certification Authorities may be sent directly by a Subscriber or indirectly by a Registration Authority's operator. Subscriber's applications are directly sent to a

Certification Authority or indirectly to the Registration Authority. Applications sent directly may aim a certificate registration or modification; other applications concerning the certification services rendered by a Certification Authority are also allowed.

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

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

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

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

- Certificates for natural entities – issued as following a request,
- Certificates for natural entities – issued as following the submission of a request when a Certification Authority or the Registration Authority generates the key pair and a certificate and sending a cryptographic device (token), it sends them to a natural entity,
- Certificates for natural entities – issued as following a request submitted by a representative on behalf of the natural entity,
- Certificates for natural entities – issued as following the submission of a request by the representatives or employees of an organization that empowers them with the respective authorization.
- Certificates for devices (that apply to servers for instance) or certificates of the applications owned by the natural entities (employees of the organization or their agents) authorized to use that device or application.

4.1.1 Registration request

A registration request is sent by a Subscriber indirectly to the Registration Authority or directly to a Certification Authority and contains at least the following information:

- Full name of the institution or the first name and surname of the Subscriber,

- The distinctive name which structure depends on the Subscriber's category (see Chapter 3.1.2),
- identifiers: Registration Code of the Company / Personal Serial Number
- Subscriber's address,
- Type of requested certificate,
- Identifier of the certification policy based on which the certificate is issued;
- e-mail address,
- public key to be certified.

Following the Subscriber's identity authentication (see Chapters 3.1.8 and 3.1.9) that requests the registration and after receiving the Registration Authority's confirmation, the request is sent to a Certification Authority.

4.1.2 Certificate Renewal, Rekey or Modification Request

A certification request, rekey or certificate renewal must contain at least:

- Distinctive name of the solicitor (Subscriber);
- Type of certificate requested by the Subscriber;
- Identifier of the certification policy based on which the certificate must be issued;
- Public key (previously used in case of certificate renewal or new in case of certificate rekey) that will be certified.

4.1.3 Certificate Revocation Request

Information included in the certificate revocation request are the following:

- Distinctive name of the solicitor (Subscriber),
- List of certificates revoked or suspended as a pair: serial number, reason for revocation.

Partial or full data included in the request above must be authenticated by electronic signature if a Subscriber already owns a valid private key to create a signature.

A revocation request may be sent via e-mail along with the authentication data in written (letter, fax), or orally (by phone). In the last two cases, the certificate is suspended until the submitted request is checked.

4.2 Request Processing

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

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

The request sent off-line may be done:

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

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

4.2.1 Request Processing in Registration Authority

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

- Registration Authority's operator receives the Subscriber's request
- The operator verifies the data from the request such as Subscriber's personal data (see the procedure described in Chapter 3.1.8) and verifies the existence of the proof of the private key possession (see Chapter 3.1.6),
- Following the verification, the operator confirms the identity between the data stated and those included in the request; if the request contains non compliant data it is rejected,
- The request confirmed is sent to the Certification Authority,
- The Registration Authority checks also other data that are not specified in the request but they are also necessary for issuing the certificate.

4.2.2 Request Processing in the Certification Authority

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

4.3 Certificate Issuance

After receiving and processing a request (see Chapters 4.1 and 4.2) the Certification Authority issues a certificate. A certificate is considered valid (in active status or prepared) when it is accepted by a Subscriber (see Chapter 4.4). The issued certificates' availability period depends on the certificate's type and the Subscriber's category and is compliant with the periods presented in Table 6.3.2.2.

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

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

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

certSIGN Certification Authority uses two basic methods to inform a Subscriber about the certificate issuance:

- First method implies using the electronic mail and consists of sending (at the address rendered by the Subscriber) information that allows the Subscriber to obtain the certificate. This method is also used when it is necessary to inform all Subscribers of a certain Certification Authority about the issuance of a new certificate for the respective authority.
- The second method consists of issuing a new certificate and placing it (usually along with a private key) on a cryptographic device and sending the certificate (by mail) on the Subscriber's (a PIN code is sent in a distinctive letter).

Every certificate issued is published in certSIGN's Repository. The certificate publication is equivalent with the notification of other Relying Parties about the fact that a certificate was issued for a Subscriber. certSIGN publishes a certificate in the Repository after the certificate acceptance by the Subscriber (see Chapter 4.3).

4.3.1 Certificate Issuance Awaiting

The registration and certification or renewal request (key or certificates) will be examined, and the Certification Authority will issue a certificate during the period of time specified in Table

4.3.1. These periods depend on first hand on the accuracy of the data sent and the cooperation way between certSIGN and the solicitor.

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

Table 4.3.1. Maximum awaiting period for certificate issuance

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

4.3.2 Certificate Issuance Rejection

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

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

Information concerning the denial decision for issuing a certificate and its reasons are sent to the solicitor. The solicitor may request again the issuance of a certificate only after the reasons that lead to the denial are solved.

4.4 Certificate Acceptance

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

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

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

If a certificate is rejected in 7 calendar days from its receiving then the certificate is considered accepted.

Every certificate accepted is published in certSIGN's Repository and is available for the public. Certificate acceptance is univocal to the Subscriber, prior to its usage 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 Certificate and Key Usage

The Subscribers must use the private key and certificates:

- In compliance with the purpose stated in the present CPS and in compliance with the certificate's content (fields *keyUsage* and *extendedKeyUsage*, see Chapter 4.3),
- In compliance with the provisions of the agreement between the Subscriber and certSIGN,

- Only during the availability period (does not apply to certificates for digital signature checking),

When the certificate is suspended until its possible revocation, the Subscriber cannot use the private key to create a signature.

Relying Parties must use the private keys and certificates:

- In compliance with their stated purpose in the present CPS and in compliance with the certificate content (fields *keyUsage* and *extendedKeyUsage*, see Chapter 4.3),
- In compliance with the provisions of the agreement between the Subscriber and certSIGN,
- Only after verification of their status (see Chapter 4.9) and verification of the Certification Authority's signature that issued the respective certificate.

4.6 Recertification

certSIGN provides recertification services for the same cryptographic key pair.

4.7 Key Certification and Certificate Rekey

Key certification and rekey is done when a Subscriber (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. Certification and certificate rekey must be interpreted as it follows:

- Key certification is not associated to any valid certificate and used by Subscribers to obtain one or more certificates of any type, not necessarily within the same certification policy (in case the class of the new certificate is smaller than that of the already existing certificates – for example the Subscriber has a class 3 certificate and requests one of class 2 – the identity authentication is based on these certificates or on the corresponding management passwords; otherwise, the procedures are identical with those used for issuing a new certificate),

- Rekey refers to a certain certificate mentioned in the request; in this scenario, the new certificate has the same content; the only differences are: a new public key, a new serial number, a new availability period and a new signature of the Certification Authority.

The request for rekey sent by a Subscriber may be applied to a valid certificate that was not revoked.

Key certification or certificate rekey is realized only upon Subscriber's request and must be preceded by the submission of a request on a corresponding form filled in by the Subscriber.

Requests must 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 issuing a new certificate with the serial number,
- The Subscriber is committed to send the confirmation for certificate acceptance to a certification Authority,
- 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 Subscribers (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 Rekey

CertSIGN doesn't offer rekey services.

4.9 Certificate Modification

A certificate modification supposes the replacement of the certificate in use (currently valid) with a new certificate in which – unlike the certificate to be replaced – part of the data can be modified, except the public key.

Certificate modification:

- Is realized only upon Subscriber's request and must be done after submitting a corresponding request for certificate modification,
- Can be realized for certificates which availability period did not expire and which were not revoked either.

Only the following data can be modified:

- Subscriber's surname (for example due to marriage, divorce etc.),
- Organizational unit or job,
- e-mail address,
- Subscriber's role or rights included in the certificate,

Procedure of certificate modification requires authentication of request by a Subscriber by its electronic signing. The Subscriber must have an available private key to create the electronic signatures. If the Subscriber does not have such a key he must undertake the certification procedures described in Chapter 4.7. Requests of certificate modification must be confirmed by the Registration Authority. Procedures of certificate modification request processing is the same with the one described in Chapter 4.1, and the procedure of certificate issuing is the same with the one described in Chapter 4.2. Following this process:

- The Subscriber is notified about the issuing of a new certificate with a new serial number;
- The Subscriber is obligated to submit authorized certificate acceptance confirmation to a Certification Authority in term of 7 calendar days (see chapt 4.4);
- The new certificate is published in the Certification Authority's Repository.

If the modification procedure is successfully the modified certificate is revoked and placed in the Certificate Revocation List (CRL). As revocation reason it is mentioned *affiliationChanged* that means: (1) that the revoked certificate was replaced with another one which contains modified data such as Subscriber's name and (2) that the Relying Parties are informed that there is no reason to suspect that a private key associated to the certificate was compromised.

The revocation procedure may also be applicable to certain Certification Authorities and in such cases all Certification Authority's clients are informed about this procedure.

4.10 Certificate Revocation

A certificate revocation has a significant influence on its usage and on Subscriber's obligations. Shortly after a Subscriber's certificate revocation, the certificate must 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 does not affect nor the transactions made before the revocation and neither 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 should be safely stored until it is physically destroyed.

CertSIGN doesn't offer suspension service for its certificates.

4.10.1 Circumstances for certificate revocation

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

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 parties decide to terminate the contract concluded with these; in this case the revocation is strictly bounded with cancellation of Subscriber's registration at the

Certification Authority; if the Subscriber itself does not request the revocation, the Certification Authority or a representative of the institution where the Subscriber works, has the right to do so;

- The Subscriber owner of a public key 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 must 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,
- The Subscriber, employee of an organization, did not returned the cryptographic device used for storage of the certificate and of the corresponding private key at the termination of the labor contract,
- In other cases when the Subscriber does not comply with the rules of this CPS, Certification Policy, or the agreement.

