Certificate Practice Statement

SSC GDL CA

Version 4.10

2015

Revision history

Document version	Date	Revision details
4.3	04/15/13	New publication
4.4	04/29/13	Editorial revision
4.5.	05/29/13	OR revised version
4.6	06/21/13	ER recommendations
4.7	04/22/14	Amended with EV CA
4.8	08/01/14	Updated OID table and section 1.2
4.9	02/16/15	Amended section 3
4.10	04/1/15	Editorial revision and section 4 update

Table of Contents

1 INTRODUCTION....9
1.1 Overview....9
1.2 Document name and identification....10
1.3 PKI participants....12
1.3.1 Certification authorities....12
1.3.2 Registration authorities....13
1.3.3 Subscribers and Subjects....13
1.3.4 Relying Parties....14
1.3.5 Other participants....14
1.4 Certificate usage....15
1.4.1 Appropriate certificate uses....16
1.4.2 Prohibited certificate uses....17
1.5 Policy administration....17
1.5.1 Organization administering the document....17
1.5.2 Contact person....17
1.5.3 Person determining CPS suitability for the policy....18
1.5.4 CPS approval procedures....18
1.6 Definitions and Acronyms....18
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES....19
2.1 Repositories....19
2.2 Publication of certification information....19
2.3 Time or frequency of publication....19
2.4 Access controls on repositories....20
3 IDENTIFICATION AND AUTHENTICATION....21
3.1 Naming....21
3.1.1 Types of names....21
3.1.2 Need for names to be meaningful....21
3.1.3 Anonymity or pseudonymity of subscribers....22
3.1.4 Rules for interpreting various name forms....22
3.1.5 Uniqueness of names....22
3.1.6 Recognition, authentication, and role of trademarks....22
3.2 Initial identity validation....22
3.2.1 Method to prove possession of private key....24
3.2.2 Authentication of organization identity....24
3.2.3 Authentication of individual identity....24
3.2.4 Device authentication....25
3.2.5 Service authentication....25
3.2.6 Non-verified subscriber information....26
3.2.7 Validation of authority....26
3.2.8 Criteria for interoperation....26
3.3 Identification and authentication for re-key requests....26
3.3.1 Identification and authentication for routine re-key....26
3.3.2 Identification and authentication for re-key after revocation....27
3.4 Identification and authentication for revocation request....27

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 28
4.1 Certificate Application.....30
4.1.1 Who can submit a certificate application.....33
4.1.2 Enrollment process and responsibilities.....33
4.2 Certificate application processing.....34
4.2.1 Performing identification and authentication functions.....34
4.2.2 Approval or rejection of certificate applications.....34
4.2.3 Time to process certificate applications.....34
4.3 Certificate issuance 34
4.3.1 CA actions during certificate issuance.....34
4.3.2 Notification to subscriber by the CA of issuance of certificate 36
4.4 Certificate acceptance.....37
4.4.1 Conduct constituting certificate acceptance.....37
4.4.2 Publication of the certificate by the CA.....37
4.4.3 Notification of certificate issuance by the CA to other entities.....37
4.5 Key pair and certificate usage.....37
4.5.1 Subscriber private key and certificate usage.....37
4.5.2 Relying party public key and certificate usage.....38
4.6 Certificate renewal.....38
4.6.1 Circumstance for certificate renewal.....38
4.6.2 Who may request renewal.....38
4.6.3 Processing certificate renewal requests.....38
4.6.4 Notification of new certificate issuance to subscriber.....38
4.6.5 Conduct constituting acceptance of a renewal certificate.....39
4.6.6 Publication of the renewal certificate by the CA.....39
4.6.7 Notification of certificate issuance by the CA to other entities.....39
4.7 Certificate re-key.....39
4.7.1 Circumstance for certificate re-key.....39
4.7.2 Who may request certification of a new public key.....39
4.7.3 Processing certificate re-keying requests 40
4.7.4 Notification of new certificate issuance to subscriber.....40
4.7.5 Conduct constituting acceptance of a re-keyed certificate.....40
4.7.6 Publication of the re-keyed certificate by the CA.....40
4.7.7 Notification of certificate issuance by the CA to other entities.....40
4.8 Certificate modification.....40
4.8.1 Circumstance for certificate modification.....41
4.8.2 Who may request certificate modification.....41
4.8.3 Processing certificate modification requests.....41
4.8.4 Notification of new certificate issuance to subscriber.....41
4.8.5 Conduct constituting acceptance of modified certificate.....41
4.8.6 Publication of the modified certificate by the CA.....42
4.8.7 Notification of certificate issuance by the CA to other entities.....42
4.9 Certificate revocation and suspension.....42
4.9.1 Circumstances for revocation.....43
4.9.2 Who can request revocation.....45
4.9.3 Procedure for revocation request.....45
4.9.4 Revocation request grace period.....45