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 (see Chapter 3.4) through the Registration Authority (this implies the Subscriber to contact the authority), or directly to a Certification Authority (the request may be authenticated by signature). The revocation request must contain information that allow the secure authentication of the Subscriber by the Registration Authority in

compliance with provisions of Chapter 3.1.8, If the Subscriber's identity authentication is not successfully the Certification Authority rejects the revocation request and suspends the certificate until the revocation request will be examined in detail.

4.10.2 Who can request certificate revocation

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

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

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

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

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

Every request must be sent:

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

4.10.3 Procedure for certificate revocation

The certificate revocation may be performed in the following manners:

- First method is based on sending an electronic revocation request authorized by a password to a Certification Authority; such a revocation may be initialized only upon Subscriber's request
- The second method requires the sending of an electronic revocation request to certSIGN, confirmed (by electronic signature) by the Registration Authority; this method applies in situations when (a) the Subscriber lost its private key or its password, or the private key was stolen or (b) the revocation request was sent to the representative of the Subscriber, an authorized representative of the Certification Authority or of the Registration Authority under the condition that there are enough reasons to request such a revocation;
- The third method implies sending a non-electronic authenticated request (paper document, fax, telephone etc.) to certSIGN; the authentication of a paper document (including a fax) may be done at the Registration Authority, for example with a stamp and a hand signature of a person known by certSIGN, or by placing a password within the document, password known only by the person requesting the revocation; a request made by phone is fulfilled only after the password is sent; after the successful verification of the request the Registration Authority prepares the electronic confirmation of the revocation request and submits it to the Certification Authority.

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

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

A certificate revocation request takes place as it follows:

- The Certification Authority following the receiving of a certificate revocation request checks it; if the request is electronic the Certification Authority verifies the correctness of the revoked certificate and (optionally) the correctness of the certificate attached to the request; the request on paper requires the solicitor's authorization; such a confirmation may be obtained on the phone, by fax, or while the Subscriber personally visits an authorized representative of the Certification Authority (or vice versa);
- If the request is successfully verified, the Certification Authority places the information concerning the certificate revocation in the Certificate Revocation List (CRL) along with information concerning the reasons for revocation (see Chapter 7.2.1);
- The Certification Authority notifies electronic or by mail the entity that requests the revocation about the revocation or about the decision of request cancellation along with the reasons for this cancellation.
- Moreover, if the party requesting the revocation is not the Subscriber, the Certification Authority must notify the Subscriber about the certificate revocation or about the starting of the revocation process.

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

4.10.4 Certificate Revocation Maximum Period

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

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

As it is described in Table 4.9.4.

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

Table 4.9.4. The maximum period for processing a certificate revocation request

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

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

4.10.5 CRL issuance frequency

Every Certification Authority part of certSIGN issues different Certificate Revocation Lists. A new CRL is published in the Repository after every certificate revocation, within maximum one day. If the key compromising is the reason for the revocation the new CRL is issued immediately after the revocation request processing (see Chapter 4.9.4). 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 authorities affiliated to certSIGN CA.

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

4.10.6 Certificate Revocation List Checking

A Relying Party as following of receiving a document electronically signed by the Subscriber, is committed to verify if the public key certificate corresponding to the private key of the Subscriber used for creating electronic signature is not placed in the Certificate Revocation List. The Relying Party is committed to use the current CRL.

A certificate's status verification may be based exclusively on CRL only in case the CRL's issuing period frequency stated by certSIGN cannot bring any important damage or loss for the Relying Party. Otherwise, a Relying Party is committed to contact (by phone, fax etc.) the certificate issuing authority or to use the *on-line* certificate status verification service.

If a certificate to be checked is placed in a CRL, the Relying Party is committed to reject the document associated to this certificate if the revocation reason is one of the following:

- a. *unspecified* – not known
- b. *keyCompromise* – compromise of the private key security
- c. *cACompromise* – compromise of the Certification Authority security
- d. *cessationOFOperation* – termination of the services associated to the private key

If a certificate was revoked for one of the following reasons:

- e. *affiliationChanged* – data modification,
- f. *superseded* – key modification,

The final decision over the certificate's credibility will be taken by the Relying Party. When taking this decision the Relying Party must take into consideration that the reason specified in paragraph 4.10.6 lit f do not represent the Subscriber's private key compromise.

4.10.7 On-line Certificate Status Verification

certSIGN provides the certificate's status verification service in real time. This service is realized based on the OCSP protocol described in RFC 2560. Using OCSP it is possible to obtain more exact data (compared to the exclusive usage of the CRL) concerning a certificate status.

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

- *good* – meaning a positive response to a request that must be seen as confirmation for the certificate validity,
- *revoked* – meaning the certificate was revoked,
- *unknown* – meaning the certificate was not issued by none of the affiliated Certification Authorities.

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

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

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

4.10.8 Revocation of CA certificate

Certificate belonging to a Certification Authority can be revoked by the issuing authority. Such a revocation may appear in the following situations:

- The Certification Authority has reasons to believe that the data within the respective authority's certificate do not correspond to the reality,
- The private key of the Certification Authority or its informatic system were compromised thus the credibility of the issued certificates is damaged,
- The Certification Authority violated the material obligations of the present CPS, the Certification Policy or the contract.

4.10.9 Circumstances for certificates suspension

Does not apply.

4.10.10 Who can request the suspension of a certificate

Does not apply.

4.10.11 The procedure for certificates suspension

Does not apply.

4.10.12 Limitation of the suspension period of a certificate

Does not apply

4.11 Tokens or smartcards management

For the moment certSIGN does not have tokens or smartcards lifecycle management processes in place.

4.12 Events recording and auditing 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 at any time they need it, in order to solve legal disputes or to detect security breaches. 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. (see Chapter 2.7).

The internal auditor of certSIGN has to perform annually an audit to check if the controls implemented are compliant with the current CPS and are efficient.

4.12.1 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 overwritten to prevent their modification or forgery.

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.

The records' content refers to:

- firewall's and IDS' alerts,
- operations associated to the recording, certification, renewal, revocation, etc.,

- modifications of the hard or soft structure,
- modifications of the network and connections,
- physical recordings in the secured areas and security violations,
- password changes, rights over PIN codes, employee's roles,
- the successful or unsuccessful access to certSIGN's database and to the server's applications,
- key generation for CA, RA etc.,
- every request received and the issued electronic decision changed between Subscriber and CA/RA,
- history of the backup copies creation and of the records archives.

Registration requests associated to services rendered sent by a Subscriber, apart from their usability in dispute resolving and abuse detection, allow calculation of a fee for certificate issuance.

Access to logs is exclusively allowed for the security administrator, the administrators of the Certification Authorities and auditors (see Chapter 5.2).

4.12.2 Frequency of Logs Processing

Records from the logs must be reviewed in detail at least once a month. Any event with a significant importance must be explained and described in a log. The log verification process includes the verification of possible forgeries or modifications and the verification of any alert or anomaly registered in the logs. Any action performed as a result of a detected malfunction must be recorded in the journal.

4.12.3 Event Journals Retention Period

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 person's request, or authorized process. After exceeding the allowed capacity, journals are kept and archived and can be accessed exclusively off-line, from a certain workstation.

The archived journals are kept at least 2 years.

4.12.4 Protection of event journals

Weekly, every journal record makes the object of archiving on magnetic tape. After surpassing the accepted number of records for a journal, its content is archived. The archives can be encrypted using Triple DES or AES algorithm. A key used for archives encryption is placed under the security administrator's command.

Only the security administrator, the Certification Authority's administrator, 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 administrator 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. (Chapter 4.10.3).

4.12.5 Procedures for logs backup

certSIGN security policies require that the event journal should have a monthly backup. These backups are stored in auxiliary locations of certSIGN.

4.12.6 Notification to entities responsible for responding to events

Module for analysis of the event journal implemented in the system examines current events and automatically notifies about suspected or security violating activities. In the case of activities having influence on the system security, the security administrator and Certification Authority administrator are automatically notified. In the other cases, the notification is directed only to the system administrator. Information transmission to authorized persons about critical – from the point of view of the system security – situations is carried out by other, appropriately secured, means of communication, for example pager, mobile phone, electronic mail. Notified entities take appropriate actions to prevent the system from detected threat.

4.12.7 Vulnerability Assessment

The Certification Authorities, the Registration Authority and the Repository must perform a vulnerability assessment for every internal procedure, application and informatic system. Requirements for analysis may be also determined by an external institution, authorized to carry out certSIGN audit. The security administrator is responsible for an internal audit which should control compliance of entries in the security journal, correctness of its backup copy retention, activities executed in the case of threats and compliance with this Certification Practice Statement.

An external institution carrying our security audit executes this activity according to guidelines described in ISO/IEC 13335 (Guidelines for Management of IT Security) and ISO/IEC 17799 (Code of Practice for Information Security Management).

4.11 Token/Smartcard management

Now certSIGN doesn't have management processes for the token/smartcard lifecycle.

4.12 Events and Audit Procedures Recording

To efficiently manage certSIGN's systems and to be able to audit the user's and staff actions, all the events occurred in the system are recorded. Information recorded make up event journals (logs) and must be kept thus to allow the Relying Parties access the corresponding and

necessary information to solve disputes or to detect attempts of compromising certSIGN's security. The recorded events make the object of archiving procedures. The archives are kept outside certSIGN's perimeter.

When it is possible, the logs are automatically created. If the logs cannot be automatically created there will be used logs on paper. Every registration in log, electronically or by hand, is kept and disclosed when an audit takes place (see Chapter 2.7).

In certSIGN's systems the internal security auditor is committed to perform an yearly audit concerning the following of the present CPS regulations by the mechanisms and procedures implemented and to evaluate the efficiency of the current security procedures

4.13 Backup and recovery procedure

The safety copies allow complete recovery (if there is necessary, for example, after damaging the system) of data essential for certSIGN activity. To perform this aspect there are copied the following applications and files:

- Installation disks for system applications (for example operating system),
- Installation disks for Certification and Registration Authorities applications.
- Web server and disks to install the Repository,
- History of keys, certificates and authority's CRL,
- Repository data,
- Data concerning the Subscribers and certSIGN employees,
- Event journals.

The way the backup copies are created influences the time and cost to restore the Certification Authority after damaging or destroying the system. certSIGN uses both full backups (weekly), and incremental backups (daily), all copies are cloned and the clones are kept in other location, under the same security conditions as those in the primary location.

The restoring procedure will be checked at least once in three months to check the backup's usefulness in case of crash. There must be checked if the data saved on tape are enough to restore the system as quickly as possible. The tests' results will be recorded.

4.14 Records archival

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

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

The *off-line* archive contains 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 Subscriber.

On the basis of the archives, backup safety copies are created and retained outside certSIGN location.

4.14.1 Types of data archived

The following data are subjected to archive:

- information from examination and evaluations (arising from an audit) of logical and physical protections of a Certification Authority, a Registration Authority and the Repository,
- received requests and issued decisions in an electronic form, submitted by a subscriber or to the Subscriber as files or electronic messages,
- Subscribers database,

- Certificates database,
- Issued Certificate Revocation Lists,
- History of Certification Authority Key, from its generation to destruction,
- History of the Subscribers keys, from their generation to destruction, if the keys are subjected to archive in Certification Authority databases

4.14.2 Frequency of data archive

Data archival is carried out on several levels, such as:

- Certificate database and subscriber's database are retained on certSIGN CA media, for a period of three years (from the time of certificate issuance). For the following three years, archives are stored on magnetic tapes or CDs, still available on-line. In the seventh year (six years after certificate issuance) all information regarding Subscribers and their certificates are stored on CDs and available off-line,
- CRL, electronic correspondence and requests submitted by Subscribers, as well as issued decisions are subjected to archive in the same pattern and frequency as for the certificate and Subscribers databases
- Certification Authorities and Registration Authorities' keys are stored – after expiration of corresponding certificate – on unrewritable media and encrypted with the key, controlled by the security administrator; archived keys are available only off-line.

4.14.3 Archive retention period

Archived data (in paper or electronic form), described in Chapter 4.12, are retained for the period of time presented in Tab.4.4. After expiration of the declared retention period, archived data are destroyed.

Certificate Policy	Minimal archive retention period
certSIGN Class 2	15 years
certSIGN Class 3	15 years
certSIGN Class 4	15 years

Table 4.4. Minimal archive retention period

4.14.4 Requirements for time stamping of the records

It is recommended that archived data should be signed with a timestamp, created by the authorized Time Stamp Authority (TSA), having a certificate issued by the operational Certification Authority affiliated by certSIGN CA. Timestamp service is available at certSIGN.

4.14.5 Access procedures and archived information verification

To verify the integrity of archived information, data are periodically tested and verified against original data (if still accessible in the system). This activity may be carried out solely by the security administrator and should be recorded in the event journal. If any damages or modifications to original data are detected, the damages are to be corrected as promptly as possible.

4.14.6 Responsible entities notification for events treatment

The analyse mode for the events journal implemented in the system examine the current events and observe automatically the weird activities or the one that can compromise the security. For the activities that influence the system security the security administrator and the Certification Authority are notified. In other cases, the notification is redirected to the system administrator only. The information transmission about the critical situations to the authorised persons as security concern is made through other communication means,

accordingly protected, like pager, cell phone, electronic mail. The notified entities take the adequate measures to protect the system from the detected threat.

4.14.7 The vulnerabilities analyse

The Certification Authorities, the Registration Authority and the Repository are committed to analyse the vulnerabilities for every internal procedures, application and informatic system. The analyse requests can be established by a external institution, authorised to audit certSIGN. The security administrator has the task to make internal audits to verify the concordance of the registrations from the security journal, the correctness of the backup copies and the activities in case of a threat and the concordance of the Certificate Practice Statement.

The external institution that realises the security audit must respect the recommendation of ISO/IEC 13335 (Guidelines for Management of IT Security) and ISO/IEC 17799 (Code of Practice for Information Security Management).

4.15 Key Change over of a Certification Authority

The procedures for key changeover applies to the keys of the Certification Authorities affiliated to certSIGN and it describes the way in which the key changeover for authorities certificates is carried out, used for signing users certificates or CRLs. Rekey procedure is based on issuance of special certificates by a Certification Authority, facilitating a Subscriber who has old certification authority to obtain the new one and allowing the new Subscribers who already have a new certificate to obtain the old certificate to check the current data. Every key changeover of the Certification Authority is announced in advance by Web pages of certSIGN and delivered by electronic mail to every Subscriber of the Certification Authority whose keys are subjected to changeover. Additionally, in case of certSIGN ROOT CA key changeover, information about this event will be published by means of mass-media in the month preceding the expiration of private key's availability. The frequency of keys changeover of a Certification Authority

affiliated to certSIGN is given by the availability period of the authority's certificate, as it is presented in Table 6.3.2.1

From the moment of key changeover, the Certification Authority uses only a new private key for signing issued certificates and CRLs.

4.16 Key Security Violation 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.

4.16.1 IT&C systems applications and data security violation

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.

4.16.2 Key compromise or suspicion of Certification Authority private key compromise

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

- The Certification Authority generates a new key pair and a new certificate,
- All certificate users are immediately informed about the compromise of the private key, by means of mass media system and electronic mail,
- A certificate corresponding to the compromised key is placed on Certificate Revocation List
- All certificates in the certification path of the compromised certificate are revoked and a suitable reason for revocation is submitted,
- New certificates for Subscribers are generated
- The new certificates for Subscribers are submitted to them without charging any fees.

4.16.3 Security coherence after disaster

Upon every system recovery after disaster, the security administrator or Certification Authority administrator should act in conformity with Business Continuity and Disaster Recovery Plan.

4.17 Certification Authority termination or service transition

Obligations described below are developed to minimize disruptions to 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 Subscribers of the authority that certified the Certification Authority subjected to termination (if such exists) and transition of responsibilities (services provided to the Subscribers, databases, etc.), in compliance with the regulations in force of other Certification Authority.

4.17.1 Requirements associated to duty transition

Before a Certification Authority ceases its activity, it has to:

- notify the Certification Authority that issued its certificate about their intention to terminate services as the authorized certification authority; the notification should be made 90 days before the agreed date of the termination,
- notify (at least 30 days in advance) its Subscribers who hold active (unexpired and unrevoked) certificates issued by this authority about decision to terminate its services,
- revoke all certificates which remain active (unexpired and unrevoked) in the declared moment of service termination, regardless of the fact if a subscriber has submitted or has not submitted a suitable request,
- notify all Subscribers of the Certification Authority about the termination of activity,
- make all necessary effort to minimize disruptions to interests of Subscribers and legal entities engaged in an ongoing process of electronic signature verification using digital certificates issued by the Certification Authority subjected to termination of activity,
- prepare an agreement (for example, with another Certification Authority according to Chapter 4.14.2) guaranteeing protection of data,
- pay compensations (not exceeding fees for issuance and storage of certificates) to the Subscribers whose unexpired and unrevoked certificates will be revoked before their expiration date.

4.17.2 Certificate issuance by the successor of terminated Certification Authority

To provide continuity of certificate issuance services for Subscribers, 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.

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 Personal CA Class 2, certSIGN Qualified CA Class 3, certSIGN Enterprise CA Class 3, certSIGN Non-Repudiation CA Class 4) or to the institution which the agreement was signed up with (in the case of termination of services of certSIGN ROOT CA).

5 Physical, Organizational and Personnel Security 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.

5.1 Physical Security Controls

5.1.1 certSIGN physical security 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.

5.1.1.1 Site location

certSIGN is located in Bucharest, at the following address: 133 Calea Șerban Vodă, C1

5.1.1.2 Physical access

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

certSIGN facility and Certification Authority are publicly available every working day between 10.00 and 16.00. 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:

- Servers area,
- CA operators area
- RA operators and administrators area,
- Developing and testing area.

Servers' area is equipped with monitored security system built on the basis of motion, fire and flood sensors. Access to this area is granted only to authorized personnel, i.e. the security administrator, Certification Authority administrator and the system administrator. 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 from the area is automatically recorded in the event journal.

Access to the *operators and administrators 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.

5.1.1.3 Power and air conditioning

The operators and administrators area, as well as the developing and testing area, are air conditioned. 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.

5.1.1.4 Water exposure

The risk of flood in the servers' area is minimal due to a very large distance to the water pipes and certSIGN is located at the last floor. Additionally, the security personnel is placed next to the servers' area and they are instructed to immediately announce certSIGN administrator and the building administrator.

5.1.1.5 Fire prevention

certSIGN location benefits of a fire prevention and extinction system in compliance with the corresponding standards and regulations in this field.

5.1.1.6 Media storage

In accordance with the sensitivity of information, media containing archives and current data backup are stored in fireproof safes, located in a highly secured room. Access to the room and safes is allowed only for authorized persons.

5.1.1.7 Waste disposal

Paper and electronic media containing information significant for certSIGN security after expiration of the retention period (see Chapter 4.12) are destroyed. Security hardware modules are reset and deleted in compliance with the manufacturer's recommendations. These devices are, as well, reset and deleted when sent to service or repaired.

5.1.1.8 Offsite backup storage

Copies of passwords, PIN numbers and cryptographic cards are stored in safe-deposit box outside certSIGN seat.

Offsite storage affects 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.

5.1.2 Physical security controls within the Registration Authority

Computers registering Subscriber's requests and issuing their confirmations should be located in specially designated area and operate in on-line mode (have to be connected to the network). Access to these computers is physically secured against unauthorized individuals.

5.1.2.1 Site location

The Registration Authority (RA) is located in the operators and administrators area in certSIGN (see Chapter 5.1.1.2),

5.1.2.2 Physical access

Access to the Registration Authority has to be granted as described in Chapter 5.1.1.2 Access has to be monitored and limited to authorized individuals associated with the activity of the Registration Authority (Registration Authority operators, administrators) and to its customers.