4.9.5 Time within which CA must process the revocation request....45
4.9.6 Revocation checking requirement for relying parties....46
4.9.7 CRL issuance frequency....46
4.9.8 Maximum latency for CRLs....46
4.9.9 On-line revocation/status checking availability....46
4.9.10 On-line revocation/status checking requirements....46
4.9.11 Other forms of revocation advertisements available....47
4.9.12 Special requirements re key compromise....47
4.9.13 Circumstances for suspension....47
4.9.14 Who can request suspension....47
4.9.15 Procedure for suspension request....47
4.9.16 Limits on suspension period....47
4.10 Certificate status services....47
4.10.1 Operational characteristics....48
4.10.2 Service availability....48
4.10.3 Optional features....48
4.11 End of subscription....48
4.12 Key escrow and recovery....48
4.12.1 Key escrow and recovery policy and practices....48
4.12.2 Session key encapsulation and recovery policy and practices....48
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS....49
5.1 Physical controls....49
5.1.1 Site location and construction....49
5.1.2 Physical access....50
5.1.3 Power and air conditioning....50
5.1.4 Water exposures....50
5.1.5 Fire prevention and protection....50
5.1.6 Media storage....50
5.1.7 Waste disposal....51
5.1.8 Off-site backup....51
5.2 Procedural controls....51
5.2.1 Trusted roles....51
5.2.2 Number of persons required per task....52
5.2.3 Identification and authentication for each role....52
5.2.4 Roles requiring separation of duties....52
5.3 Personnel controls....53
5.3.1 Qualifications, experience, and clearance requirements....53
5.3.2 Background check procedures....53
5.3.3 Training requirements....54
5.3.4 Retraining frequency and requirements....54
5.3.5 Job rotation frequency and sequence....54
5.3.6 Sanctions for unauthorized actions....55
5.3.7 Independent contractor requirements....55
5.3.8 Documentation supplied to personnel....55
5.4 Audit logging procedures....55
5.4.1 Types of events recorded....55
5.4.2 Frequency of processing log....56

5.4.3 Retention period for audit log....56
5.4.4 Protection of audit log....56
5.4.5 Audit log backup procedures....56
5.4.6 Audit collection system (internal vs. External)....56
5.4.7 Notification to event-causing subject....56
5.4.8 Vulnerability assessments....57
5.5 Records archival....57
5.5.1 Types of records archived....57
5.5.2 Retention period for archive....57
5.5.3 Protection of archive....57
5.5.4 Archive backup procedures....57
5.5.5 Requirements for time-stamping of records....57
5.5.6 Archive collection system (internal or external)....58
5.5.7 Procedures to obtain and verify archive information....58
5.6 Key changeover....58
5.7 Compromise and disaster recovery....58
5.7.1 Incident and compromise handling procedures....58
5.7.2 Computing resources, software, and/or data are corrupted....59
5.7.3 Entity private key compromise procedures....59
5.7.4 Business continuity capabilities after a disaster....59
5.8 CA or RA termination....59
6 TECHNICAL SECURITY CONTROLS....61
6.1 Key pair generation and installation....61
6.1.1 Key pair generation....61
6.1.2 Private key delivery to subscriber....61
6.1.3 Public key delivery to certificate issuer....62
6.1.4 CA public key delivery to relying parties....62
6.1.5 Key sizes....62
6.1.6 Public key parameters generation and quality checking....62
6.1.7 Key usage purposes (as per X.509 v3 key usage field)....63
6.2 Private Key Protection and Cryptographic Module Engineering Controls....63
6.2.1 Cryptographic module standards and controls....63
6.2.2 Private key (n out of m) multi-person control....63
6.2.3 Private key escrow....63
6.2.4 Private key backup....63
6.2.5 Private key archival....64
6.2.6 Private key transfer into or from a cryptographic module....64
6.2.7 Private key storage on cryptographic module....64
6.2.8 Method of activating private key....64
6.2.9 Method of deactivating private key....64
6.2.10 Method of destroying private key....65
6.2.11 Cryptographic Module Rating....65
6.3 Other aspects of key pair management....65
6.3.1 Public key archival....65
6.3.2 Certificate operational periods and key pair usage periods....65
6.4 Activation data....65
6.4.1 Activation data generation and installation....65

6.4.2 Activation data protection....65
6.4.3 Other aspects of activation data....66
6.5 Computer security controls....66
6.5.1 Specific computer security technical requirements....66
6.5.2 Computer security rating....67
6.6 Life cycle technical controls....67
6.6.1 System development controls....67
6.6.2 Security management controls....67
6.6.3 Life cycle security controls....67
6.7 Network security controls....68
6.8 Time-stamping....68
7 CERTIFICATE, CRL, AND OCSP PROFILES....69
7.1 Certificate profile....69
7.1.1 Version number(s)....69
7.1.2 Certificate extensions....69
7.1.3 Algorithm object identifiers....70
7.1.4 Name forms....70
7.1.5 Name constraints....70
7.1.6 Certificate policy object identifier....70
7.1.7 Usage of Policy Constraints extension....70
7.1.8 Policy qualifiers syntax and semantics....70
7.1.9 Processing semantics for the critical Certificate Policies extension....70
7.2 CRL Profile....71
7.2.1 Version number(s)....71
7.2.2 CRL and CRL entry extensions....71
7.3 OCSP profile....71
7.3.1 Version number(s)....71
7.3.2 OCSP extensions....71
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS....72
8.1 Frequency or circumstances of assessment....72
8.2 Identity/qualifications of assessor....72
8.3 Assessor's relationship to assessed entity....72
8.4 Topics covered by assessment....72
8.5 Actions taken as a result of deficiency....72
8.6 Communication of results....73
9 OTHER BUSINESS AND LEGAL MATTERS....74
9.1 Fees....74
9.1.1 Certificate issuance or renewal fees....74
9.1.2 Certificate access fees....74
9.1.3 Revocation or status information access fees....74
9.1.4 Fees for other services....75
9.1.5 Refund policy....75
9.2 Financial responsibility....75
9.2.1 Insurance coverage....75
9.2.2 Other assets....75
9.2.3 Insurance or warranty coverage for end-entities....75
9.3 Confidentiality of business information....75

9.3.1 Scope of confidential information....76
9.3.2 Information not within the scope of confidential information....76
9.3.3 Responsibility to protect confidential information....76
9.4 Privacy of personal information....76
9.4.1 Privacy plan....77
9.4.2 Information treated as private....77
9.4.3 Information not deemed private....77
9.4.4 Responsibility to protect private information....77
9.4.5 Notice and consent to use private information....77
9.4.6 Disclosure pursuant to judicial or administrative process....77
9.4.7 Other information disclosure circumstances....77
9.5 Intellectual property rights....78
9.5.1 Certificates and CRLs....78
9.5.2 CP/CPS....78
9.5.3 Trademarks....78
9.5.4 Signature creation data....78
9.6 Representations and warranties....78
9.6.1 CA representations and warranties....79
9.6.2 RA representations and warranties....79
9.6.3 Subscriber representations and warranties....79
9.6.4 Relying party representations and warranties....79
9.6.5 Representations and warranties of other participants....79
9.7 Disclaimers of warranties....79
9.8 Limitations of liability....79
9.9 Indemnities....80
9.10 Term and termination....80
9.10.1 Term....80
9.10.2 Termination....80
9.10.3 Effect of termination and survival....80
9.11 Individual notices and communications with participants....80
9.12 Amendments....80
9.12.1 Procedure for amendment....80
9.12.2 Notification mechanism and period....80
9.12.3 Circumstances under which OID must be changed....81
9.13 Dispute resolution provisions....81
9.14 Governing law....81
9.15 Compliance with applicable law....81
9.16 Miscellaneous provisions....81
9.16.1 Entire agreement....81
9.16.2 Assignment....81
9.16.3 Severability....81
9.16.4 Enforcement (attorneys' fees and waiver of rights)....82
9.16.5 Force Majeure....82
9.17 Other provisions....82
10 REFERENCES....83
10.1 Normative References....83
10.2 Informative References....83

1 INTRODUCTION

The SSC GDL Certification Authority (CA) provides and manages certificates used for various applications. SSC GDL CA use a Public Key Infrastructure (PKI) for the management of certificates.