5.1.2.3 Power and air conditioning

Registration authority building should be equipped with emergency power source system (UPS), allowing several minutes of continuous work of the system from the time of power cut. Air conditioning is not required.

5.1.2.4 Water exposure

The present CPS does not state any conditions in this respect for the Registration Authority.

5.1.2.5 Fire prevention and protection

The present CPS does not state any conditions in this respect for the Registration Authority.

5.1.2.6 Media storage

Media used for storage of archives and current information backup copies are held in the safes located in the Certification Authority area.

5.1.2.7 Waste disposal

Paper and electronic media, containing confidential or secret information are, upon expiration of the retention period (see Chapter 4.12), destroyed.

5.1.2.8 Offsite archive storage

The archives and current information processed by the computer system backup copy must be stored outside the location of the Registration Authority.

5.1.2.9 Emergency backup copy and archive storage

Archived data, emergency backup copies and other sensitive information is held in boxes of the safe, accessible solely to the authorized certSIGN employees.

5.1.3 Subscriber's physical security

Subscribers have to protect their system access password and PIN. Certificate owners should not leave their workstation unattended while it is in the unsecured cryptographic state, i.e. password or PIN has been entered.

In the case of a private key (after encryption with a Subscriber's password) storage on unsecured media, for example floppy disk, the media should be protected from unauthorized access.

5.2 Organizational security control

This Chapter presents the roles which can be defined for personnel, employed in certSIGN and in the Registration Authority and Subscribed institutions. This Chapter also describes responsibilities and duties associated with each defined role.

5.2.1 Trusted roles

5.2.1.1 Trusted roles in certSIGN

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

- **Security administrator** – Overall responsibility for the implementation of the security practices and policies. Additionally approve the generation/revocation of certificates.
 - Initiates installation, configuration and management of software applications and hardware (including network resources) of certSIGN; initiates and suspends services provided by certSIGN; manages the administrators, initiates and supervises key and shared secret generation; assigns rights in the field of security and user's access privileges; assigns passwords for new users' accounts; reviews event journals; supervises internal and external audits; receives and answers post-audit reports; supervises post-audit deficiency removal.
 - Oversees Certification Authority operators; configures the systems and the network; activates and configures network protections; creates accounts for certSIGN users; reviews system logs; verifies compliance of Certification Policy and CPS; generates shared secrets and keys; manages Certificate Revocation List; creates emergency backup copies; modifies server names and addresses.
- **System administrator** – Authorized to install, configure and maintain the Certification Authority's trustworthy systems for registration, certificate generation, subject device provision and revocation management. Installs hardware and operating systems; installs and configures the network equipments.
- **System operator** – Responsible for operating the Certification Authority's trustworthy systems on a day to day basis. Authorized to perform system backup and recovery. Has access to Subscribers' certificates; revokes Subscribers' certificates; provides continuity of backup copies and archives of database and system logs creation; manages databases; has access to confidential information about Subscribers but is not allowed to physically access any other system resources; transfers archive copies and current backup copies outside certSIGN seat.
- **System Auditor** – Authorized to access archives and audit logs of the Certification Authority's trustworthy systems. Responsible for performance of internal audit, compliance of a Certification Authority with this CPS; this responsibility extends also on Registration Authority, operating within certSIGN.

- **Repository administrator** – manages folders of certSIGN available to the public, creates and updates contents of repository folders, creates Web page and manages links.

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

5.2.1.2 Trusted roles in Registration Authority

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

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

5.2.1.3 Subscriber's trusted roles

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

5.2.2 Number of persons required per task

Keys – for the needs of certificate and CRL signing – generation process is the one of the operations requiring particular attention. The generation requires presence of at least two persons, acting as the security administrator and the system administrator. Certification Authority key generation process may be also observed by shared secret holders who retain their part of the key in secure location.

Presence of the security administrator, 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. Loading of cryptographic keys into Registration Authority hardware security module requires presence of the secret administrator and a Registration Authority operator.

Any other operation or role, described within this CPS or connected with a Subscriber, may be performed by a single person, assigned in this respect.

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.

5.3 Personnel control

certSIGN has to make 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 a Registration Authority acting on behalf of it.

5.3.1 Personal background, qualifications and required confidentiality clauses

The personnel employed in certSIGN and performing trusted role should obtain the approval from the security responsible. The approval is not required in the case of a person not performing a trusted role.

All personnel employed performing jobs which require access to classified information is authorized in this regard by ORNISS (National Registry Office for Classified Information).

Performance of trusted role as security administrator, the Certification Authority administrator and secret administrator (within Registration Authority) authorizes the access to classified information. Unauthorized reveal of this information may cause loss or disruption to the law-protected interests of a private person or an organization.

Procedures for access to undisclosed information and personnel trustiness verification check procedures comply with Private Information Protection law.

5.3.2 Personnel training requirements

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

- regulations of Certification Practice Statement,
- regulations of Certification Policy,
- procedures and security controls employed by a Certification Authority and a Registration Authority
- system software of a Certification Authority and a Registration Authority,
- responsibilities arising from roles and tasks performed in the system,
- procedures executed upon system malfunction, corruption to a Certification Authority

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.

5.3.3 Training frequency

Trainings described in Chapter 5.3.2 have to be repeated or supplemented always in situation when significant modification to certSIGN or its Registration Authority operation is executed.

5.3.4 Job rotation

This Certification Practice Statement does not imply any requirements in this field.

5.3.5 Sanctions for unauthorized actions

In the case of a discovery or suspicion of unauthorized access, the system administrator together with the security administrator (in the case of certSIGN employees) may suspend the perpetrator's access to certSIGN system. Disciplinary actions for such accidents should be described in suitable regulations and should comply with law in force.

5.3.6 Contract personnel

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 seat have to be escorted by certSIGN or the registration authority employee, except those who have previous approval from behalf of the security administrator and who can access internal classified information or in compliance with the law in force.

5.3.7 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

6 Technical information security controls

This Chapter describes procedures for generation and management of a cryptographic key pair of a Certification Authority, a Registration Authority and a Subscriber, including associated technical requirements.

6.1 Key pair generation and usage

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

certSIGN ROOT CA Certification Authority owns at least one self-signed certificate. A private key corresponding to the public key contained in the self-signed certificate is used exclusively to sign the public keys of the Certification Authorities **certSIGN CA Class 2**, **certSIGN Qualified CA Class 3**, **certSIGN Enterprise CA Class 3** and **certSIGN Non-Repudiation CA Class 4**, signing operational certificates and the Certificate Revocation List necessary for the authorities' functioning. A similar purpose is intended for private keys held by each authority: **certSIGN Demo CA Class 1**, **certSIGN CA Class 2**, **certSIGN Qualified CA Class 3**, **certSIGN Enterprise CA Class 3** and **certSIGN Non-Repudiation CA Class 4** and corresponding to public keys included in certificates issued by **certSIGN ROOT CA** for each of the authorities.

Key pairs owned by each Certification Authority should allow certificate and CRL signing – a public key associated with a private key authenticated with a self-signed certificate (in case of **certSIGN ROOT CA**) or certificate (in case of **certSIGN Demo CA Class 1**, **certSIGN CA Class 2**, **certSIGN Qualified CA Class 3**, **certSIGN Enterprise CA Class 3** and **certSIGN Non-Repudiation CA Class 4**).

An electronic signature is created by means of RSA algorithm in combination with SHA-1 cryptographic digest.

6.1.1 Key pair generation

certSIGN Demo CA Class 1, certSIGN CA Class 2, certSIGN Qualified CA Class 3, certSIGN Enterprise CA Class 3, certSIGN Non-Repudiation CA Class 4 keys, as well as of other subordinated authorities are generated within certSIGN seat, in the presence of a trusted group of persons (the security administrator and the Certification Authority administrator have to be members of this group).

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

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

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

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

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

6.1.1.1 Procedures of generation of certSIGN ROOT CA initial keys

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

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

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

6.1.1.2 Procedures of generation of certSIGN CA initial keys

Procedures of generation of initial certSIGN CA keys include:

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

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

6.1.1.3 certSIGN ROOT CA certificate rekey procedure

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

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

to securely retrieve expired certificate, which may be needed for verification of the data signed in the past.

A particular procedure is applied for update of key pair used for certificate and CRL (certificate) signing. It is based on the issuance of special certificates by **Ro-Trust ROOT CA**. The certificates enable subscribers who have already installed an expired certificate of **Ro-Trust ROOT CA** to securely migrate to work with a new certificate: new subscribers already possessing a new certificate are enabled to securely retrieve expired certificate, which may be needed for verification of the data signed in the past (see RFC 2510).

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

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

- generation of a new key pair,
- creation of a certificate, containing new public key of certSIGN ROOT CA, signed with old private key (certificate **NewWithOld**),
- deactivation of old private key and activation of new private key within hardware security module a new private key for certificate and CRL signing is loaded,
- creation of a certificate, containing old public key certSIGN ROOT CA, signed with new private key (certificate **OldWithNew**),
- creation of a certificate containing new public key of certSIGN ROOT CA, signed with new private key (certificate **NewWithNew**),

- publication of new certificates in the repository, submission of the information about new available certificates and, optionally, placement of the cryptographic digest of the new public key in newspapers.

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

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

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

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

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

6.1.1.4 Subordinate certification authority rekey procedure

Procedures for certification authority rekey (key update) of Certification Authority for **certSIGN CA Class 2**, **certSIGN Qualified CA Class 3**, **certSIGN Enterprise CA Class 3** and **certSIGN Non-Repudiation CA Class 4** are executed similarly as for certSIGN **ROOT CA** (see Chapter 6.1.1.3) except one step: certificate **NewWithNew** is issued by superior authority.

6.1.2 Private Key Delivery to Entities

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

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

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

6.1.3 Public key delivery to the Certification Authority

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

Requests submitted to a Certification Authority may, in particular cases, require confirmation issued by the Registration Authority (see Chapter 3 and 4).