Glossary of terms used in the present document is mainly based on [RFC3647] .

The words "MUST" (“REQUIRED”, “SHALL”), “MUST NOT” (“SHALL NOT”), “SHOULD” (“RECOMMENDED”), 'SHOULD NOT” (“NOT RECOMMENDED”), “MAY” (“OPTIONAL”) , should be interpreted as described in [RFC2119].

Depending on the context “*No stipulation”* in this document should be read as one of following:

a) *according to the SSC GDL CA CP*;

b) *according to an applicable normative publication listed in this document (see section 10)*;

c) *according to CA's internal document*.

The expression "SSC GDL CA" is used to describe the CA, whose activity correspond to the conditions referred to in [SSC_CP].

1.1 Overview

The practices adopted in this document cover a number of core services, each service having defined functions to meet security standards for achieving trustworthy status. In the context of this Certificate Practice Statement (CPS), SSC GDL CA provides these core services:

- Root CA Service;
- Issuing CA Service including:

- ✔ Registration Service – to verify the identity of a Subject;
- ✔ Certificate Generation Service – to create certificates;
- ✔ Dissemination Service – to deliver certificates and other information to Subjects;
- ✔ Revocation Management Service – to process revocation requests;
- ✔ Revocation Status Service – to provide certificate status information to relying parties;

➢ SSC GDL CA also provides additional services:

- ✔ Subject Device Provision Service – to prepare a Signature-Creation Device (SSCD);
- ✔ Time-Stamping Service – to generate time stamp tokens.
- ✔ On-line Subject authentication service;
- ✔ Customer Support Service[1];
- ✔ Signature creation Software as a Service (SaaS);
- ✔ Signature verification WEB application.

This CPS can be used to determine the applicability of certificates and reliability of the certificate authority.

SSC GDL CA provide the functionality that meet the security requirements specified in [SSC_CP].

Although the CPS is not intended to specify all types of certificates it issues, the aspects related to issuing Qualified Certificates have been specified in a way to demonstrate the compliance with the requirements of Annex I and Annex II of [Dir1999/93/EC].

1.2 Document name and identification

SSC GDL CA Certificate Practice Statement is structured according to [SSC_CP]. The CPS is referenced by following generic OIDs:

IANA: 1.3.6.1.4.1.22501.0.2

National OID Registry[2]: 2.16.440.1.4.30003763.0.2

OIDs of specific CPS versions are identified by extending the generic reference by version and modification numbers, e.g.:

1 Includes live chat and help desk services
2 To be approved by national authorities.

IANA: 1.3.6.1.4.1.22501.0.2.v.m

National OID Registry: 2.16.440.1.4.30003763.0.2.v.m

All certificates issued under this CPS contain a registered CP object identifier (OID). Some of these OIDs and corresponding policy requirements are managed by third parties that SSC GDL CA has entered either explicit or implicit agreement with. Although this CPS addresses the essential part of all integrated third party policies, however while evaluating applicability of a specific certificate, the priority should be given to the policy whose OID has been explicitly referenced in the certificate. For the usability purposes this CPS doesn't repeat the requirements or provisions of these third party policies, rather their respective OIDs are presented in the table below. Certificates issued in accordance with this CPS assert at least one of the following OIDs in the certificate policy extension:

Policy	**OID**
NCP	0.4.0.2042.1.1
NCP+	0.4.0.2042.1.2
EVCP	0.4.0.2042.1.4
EVCP+	0.4.0.2042.1.5
DVCP	0.4.0.2042.1.6
OVCP	0.4.0.2042.1.7
QCP + SSCD	0.4.0.1456.1.1
QCP	0.4.0.1456.1.2
CAB Forum EV SSL	2.23.140.1.1
CAB Forum BR (*Subject* identity information asserted)	2.23.140.1.2.2
CAB Forum BR (No *Subject* identity information asserted)	2.23.140.1.2.1
anyPolicy	2.5.29.32.0
ETSI TS 102 023 Baseline TSA policy	0.4.0.2023.1.1
LTV time stamp for *Qualified signature* (where, v - version #, m – modification #)	1.3.6.1.4.1.22501.0.6.v.m 2.16.440.1.4.30003763.0.6.v.m
SSC GDL CA Certificate Policy (Generic Reference OID)	1.3.6.1.4.1.22501.0.1 2.16.440.1.4.30003763.0.1
SSC GDL CA CP	1.3.6.1.4.1.22501.0.1.v.m

Policy	OID
(Specific Reference OID, where, v – version number, m – modification number)	2.16.440.1.4.30003763.0.1.v.m
SSC GDL CA CPS (Generic Reference OID)	1.3.6.1.4.1.22501.0.2 2.16.440.1.4.30003763.0.2
SSC GDL CA CPS (Specific Reference OID, v – version number, m – modification number)	1.3.6.1.4.1.22501.0.2.v.m 2.16.440.1.4.30003763.0.2.v.m
SSC_Authentication_Only	1.3.6.1.4.1.22501.9.6.2.0 2.16.440.1.4.30003763.9.6.2.0
SSC_AIO	1.3.6.1.4.1.22501.9.8.1.0 2.16.440.1.4.30003763.9.8.1.0

Some parts of this document are left for compatibility, although are not directly applicable for the services provided under this CPS.

Interoperation with CAs that issue certificates under different policies may be achieved through *Trust Lists* (TL), policy mapping and cross-certification through the SSC GDL CA hierarchy. This CA service is part of Microsoft Windows Trust Program, Lithuanian and European *Trust List*[3], Google Chrome Root Certificate Program, Opera Software, Adobe Acrobat Trust List[4], Mozilla CA Certificate Inclusion Program[5], Apple iOS Root Certificate Program[6], and Android Root Certificate[7] Programs.

1.3 PKI participants

This section describes the entities that performs the roles of participants within the PKI. In case if SSC GDL CA involves any third party in provisioning of its services the CA has a properly documented agreement. Dependent of nature of the outsourced service the third party may be disclosed in SSC_PDS.

1.3.1 Certification authorities

Within SSC PKI there are two general types of CAs: Root and Issuing CAs. Currently, the

3 https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf
4 Pending approval
5 Pending approval
6 Pending approval
7 Pending approval

PKI hierarchy consists of the following CAs:

Root CA	Issuing CA name	Description
Root A	SSC GDL Class 1-2 CA	Certificates for unverified Subjects and non qualified certificates.
	SSC GDL Class 2-4 QCA	Qualified el. signature certificates issued to Public.
Root B	SSC GDL NH CA	All types of Device\Service certificates
	SSC GDL EV CA	EV SSL certificates
VS Root	SSC GDL VS Class 2-4 QCA	Qualified el. signature certificates issued to Public Sector *Subjects*.

Root CAs. Assure trustworthiness of issuing CAs. Root CAs issue the certificates only to CAs which meet the requirements of the associated CP and are responsible for management of these CA and implementation of these practices.

Issuing CAs. Issue certificates only to *Subscribers* and provide other related services. SSC GDL CA is managed according to [Dir1999/93/EC] and [LT-ES-LAW].

In the event when any of the CAs listed above in the table become a *Subject* of a third party issued certificate, the CA shall disclose all cross signing certificates.

1.3.2 Registration authorities

SSC PKI currently operates a RA which is a wholly owned division of SSC. Besides establishing enrollment procedures, identity verification, identification and authentication of applicants the RA also conveys the Root and CA public key certificates and performs other functions detailed in this CPS.

1.3.3 *Subscribers* and *Subjects*

In some situations the party requesting (e.g. an organization) a certificate – *Subscriber* - is different from the individual to whom the certificate applies - *Subject*. A *Subscriber* may represent several *Subjects*, which are the entities issued a certificate in accordance with this CPS, and whose public key and distinguished name are certified in the certificate.