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

6.1.4 Certification Authority public key delivery to Relying Parties

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

certSIGN Certification Authorities distribute their certificates in two different methods:

- placement in the publicly available repository of certSIGN; retrieval of the certificates requires the subscribers to visit web page available at <http://www.certsign.ro/repository>,
- distribution together with the software (Web browsers, email clients, etc.), which allows usage of services offered by certSIGN.

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

6.1.5 Key sizes

Sizes of keys deployed by Certification Authorities, Registration Authority operators and Subscribers are presented in Table 6.1.

Key owner	Primary key usage		
	RSA for certificate and CRL signing	RSA for message signing	RSA for key exchange
certSIGN ROOT CA	2048 bit	-	-
certSIGN CA	2048 bit	-	-
certSIGN Demo CA Class 1	2048 bit	-	-
certSIGN CA Class 2	2048 bit	-	-
certSIGN Qualified CA Class 3	2048 bit	-	-
certSIGN Enterprise CA Class 3	2048 bit	-	-
certSIGN Non-Repudiation CA Class 4	2048 bit	-	-
Registration Authority's operator	-	1024 bit	-
Private entities and their hardware	-	1024 bit	1024 bit
Legal entities and their hardware	-	1024 bit	1024 bit

Table 6.1. Size of keys used

6.1.6 Public Keys parameters generation and parameter quality checking

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

- ability to execute encryption and decryption operation, including electronic signature creation and its verification,
- key generation process, which should be based on strong random cryptographic number generators – physical sources of white noise, if possible,

- immunity to known attacks (applies to RSA and DSA algorithms).

6.1.7 Hardware and/or software key generation

Allowable methods for key generation depend on applicable Certification Policy and presented in Table 6.2. In the case of Certification Authorities, keys are generated by means of hardware security modules complying with requirements presented in Chapter 6.2.1. Registration Authority operators' keys are generated by means of hardware security modules of lesser requirements (than described in Chapter 6.2.1). In the case of key generation by a Subscriber, a Certification Authority allows hardware and software key generation method (Chapter 6.2.1).

Certification Policy	Key generation method	Observations
certSIGN Class 1	Hardware or software	
certSIGN Class 2	Hardware or software	
certSIGN Class 3	Hardware	Except web and VPN servers, in which case the keys are generated by the subscriber
certSIGN Class 4	Hardware	

Table 6.2. Subscriber's key generation method

6.1.8 Key usage

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

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

- digitalSignature**: certificate intended for verification of electronic signature,
- 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,
- keyEncipherment**: intended to encrypt symmetric algorithm keys, providing data confidentiality,

- d) **dataEncipherment**: intended to encryption of Subscriber'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,

6.2 Private key protection

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

6.2.1 Standards for cryptographic modules

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

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

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

6.2.2 Private key dual access control

Multi-person control of a private key applies to private keys of certification authorities' **certSIGN CA Class 2**, **certSIGN Qualified CA Class 3**, **certSIGN Enterprise CA Class 3** and **certSIGN Non-Repudiation CA Class 4** used for certificate and CRL signing.

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

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

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

certSIGN Enterprise CA Class 3	2	3
certSIGN Non-Repudiation CA Class 4	2	3

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

The bridge access schemes are also used to insure the Subscriber's private key recovery. The accepted number of shared secrets and the necessary number of secrets allowing the private key restoration are disclosed in Table 6.2.3.

Certificate issuing authority	Number of shared secrets	Total number of distributed secrets
certSIGN CA Class 2	2	3
certSIGN Enterprise CA Class 3	2	3

Table 6.2.3. Distribution of shared secrets for User's encryption keys' recovery

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

6.2.2.1 Acceptance of secret shared by its holders

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

6.2.2.2 Protection of shared secret

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

- will not reveal, copy or share the secret with any other party and that he/she will not use the share in an unauthorized manner,

- will not reveal (directly or indirectly) that he/she is the holder of the secret,

6.2.2.3 Availability and erasure (transfer) of the shared secret

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

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

6.2.2.4 Responsibilities of shared secret holder

Shared secret holder should perform his/her duties and obligations according to the requirements of this Certification Practice Statement and in a deliberate and responsible manner in any possible situation. A shared secret holder should notify the issuer of the share in the case of the secret theft, loss, unauthorized revelation or security violation immediately after the incident occurrence. A shared secret holder is not responsible for neglecting his/her duties because of the reasons that are impossible to control by the holder, but is responsible for inappropriate revelation of the secret or neglecting the obligation to notify the issuer of the secret about inappropriate revelation or security violation of the secret, resulting from the holder mistake, neglect or irresponsibility.

6.2.3 Private Key custody

Subscriber's signature private keys or private keys of Certification Authorities are not subjected to custody.

6.2.4 Private Key backup

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

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

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

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

6.2.5 Private Key archival

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

6.2.6 Private Key entry into cryptographic module

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

- keys are generated outside the cryptographic module; this situation occurs for example in the case of Subscriber's key generation (on his/her demand) by a Certification Authority, their entry into a cryptographic card or any other hardware token prior to transfer of the media to Subscriber. A similar operation of key entry into a cryptographic module may be carried out by a Subscriber when the keys are delivered in an encrypted form and require local storage on a cryptographic device,

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

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

Introducing a private key into a security hardware module of the Certification Authority **certSIGN ROOT CA** or **certSIGN Demo CA Class 1**, **certSIGN CA Class 2**, **certSIGN Qualified CA Class 3**, **certSIGN Enterprise CA Class 3** and **certSIGN Non-Repudiation CA Class 4** requires the restoration of the key on cards in the presence of a corresponding number of shared secret owners that protects the module containing the private keys (see Chapter 6.2.2). Due to the fact that every Certification Authority can retain an encrypted copy of its private key (see Chapter 6.2.4), the keys may also be transferred between modules.

6.2.7 Method of activating the private key

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

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

All private keys of **certSIGN ROOT CA** or **certSIGN Demo CA Class 1**, **certSIGN CA Class 2**, **certSIGN Qualified CA Class 3**, **certSIGN Enterprise CA Class 3** and **certSIGN Non-Repudiation**

CA Class 4, entered into the module after their generation, import in an encrypted form from another module or restoration from shared secret remain in the active state until their physical erasure from the module or removal from certSIGN services. Activation of private keys is always preceded by the operator's authentication. The authentication is carried out on the basis of a cryptographic card held by the operator. After insertion of the card into the cryptographic module and provision of the PIN number, the private key remains in the active state until removal of the card from the module.

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

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

6.2.8 Method of deactivating private key

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

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

In the case of certSIGN, deactivation of a private key is carried out by the security officer only in the situation when the validity period of the private key has expired, the key has been revoked

or there is immediate requirement to temporary suspend the activity of the system. Deactivation of a private key is carried out by the removal of the card from the module.

6.2.9 Method of destroying the private key

Erasures of private keys of Subscriber or Registration Authority operators involve respectively their erasure from the media (floppy disc, cryptographic card, memory, hardware security module, etc).

If a private key is owned by a Subscriber that is a legal entity, the key may be destroyed solely by the authorized representative of the Subscriber.

Every private key's destruction is recorded in the event journal.

6.3 Other aspects of key pair management

From the point of view of technology, it is possible to use the same key pair either for electronic signature creation or for data encryption. Notwithstanding, this Certification Practice Statement does not recommend this practice. In the case of certificates issued within certSIGN Class 3 and 4 policies this practice is prohibited.

Remaining requirements of this Chapter apply to public key archive procedure and validity period of public and private keys of every Subscriber, including the Certification Authorities.

6.3.1 Public key archival

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

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

Every authority issuing certificates archives public keys of Subscribers to whom certificates were issued. Certification Authority public keys are archived together with private keys, in the

manner described in Chapter 6.2.5. Certificates may also be archived locally by Subscribers, especially when it is required by used application (e.g. electronic mail systems).

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

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

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

Public keys are retained in the digital certificate archive for a period of 15 years, according to table 4.4.

6.3.2 Usage period of public and private keys

Usage period of public keys is defined by the value of the field validity of every public key certificate (see Chapter 7.1). It is also a validity period of a private key. The maximal usage period of Subscriber's keys cannot exceed twice the life period of a certificate, which period is mentioned below.

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

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

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

Key owner	Main purpose of key usage
-----------	---------------------------

	RSA for certificate and CRL signing
certSIGN ROOT CA	25 years
certSIGN Demo CA Class1	10 years
certSIGN CA Class 2	10 years
certSIGN Qualified CA Class 3	10 years
certSIGN Enterprise CA Class 3	10 years
certSIGN Non-Repudiation CA Class 4	10 years

Table 6.3.2.1 Maximum usage period of CA certificates

Key owner	Certification Policy	Main key usage
Registration Authority's operator	certSIGN Class 2	1 year
	certSIGN Class 3	1 year
	certSIGN Class 4	3 years
Private persons and their hardware devices	certSIGN Class 1	3 months
	certSIGN Class 2	1 years
	certSIGN Class 3	1 years
Legal entities and hardware devices of private persons	certSIGN Class 4	2 years
	certSIGN Class 1	3 months
	certSIGN Class 2	1 year
	certSIGN Class 3	1 year
	certSIGN Class 4	3 years

Table 6.3.2.2. Maximum usage periods of Subscriber's certificates

6.3.3 Subscribers key management

CertSIGN doesn't provide any key management services for the subscribers.

6.4 Activation data

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

6.4.1 Activation data generation and installation

Activation data are used in two basic cases:

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

Registration Authority and Certification Authority operators, as well as other persons performing the roles described in Chapter 5.2 should operate passwords immune for brute force attacks (also called exhaustive attacks). It is recommended for Subscribers to use such passwords.

In the case of private key activation, it is recommended to use multi-factor authentication procedures, for example a cryptographic card and an authentication phrase or a cryptographic token and biometric (e.g. fingerprint reader).

The above authentication phrase should be generated in accordance with the requirements of FIPS-112.

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.