The *Subscriber* bears responsibility towards SSC GDL CA for the use of the private key associated with the public key certificate but the *Subject* is the individual entity that is authenticated by the private key and that has control over its use. If certificate issued to an

individual for his/her own use, the S*ubscriber* and *Subject* is the same entity.

The CA MAY issue EV Certificates to Private Organization, Government Entity, Business Entity and Non-Commercial Entity *Subjects* in accordance with the requirements of [CABF-EV].

Each *Subscriber* MUST sign an agreement prior to the time of issuance of the certificate.

1.3.4 Relying Parties

The legal or physical persons that trust SSC GDL CA issued certificates are *Relying parties*[8]. To determine the validity of a certificate, the relying party has to contact the certificate status service as described in [SSCGDLRPA].

1.3.5 Other participants

The following roles are identified for the issuance of EVCP and EVCP+ certificates:

Certificate Requester: a natural person who has express authority to represent the Applicant, or a third party that completes and submits an EV Certificate Request on behalf of the Applicant;

Certificate Approver: is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters;

Contract Signer: a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements;

Applicant Representative: a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who

8 *'relying party' means a natural or legal person that relies upon an electronic identification or a trust service*, REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

has authority on behalf of the Applicant to acknowledge and agree to the Terms of Use;

Subcontractor – a hosting service provider.

Application Software Supplier: a natural or legal entity with whom the SSC GDL CA has entered into a contract for inclusion of its (Root CA and/or Issuing CA) Certificate in software distributed by such Application Software Supplier.

The *Applicant* MAY authorize one individual to occupy two or more of these roles.

1.4 Certificate usage

Depending on the level of identity validation and security requirements to the associated key material the certificates issued under this CPS may be grouped into following classes:

Class 1 – The *Subject* of the certificate indicates a *Name* that is not bound to any person whose identity has been validated. Only existence of a communication resource (e.g. an email address, a phone number, etc.) is guaranteed. The *Subject* of the certificate can be a human, an organization, a device or a service.

Class 2 – The *Subject* of the certificate indicates a *Name* that is bound to the person whose identity has been reliably verified. The *Subject* of the certificate can be a human, an organization, a device or a service.

Class 3 – The *Subject* of the certificate indicates a *Name* that is bound to the person whose identity has been reliably verified. The associated private key is stored in a secure device under the sole control of the *Subject*. The *Subject* of the certificate can be a human, an organization, a device or a service.

Class 4 – The *Subject* of the certificate indicates a *Name* and an associated biometric data that are bound to a person whose identity has been reliably verified. The associated private key is stored in a secure device under the sole control of the *Subject*. The *Subject* of the certificate can be a human only.

The CA issues specific types of certificates that are based on the policies defined in third

party documents as reference certificate policies or frameworks (e.g. [CABF-BR], [CABF-EV]). The applicability of these policies to the types of certificates is shown below:

Issuing CA	Referenced Policy				
	QCP[9]/QCP+[10]	NCP[11]/NCP+[12]	EVCP[13]/EVCP+[14]	DVCP[15]	OVCP[16]
SSC GDL Class 1-2 CA	-	+	-	+	-
SSC GDL Class 2-4 QCA	+	-	-	-	+
SSC GDL NH CA	+	-	-	-	+
SSC GDL EV CA	-	-	+	-	-
SSC GDL VS Class 2-4 QCA	+	-	-	-	-

In the context of a specific certificate type, the requirements of the indicated certificate policies[17] assumed to have a default dominance in all cases. Upon request the Issuing CAs provides *certificate users* and *Relying parties* with test certificates and options for certificate checking.

SSC GDL CA conforms to the current versions of the [CABF-BR] and [CABF-EV][18]. In the event of any inconsistency between this CPS and those Guidelines, the Guidelines take precedence over the CPS.

SSC GDL CA also confirms to the current version of [CABF-NCSSR] which has been adopted into internally identified document.

1.4.1 Appropriate certificate uses

For non-repudiation and for encryption/decryption functions SSC GDL CA issues only separate certificates.

A single certificate (SSC_AIO) for both digital signature or authentication can be issued if

9 CP for qualified certificates issued to Public as defined in [ETSI101456].
10 QCP with a SSCD as defined in [ETSI101456].
11 Normalized CP as defined in [ETSITS101042] and provides a level of quality equal to that offered by qualified certificates without being tied to the [Dir1999/93/EC].
12 NCP with a secure device.
13 Extended Validation Certificates Policy (EVCP) for code signing or TLS/SSL certificates as specified in the [CABF-EV].
14 EVCP with a secure device.
15 Domain Validation Certificates Policy (DVCP) for TLS/SSL certificates as specified in the [CABF-BR].
16 Organizational Validation Certificates Policy (OVCP) for TLS/SSL certificates as specified in the [CABF-BR].
17 Applicable policies are: [ETSITS101042] [ETSI101456].
18 Published at http://www.cabforum.org

requested by *Subscribers*.

1.4.2 Prohibited certificate uses

No applications have ever been identified that prohibit use of certificates issued according to this CPS.

SSC GDL CA certificates are not designed, intended, or authorized for use as control equipment in hazardous environments or for the operation of nuclear facilities, navigation, communication or any other control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

1.5 Policy administration

Revisions to this CPS is available to *Subscribers* and *Relying parties* in the working documents section of the SSC GDL CA Repository before its approved by the authority indicated in section 1.5.3.

SSC GDL CA appreciates and values recommendations and suggestions sent to the email address indicated in section 1.5.1 by filling out the downloadable Template for comments.

1.5.1 Organization administering the document

This CPS is administered by:

Skaitmeninio sertifikavimo centras (SSC)

Jogailos 8, LT-01116, Vilnius, LITHUANIA

Web: http://www.ssc.lt

Email: info@ssc.lt

Fax: +370.700.22715

1.5.2 Contact person

For any questions regarding this document, please contact:

Skaitmeninio sertifikavimo centras (SSC)

Jogailos 8, LT-01116 Vilnius, LITHUANIA

Web: http://www.ssc.lt

Phone: +370.700.22722

Email: info@ssc.lt

Fax: +370.700.22715

1.5.3 Person determining CPS suitability for the policy

Skaitmeninio sertifikavimo centras

Policy Authority

Jogailos 8, LT-01116 Vilnius, LITHUANIA

Phone: +370.700.22722

Fax: +370.700.22715

Email: info@ssc.lt

1.5.4 CPS approval procedures

Any revisions of this CPS must be approved by the SSC GDL CA Policy Authority. Projected amendments may be available in the SSC GDL CA repository for public comments. Depending on the revision circumstances the PA determines if the revised CPS require any change in the OID of a certificate issued pursuant to this CPS.

1.6 Definitions and Acronyms

For the purposes of the present document, the terms and definitions given in [CWA14167-1] , [ETSITS101042], [ETSI101456], [ETSI102023], [CABF-BR] and [CABF-EV] apply.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Repository https://gdl.repository.ssc.lt is operated by SSC GDL CA.

SSC GDL CA makes following information available to *Subscribers*, *Subjects*, *Relying parties* in its repository:

a) This CPS (http://gdl.repository.ssc.lt/CPS);

b) Root CA and Issuing CA certificates (http://gdl.repository.ssc.lt/certs);

c) Most recent versions of CRLs for the Issuing CAs:

http://gdl.repository.ssc.lt/rootacrl

http://gdl.repository.ssc.lt/rootbcrl

http://gdl.repository.ssc.lt/rootvs

2.2 Publication of certification information

The certificates upon generation are delivered to the S*ubscriber* or S*ubject* for whom the certificate is being issued. Certificates may be available for retrieval from the SSC GDL CA Repository if *Subject's* consent has been obtained.

The terms and conditions regarding the use of certificates are internationally available to *Relying parties* 24 hours per day, 7 days per week in the SSC GDL CA Repository.

Upon any failure out of control of SSC GDL CA, SSC GDL CA ensures that the information service may be unavailable for no longer than 48 hours.

2.3 Time or frequency of publication

The certificates and other relevant information is published promptly upon issuance or

acceptance by SSC GDL CA.

2.4 Access controls on repositories

The CPS, CA certificates and CRLs in the Repository are publicly available through the Internet. Access to other information in SSC GDL CA Repository is determined according to procedures approved by SSC GDL CA.