6.4.2 Activation data protection

Activation data protection includes activation data control methods preventing from their revelation. Activation data protection control methods depend on the fact whether they are

authentication phrases and whether control is enforced on the basis of private key or its activation data distribution into shared secrets. In the case of the authentication phrase, the recommendations described in FIPS 112 should be enforced, while protection of shared secrets requires implementation of FIPS 140 standard.

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

6.4.3 Other aspects of activation data

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

6.5 Computer security controls

Tasks of Registration Authorities and Certification Authorities operating within certSIGN are carried out by means of credible hardware and software.

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.

6.5.2 Computer security rating

certSIGN computer system complies with requirements described in ETSI Standards: ETSI TS 101456 (Policy requirements for Certification Authorities issuing qualified certificates) and CEN CWA 14167 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures).

6.6 Technical controls specific for life cycle

6.6.1 System development specific controls

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

Similar rules apply to hardware components replacement, such as:

- hardware is supplied in a manner allowing its tracing and evaluation of the route of the component to the place of its installation,

- replacement 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.

Current configuration of certSIGN system, as well as any modifications and updates to its system are recorded and controlled

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

6.7 Network security controls

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.

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.

6.8 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 2560. Information stated below describes the meaning of respective certificate fields, CRL and OCSP, applied standard and private extensions used by certSIGN.

7.1 Certificate profile

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

7.1.1 Contents of the certificate

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

Extensions defined in a certificate according to norms allow assignation of additional attributes to the Subscriber and his/her/its public key and simplify management of hierarchical certificate structure. Certificates issued in accordance with X.509 v.3 standard allow definition of proprietary extensions, unique for a given implementation.

7.1.1.1 Basic fields

certSIGN supports the following basic fields:

- **Version**: third version (X.509 v.3) of certificate format,
- **SerialNumber**: certificate serial number, unique within Certification Authority domain,
- **signatureAlgorithm**: identifier of the algorithm applied by a issuing Certification Authority,
- **Issuer**: distinguished name (DN) of a Certification Authority,

- **Validity:** validity period, described by the beginning date (**notBefore**) and the ending date (**notAfter**) of the certificate,
- **Subject:** distinguished name (DN) of the Subscriber that is the subject of the certificate,
- **SubjectPublicKeyInfo:** value of a public key along with the identifier of the used cryptographic algorithm associated with the key.

In certificates issued by certSIGN values of the above fields are set in accordance with rules described in Table 7.1.

Field name	Value or value's constraint	
Version	Version 3	
Serial Number	Unique value for all certificate issued by Certification Authorities within certSIGN	
SIGNature Algorithm	md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) or sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (Distinguished Name)	Name (CN) =	certSIGN {CA Class {1,2,3,4}}
	Organization (O) =	certSIGN
	Country (C) =	RO
Not before (validity period beginning date)	Universal Time Coordinated based. certSIGN owns a satellite clock controlled by Atomic Frequency Standard.	
Not after (validity period end date)	Universal Time Coordinated based. certSIGN owns a satellite clock controlled by Atomic Frequency Standard.	
Subject (Distinguished Name)	Distinguished names comply with the X.501 requirements. Values of all attributes of these fields are optional and their signification is described below.	
Subject Public Key Info	Encoded in accordance with RFC 2459, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key); RSA key size is presented in Chapter 6.1.5.	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 3280.	

Table 7.1. Profile of the basic fields of certificates

Profiles of all certificate (Subject fields):

Signing/encrypting/code signing nominal personal simple certificate

Mandatory: Name, First name, Country, Email

Optional: n/a

Clear name:

Subject: C=Country, CN=First Name Initial Name

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Signing/encrypting anonymous personal simple certificate

Mandatory: Pseudonym, Country, email

Optional: n/a

Pseudonym:

Subject: C=Country, CN=Pseudonym

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Signing/encrypting nominal professional simple certificate

Mandatory: Name, First Name, Country, Organization, City, email

Optional: Department, Function

Clear name:

Subject: C=Country, O=Organization, OU=Department*, CN = First Name Initial Name, T*
= Function, L = City

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Legal entities simple certificate/code signing professional certificate

Legal entities:

Subject: C=Country, O=Organization, OU=Department*, CN = Legal entity's name, L = city

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Nominal personal qualified certificate

Mandatory: Name, First name, Country, City, email

Optional: Telephone, County/Sector, Street, No., Block, Apartment, Postal Code

Clear name:

Subject: C=Country, CN=First name Initial Name, Phone*=Telephone, Serial Number = Personal Serial Number, L = City, STREET*=Address (Street, No, Block, Entrance, Apartment, Postal Code), S*=County/Sector, 2.5.4.41(Name)=First name Initial Name, G=First name, SN=Name

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Anonymous personal qualified certificate

Mandatory: Pseudonym, Country, City, email

Optional: n/a

Pseudonym:

Subject: C=Country, P=Pseudonym, Serial Number = Personal Serial Number, L = City, S=County/Sector

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Nominal professional qualified certificate

Mandatory: Name, First name, Organization, Country, City, email

Optional: Department, Function, Telephone, County/Sector, Street, No., Block, Apartment,
Postal Code

Clear Name:

Subject: C=Country, O=Organization, OU*=Department, CN=First name Initial Name,
T*=Function, Phone*=Telephone, Serial Number=Personal Serial Number, L=City,
STREET*=Address (Street, No, Block, Entrance, Apartment, Postal Code), S*=County/Sector,
2.5.4.41(Name)=First name Initial Name, G=First name, SN=Name

Legal entities qualified certificates

Mandatory: Name of the legal entity, Country, City, email

Optional: Telephone, County/Sector, Street, No., Block, Apartment, Postal Code

Clear Name:

Subject: C=Country, O=Organization, CN=Legal entity's name, Phone*=Telephone, Serial
Number=Sole Identification Number, L=City, STREET*=Address (Street, No, Block, Entrance,
Apartment, Postal Code), S*=County/Sector

Subject Alternative Name: Other Name – Principal Name = e-mail, RFC822 Name=e-mail

Web and VPN certificates

Subject: is given by subject field from the certificate request in PKCS10 format of the web server, or of the VPN device, under the condition that the client should prove the information in the field content represents identification data and he is authorized to use them.

Subject Alternative Name: DNS=optional server's name, IP Address=optional server's IP address

7.1.1.2 Standard extensions

Function of every extension is defined by the standard value of the corresponding object identifier (**OBJECT IDENTIFIER**). Extension, depending of the choice of issuing authority, may be **critical** or **non-critical**. If an extension is defined as **critical**, the application supporting certificate usage must reject every certificate containing an unrecognized critical extension. On the other hand, extensions defined as **non-critical** may be omitted.

certSIGN supports the following fields of standard extensions:

- **AuthorityKeyIdentifier**: identifier of a Certification Authority public key certificate associated with a private key, used for signing issued certificates – **this extension is not critical**,
- **SubjectKeyIdentifier** – subject key identifier – **this extension is not critical**,
- **KeyUsage**: allowed key usage – **this extension is critical**. This extension describes the usage of the key, e.g. key for data encryption, key for data exchange, key for electronic signature, etc:

digitalSignature (0) – key for electronic signature creation

nonRepudiation (1) – key associated with the non-repudiation services

keyEncipherment (2) – key for key exchange

dataEncipherment (3) – key for data encryption

keyAgreement (4) – key for key agreement

keycertsign (5) – key for certificate signing

CRLsign(6) – key for CRL signing

encipherOnly (7) – key only for encryption

decipherOnly (8) – key only for decryption

- **ExtKeyUsage**: defines the constraints related to the key usage – **this extension is not critical**. This field defines one or more areas, in addition to standard key usage, defined by **keyUsage** field, of the possible usage of a certificate. This field should be interpreted as constraint of allowed key usage purpose defined in field **keyUsage**. certSIGN issues certificates which may contain one of the following value or combination of such values in ExtKeyUsage field:

serverAuth – authentication of TLS Web servers; **keyUsage** field bits are set for: digitalSignature, keyEncipherment or keyAgreement

clientAuth – authentication of TLS Web clients; **keyUsage** field bits are set for: digitalSignatureand/or keyAgreement

codesigning – signature of executable codes; **keyUsage** field bits set for digitalSignature

emailProtection – E-mail protection; keyUsage field bits set for: digitalSignature, nonRepudiation and/or (keyEncipherment or keyAgreement)

ipsecEndSystem – IPSEC protocol protection,

ipsecTunnel – IPSEC protocol Tunnelling,

ipsecUser – IP protocol protection in user application,

timeStamping – binding of the digest value with the time provided by previously accepted trusted time source; **keyUsage** field bits are set for:digitalSignature, nonRepudiation.

OCSPsigning – assigns the right to issue certificate status confirmations on behalf of CA; keyUsage field bits are set for: digitalSignature,nonRepudiation

dvcs – issuance of confirmation by a notary authority, on the basis of DVCS protocol; keyUsage field bits are set for: digitalSignature, nonRepudiation, keyCertSign, cRLSign

EncryptedFileSystem – allows the usage of the certificate to encrypt the file system (EFS); it is a mandatory request from certain applications (i.e. EFS);

SmartCardLogon – allows the usage of the certificate for „smart-card logon” operation – authentication in the operating system, based on the digital certificate;

- **Certificate Policies** – the extension indicates the policy (policies) based on a Certification Authority will issue certificates or the policy (policies) based on which a Certification Authority issued a certificate. The extension is a **PolicyInformation** list– information (identifier, electronic address) about an applied certification policy. **This extension is not critical.**

Certification Policy Name	Policy identifier
certSIGN Class 1	{certSIGN} ¹ .{id-policy} ² . {id-cp} ³ .{id-Class-1} ⁴ =1.3.6.1.4.1.25017.1.1.1
certSIGN Class 2	{certSIGN} id-policy(1) id-cp(1)id-Class-2(2)= 1.3.6.1.4.1.25017.1.1.2
certSIGN Class 3	{certSIGN} id-policy(1) id-cp(1)id-Class-3(3)=1.3.6.1.4.1.25017.1.1.3
certSIGN Class 4	{certSIGN} id-policy(1) id-cp(1)id-Class-3(3)=1.3.6.1.4.1.25017.1.1.4

Table 7.2.Policies identifiers and their names

Certificates issued by Certification Authorities include also qualifiers, recommended by the RFC 3280.

- **PolicyMapping**: policy mapping – **this field is not critical**; this field contains one or more pairs of OID, defining equivalency of the certificate issuer policy with the certificate subject policy,
- **SubjectAlternativeName**: alternative name of the subject – this field is not critical,

¹ {certSIGN}=1.3.6.1.4.1.25017= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). certSIGN’s IANNA assigned number (20715); ² {id-policy}=1; ³ {id-cp}=1; ⁴ {Class-1}=1

- **BasicConstraints:** basic constrains – defines the certificate type (CA or end entity certificate), as well as the maximum accepted length for the certificate chain – **this field is critical**;
- **CRL DistributionPoints:** point of distribution of Certificate Revocation List – **this field is not critical**; the extension defines network addresses hosting the current CLR of the issuer Authority of the respective certificate,
- **AuthorityInfoAccessSyntax:** access to Certification Authority information – **this field is not critical**; the field indicates the method of information and service provision by the issuer of the certificate,
- **OCSPNoCheck:** if it is included in a OCSP responder certificate, the clients who receive OCSP responses signed with a private key associated to the certificate may trust the certificate status during its availability period; this extension **is not critical** and it is defined by the RFC 2560 standard.
- **NetscapeCertType:** this extension limits the certificate usage only to certain applications defined by the extension's value. If it is not present, the certificate may be used for any application except the ObjectSigning applications. This extension **is not critical**, and its value may be one of the following combinations:
 - SSLClient** (bit 0) – certificate may be used to authenticate a SSL client
 - SSLServer** (bit 1) – certificate may be used to authenticate a SSL server
 - S/MIME** (bit 2) – certificate may be used by clients of S/MIME secured mail
 - ObjectSigning** (bit 3) – certificate may be used to sign objects such as Java applets or plug-ins
 - SSL CA** (bit 5) – certificate may be used to issue certificates used for SSL
 - S/MIME CA** (bit 6) – certificate may be used to issue certificates used for S/MIME
 - ObjectSigning CA** (bit 7) – certificate may be used for issuing certificates used for ObjectSigning

Observation: for the value of NetscapeCertType extension, bit 4 is not yet defined as being reserved for a future usage

7.1.2 Certificate extensions

Certificates issued by certSIGN may contain various combinations of extensions defined in 7.1.1.2.

7.1.2.1 Certification Authorities certificates

A certificate issued for Certification Authorities may contain extension from Table 7.3 and 7.4.

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=CA, Path length constraint=none	Critical
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1), keyCertSign (bit 5), cRLSign (bit 6)	Critical

Table 7.3. Extensions of certSIGN Root CA certificate

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=CA, Path length constraint=none	Critical
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1), keyCertSign (bit 5), cRLSign (bit 6)	Critical
CRL Distribution Points	http://crl.certsign.ro/root.crl ldap://ldap.certsign.ro/C=RO,O=certSIGN,OU=certSIGN Root CA ?certificateRevocationList;binary	Non-critical
Certificate Policies	Policies: 1.3.6.1.4.1.25017.1.1.{2,3,4} CPS: http://www.certsign.ro/repository	Non-critical

Table 7.4. Extensions of Subordinated Authorities certificates (Classes 2-4)

7.1.2.2 Server authentication certificates

Certificates for Web servers' authentication may contain extension from Table 7.5.

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type = End Entity, Path length constraint=none	Critical
Key Usage	digitalSignature (bit 0), keyEncipherment (bit 2)	Critical

ExtendedKeyUsage	serverAuth, clientAuth	Non-critical
Netscape Cert Type	SSLServer (bit 1)	Non-critical
Subject Alternative Name	DNS.1: Full DNS service name	Non-critical
CRL Distribution Points	http://crl.certsign.ro/enterprise.crl ldap://ldap.certsign.ro/CN=certSIGN Enterprise CA Class 3,OU=certSIGN Enterprise CA Class 3,O=certSIGN,C=RO?certificateRevocationList;binary	Non-critical
Authority Info Access	OCSP: http://ocsp.certsign.ro	Non-critical
Certificate Policies	Policies: 1.3.6.1.4.1.25017.1.1.3 CPS: http://www.certsign.ro/repository	Non-critical

Table 7.5. Server authentication certificate extensions

7.1.2.3 Code signing certificates

Certificates for code signing may contain extensions specified in Table 7.6.

Extension	Value or Value constraint	Extension Status
Basic Constraints	Subject type = End Entity, Path length constraint=none	Critical
Key Usage	digital signature (bit 0), non-repudiation (bit 1)	Critical
Extended Key Usage	codeSigning	Non-critical
Netscape Cert Type	ObjectSigning (bit 3)	Non-critical
Subject Alternative Name	RFC822 Name (ex. customer@somewhere-in-world.com)	Non-critical
CRL Distribution Points	http://crl.certsign.ro/enterprise.crl ldap://ldap.certsign.ro/CN=certSIGN Enterprise CA Class 3,OU=certSIGN Enterprise CA Class 3,O=certSIGN,C=RO?certificateRevocationList;binary	Non-critical
Authority Info Access	OCSP: http://ocsp.certsign.ro	Non-critical
Certificate Policies	Policies: 1.3.6.1.4.1.25017.1.1.3 CPS: http://www.certsign.ro/repository	Non-critical

Table 7.6. Code signing certificate extension

7.1.2.4 Private or legal entities certificates

Certificates issued to private or legal Subscribers (including encryption file system – EFS certificates, smartcard logon certificates, electronic data interchange (EDI) certificates, certificates qualified in the meaning of RFC 3039 standard) may contain extensions specified in Table 7.7.

Extension	Value or Value Constraint	Extension status
-----------	---------------------------	------------------

Basic Constraints	Subject type = End Entity, Path length constraint=none	Critical
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1), keyEncipherment (bit 2) dataEncipherment (bit 3), keyAgreement (bit 4)	Critical
Extended Key Usage	clientAuth, emailProtection, EncryptedFileSystem, SmartCardLogon	Non-critical
NetscapeCertType	SSLClient (bit 0), S/MIME (bit 2)	Non-critical
Subject Alternative Name	RFC822 Name: customer@somewhere-in-world.com , *UPN	Non-critical
CRL Distribution Points	dependant on issuing CA-see the other profiles ldap://ldap.certSIGN.ro/C=RO,O=certSIGN,OU=certSIGN Class{2,3,4}?certificateRevocationList;binary	Non-critical
Authority Info Access	OCSP: http://ocsp.certSIGN.ro	Non-critical
Certificate Policies	Politicie:1.3.6.1.4.1.25017.1.1.{2,3,4} CPS: http://www.certSIGN.ro/repository itu-t(0).identified-organization(4).etsi(0).qualified-certificate-policies(1456).policy-identifiers(1). qcp-public-with-sscd (1) – in case of qualified certificates	Non-critical

Table 7.7. Private or legal entities certificates extensions

7.1.2.5 Virtual Private Network (VPN) certificates

Certificates for creation of Virtual Private Network (VPN) may contain extensions specified in Table 7.8.

Extension	Value or Value Constraint	Extension status
Basic Constraints	Subject type = End Entity, Path length constraint=none	Critical
Key Usage	digitalSignature (bit 0), keyEncipherment (bit 2)	Critical
Extended Key Usage	IpsecUser, IpsecTunnel, IpsecEndSystem	Non-critical
Subject Alternative Name	DNS: full VPN router domain name (FQDN) IP: VPN router IP address	Non-critical
CRL Distribution Points	http://crl.certsign.ro/enterprise.crl ldap://ldap.certSIGN.ro/CN=certSIGN Enterprise CA Class 3,OU=certSIGN Enterprise CA Class 3,O=certSIGN,C=RO?certificateRevocationList;binary	Non-critical
Authority Info Access	OCSP: http://ocsp.certSIGN.ro	Non-critical
Certificate Policies	Politicile:1.3.6.1.4.1.25017.1.1.3 CPS: http://www.certSIGN.ro/repository	Non-critical

Table 7.8. VPN certificates extensions

7.1.2.6 Cross-certification and non-repudiation certificates

Cross-certification and non-repudiation certificates may contain extension specified in Table 7.9, 7.10 and 7.11.

Extension	Value or Value constraint	Extension status
-----------	---------------------------	------------------

Basic Constraints	Subject type=CA, Path length constraint={none,1,2,...}	Critical
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1), keyCertSign (bit 5) cRLSign (bit 6)	Critical
CRL Distribution Points	URI: http://crl.certSIGN.ro/class4.crl ldap://ldap.certSIGN.ro/C=RO,O=certSIGN,OU=certSIGN Class 4?certificateRevocationList;binary	Non-critical
Authority Info Access	OCSP: http://ocsp.certSIGN.ro	Non-critical
Certificate Policies	Politice:1.3.6.1.4.1.25017.1.1.4 CPS: http://www.certSIGN.ro/repository	Non-critical

Table 7.9. Cross-certification certificates extensions

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=End Entity, Path length constraint=none	Critical
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1)	Critical
Extended Key Usage	OCSPSigning	Non-critical
OCSPNoCheck	-	Non-critical
Certificate Policies	Politice:1.3.6.1.4.1.25017.1.1.4 CPS: http://www.certSIGN.ro/repository	Non-critical

Table 7.10. OCSP Authority certificates' extensions

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=EndEntity, Path length constraint=none	Critical
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1)	Critical
Extended Key Usage	timeStamping	Non-critical
CRL Distribution Points	URI: http://crl.certSIGN.ro/class4.crl ldap://ldap.certSIGN.ro/C=RO,O=certSIGN,OU=certSIGN Class 4?certificateRevocationList;binary	Non-critical
Authority Info Access	OCSP: http://ocsp.certSIGN.ro	Non-critical
Certificate Policies	Politice:1.3.6.1.4.1.25017.1.1.4 CPS: http://www.certSIGN.ro/repository	Non-critical

Table 7.11. Time Stamp Authority certificates extensions

Besides the extensions mentioned above, upon the client's request the certificates may include also particular extensions, under the conditions settled on concluding the contract.

7.1.3 Electronic signature algorithm identifier

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, RSA algorithm, in combination with SHA-1 function is used.

7.1.4 Electronic signature field

The value of the field **signatureValue** is a result of execution of cryptographic hash function algorithm for all fields of a certificate (**tbscertificate**) and signing algorithm of the obtained digest with a private key of the authority.

7.2 CRL profile

Certificate Revocation List (CRL) consists of three fields. The first field (**tbscertList**) contains information about revoked certificates, the second and the third field -**signatureAlgorithm** and **signatureValue** contain information about respectively: the identifier of the algorithm used for list signing, and electronic signature of the Certification Authority.

The field of **tbscertList** is the sequence of mandatory and optional fields. Mandatory fields identify CRL issuer, while optional fields contain information about revoked certificates and CRL extensions.

The following fields are the contents of mandatory and optional fields of CRL:

- **Version:** CRL format version,
- **signature:** contains identifier of the algorithm used by a Certification authority to sign CRL; certSIGN authorities sign CRLs by means of **sha1WithRSAEncryption** algorithm,
- **Issuer:** name of the Certification Authority issuing CRL; every authority of certSIGN issues its own Certificate Revocation List; this requirement applies to the following authorities: **certSIGN Demo CA Class 1**, **certSIGN CA Class 2**, **certSIGN Qualified CA Class 3**, **certSIGN Enterprise CA Class 3** and **certSIGN Non-Repudiation CA Class 4**,

- **ThisUpdate**: CRL publication date,
- **NextUpdate**: announcement of the date of the next CRL publication; if the field is present, its value describes the maximum date for CRL update,
- **Revokedcertificates**: : the list of revoked certificates (the field is empty in the case of lack of revoked certificates); the information consist of three sub-fields:
 - usercertificates** – serial number of a revoked certificate;
 - revocationDate** – date of the certificate revocation;
 - crIEntryExtensions** – contains additional information about revoked certificates – optional.
- **crIExtensions**: extended information about Certificate Revocation List (optional field). Among numerous extensions, the most important are the following ones: **AuthorityKeyIdentifier** (see also Chapter 7.1.1.2) allowing identification of a public key corresponding to a private key used for list signing, and **cRLNumber**, containing monotonically increased serial number of the lists issued by a Certification Authority (by means of this extension, a Subscriber is able to define when a specific CRL replaced another list).

7.2.1 Supported CRL entry extension

Function and meaning of extensions are the same as for certificate extensions (see Chapter 7.1.1.2). CRL entry extensions (**crIEntryExtensions**) supported by certSIGN contain the following fields:

- **ReasonCode**: code of the reason for revocation. This field is **non-critical**, allowing determination of the certificate revocation reason. The following reasons of certificate revocation are allowed:
 - unspecified** – not specified;
 - keyCompromise** – key compromising;
 - cACompromise** – Certification Authority key compromising;

affiliationChanged – Subscriber's data modification;

superseded – certificate renewal;

cessationOfOperation – cessation of certificate usage;

removeFromCRL – certificate removal from CRL.

7.2.2 Revoked certificate and CRL

Revoked certificates are kept for a period of 15 years, according to table 4.4. Revoked certificates are taken out from the certificate revocation list upon their expiry.

7.3 OCSP confirmation response 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, generated exclusively for this purpose.

OCSP server certificate has to contain the extension `extKeyUsage`, described in RFC 3280.

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 2560. 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.

When the OCSP answer contains an error code (message), the answer is not digitally signed (RFC 2560)

7.3.1 Version number

OCSP server operating within certSIGN issues certificate status confirmations in accordance with the RFC 2560. The only allowable value of the version number is 0 (it is an equivalent of v1 version).

7.3.2 Certificate status information

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

7.3.3 Supported standard extensions

In compliance with RFC 2560, 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 CPS Management

Every version of CPS is in force (has a **valid** status) up to the moment of publication and approval of its new version (see Chapter 8.3). A new version is developed by certSIGN 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. A committee including the general director, the deputy director, the technical departments' managers and the business development department manager are liable for the final form of the CPS. The manager of the department providing the certificate services is liable for maintaining the CPS. After completion of the approval procedure, a new version of CPS sent to the Settlement and Supervision Authority and then within 10 days it is published and labeled as **valid**. Rules and requirements concerning CPS management also govern Certification Policy management.

Subscribers have to comply only with the currently applicable Certification Policy and CPS.

8.1 CPS changes procedure

Modification to CPS may be a result of observed errors, its update and suggestions from the interested parties. Modification proposals have to be submitted by regular mail or electronic mail on certSIGN address. Suggestions have to describe the necessary modifications, their reasons and mean of contact the person requesting modification

After introduction of a modification, the issuance date of CPS or Certification Policy is updated and the serial number of the document version is modified.

Introduced modification may be generally divided into two categories: one that does not require notification of Subscribers and the one that requires (usually in advance) notification of Subscribers. The first one includes emergency or non-essential modifications.

Certification policies identifiers used by the issuing authorities can be modified as well as a result of the following changes:

- extension of a certificate user group for areas such as electronic payment systems, information interchange between banks, etc,

- introduction of new types of certificates,
- allowance within the system of the cross-certification between authorities issuing certificates,
- significant modification to content and interpretation of certificate and CRL fields, e.g. modification of fields meaning non-critical/critical.

8.2 Publication and notification procedures

A copy of CPS is available in an electronic form on the Web site at the address: <http://www.certSIGN.ro/repository> or e-mail at the address: office@certSIGN.ro. Three versions (is applicable) of CPS are always available at the Repository and via the email: the currently applicable version, the previous version and the version under approval.

8.3 CPS Approval Procedures

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 Subscribers of certSIGN, and the status of the version is changed into **valid**.

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.

Annex 1: Glossary

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 or suspended 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 update – prior to expiration of a certificate, CA may update it (or renew it), confirming validity of the same key pair for the succeeding period of validity (in accordance to the Certification Policy).

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 Subscriber 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 Subscriber and used only by that subscriber. 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 Subscriber or a Relying Party trusts. A certificate of this authority is the first certificate in each certification path created by a Subscriber 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 Subscriber 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 Subscriber 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 Subscriber’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 Subscriber’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 cryptography 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).

Revoked certificate – public key certificate placed on Certificate Revocation List.

Requester – Subscriber 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 Subscribers.

Shared secret holder – authorized holder of an electronic card, used for storage of the shared secret.

Subscriber – entity (private person or legal entity, organizational unit not having a legal identity, hardware device owned by these entities or persons) that: (1) is the subject of the certificate issued to this entity, (2) possesses a private key associated with the certificate issued to this entity and (3) does not issue certificates to other 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.

Subscriber's Sponsor – institution which on behalf of the Subscriber supports financially certification services provided by the authority issuing certificates. The sponsor is the owner of the certificate.

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 Subscriber (subject of the certificate) and (3) it has not been revoked.

Annex 2: Acronyms and definitions

CA	certification Authority
CP	certification Policy
CPS	certification Practice Statement
CRL	certificate Revocation List
DN	Distinguished Name
DSCS	Secured Device for Signature Creation
LRA	Local Registration Authority
OSCP	On-line certificate Status Protocol
PKI	Public Key Infrastructure
PSE	Personal Security Environment
RSA	Rivest, Shamir, Adleman asymmetric cryptographic algorithm
TTP	Trusted Third Party

Annex 3

Standards and international recommendations referred to in the document

Internet Engineering Task Force Recommendations- <http://www.ietf.org/rfc.html>.

RFC 822 "Standard for the format of ARPA Internet text messages"

RFC 1778 „The String Representation of Standard Attribute Syntaxes”

RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification

Practices Framework”

RFC 2560 „X.509 Internet Public Key Infrastructure Online certificate Status Protocol – OCSP”

RFC 3039 “Internet X.509 Public Key Infrastructure - Qualified certificates Profile “

RFC 3161 „Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)”

RFC 3280 “Internet X.509 Public Key Infrastructure certificate and certificate Revocation List (CRL) Profile”

Recommendation International Telecommunication Union, series X

<http://www.itu.int/rec/T-REC-X/en>

X.500 „Recommendation and International Standard that introduces the concepts of the Directory „

X.501 „Recommendation and International Standard that provides a number of different models for the Directory as a framework for the other ITU-T Recommendations în the X.500 series”

ITU-T X.509 v.3 „This Recommendation | International Standard defines a framework for public-key certificates and attribute certificates”

X.520 „This Recommendation | International Standard defines a number of attribute types and matching rules which may be found useful across a range of applications of the Directory”

PKCS standards of RSA - <http://www.rsasecurity.com/rsalabs/node.asp?id=2124>

PKCS#7 Cryptographic Message Syntax Standard

PKCS#10 certification Request Syntax Standard

PKCS#12 Personal Information Exchange Syntax Standard

ISO standards - www.iso.org

ISO/IEC 11770-1 – Key management

ISO/IEC 13335 - Guidelines for Management of IT Security

ISO/IEC 17799 - Code of Practice for Information Security Management.

FIPS standards - <http://csrc.nist.gov/publications/fips/index.html>

FIPS 112 - Password usage

FIPS 140 – 2 Security Requirements for Cryptographic Modules

Common Criteria - <http://www.commoncriteriaportal.org/>

ETSI standards - <http://www.etsi.org/>

ETSI TS 101456 (Policy requirements for qualified certificates issuing Certification Authorities)

CEN standards - <http://www.cenorm.be/cenorm/index.htm>

CEN CWA 14167 - Security Requirements for Trustworthy Systems Managing certificates for Electronic Signatures