An imposed restriction is probable in the access of the Repository only for the purpose of protection from computer attacks.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

X.509 certificates and CRLs use *distinguished names* to identify issuers, S*ubjects* of certificates. Attributes of *distinguished names* use the *DirectoryString*[19] syntax that allows encoding of names in a choice of character sets: *PrintableString*, *TeletexString*, *BMPString*, *UniversalString*, and *UTF8String*.

Name comparison is used for X.509 certificate path validation[20], name chaining and name constraints computation. For correct path validation CAs are encouraged to honor the chosen character set.

Name constraints may be included in CA certificates. The constrained name MUST be compared to the *Subject* names in subsequent certificates in a certification path. For correct name constraints processing the CAs encodes each attribute value in a name constraint using the same encoding as is used to encode the corresponding attribute value in subject names in subsequent certificates.

3.1.1 Types of names

Whether the *Subject* of a certificate issued under this CPS is a human, organization, device or service can be discovered by *Subject* DN as indicated in the EN 319 412 1-5 series standards.

The names, surnames and pseudonyms have the usual semantic meaning, which allow validating the *Subject's* identity.

3.1.2 Need for names to be meaningful

Distinguished names in the certificates issued by SSC GDL CA identify in a meaningful way the *Subscriber* to which they are assigned. The CN attribute represents the *Subscriber* in a way that is easily understandable for humans. For a natural person by indicating person's official

19 Directory Access Protocol (v3): Attribute Syntax Definitions, RFC 2522, December 1997.
20 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, May 2008

name:

CN=*Firstname Lastname*

3.1.3 Anonymity or pseudonymity of subscribers

SSC GDL CA does not issue anonymous certificates. however pseudonymous certificates may be issued.

CA may issue pseudonymous certificates that identify physical entities or legal entities by their organizational role.

3.1.4 Rules for interpreting various name forms

Rules for interpreting DN forms are specified in [X.501] and rules for interpreting e-mail addresses are specified in [RFC2822].

As the *Subject* names (X.509) include *serialNumber* attributes that do not disclose the semantics of its value, for this purpose we use RFC 3739 defined statement "*qcStatement-2*".

3.1.5 Uniqueness of names

SSC GDL CA enforces *Subject* identity name uniqueness within all issued certificates. Multiple certificates issued to the same physical entity allow to uniquely identify the *Subject* according to 3.1.4.

3.1.6 Recognition, authentication, and role of trademarks

SSC GDL CA will not issue a certificate if it infringes the trademark of another entity.

3.2 Initial identity validation

Initial identity verification is a function performed by the SSC GDL Registration authority

related to identity proofing.

In terms of *Subject* data verification assurance this CPS defines four classes (levels) of initial identity verification - Class 1 being the lowest assurance level, and Class 4 - the highest.

As a criteria of certificate class selection specific applications and transactions, after assessing the associated risks and their likelihood of occurrence in accordance with the provisions of section 1.4, define the levels of acceptable identity verification which are used by *Subscribers*.

If the S*ubject* is a physical person, evidence of the *Subject*'s identity (e.g. name, surname) is checked against a physical person either directly or would have been checked indirectly using means which provides equivalent physical presence[21] assurance.

SSC GDL CA records all the identity verification information and any reference number on the documentation used for verification, and any limitations on its validity.

If SSC GDL CA service is provided through a *Subscriber*, then evidence is provided that the subscriber is authorized to act on behalf of the *Subject* (e.g. is authorized for all members of the identified organization). The S*ubscriber* provides a physical address, or other attributes, which describe how he/she may be contacted.

Certificates are issued to devices and services, provided that a responsible person is designated for assuring appropriate control and use of private keys. SSC GDL CA documents this designation. In the certificates issued in compliance with this CPS the DN may indicate the *Subject* device or service. It is the responsibility of the designated person to insure that the keys are securely conveyed to the subject device or service.

Verification of identity information for issuing EVCP and EVCP+ certificates is conducted according to [CABF-EV].

SSC GDL CA provides a special application form for issuing EVCP and EVCP+ certificates adopted to fulfill the verification requirements for all potential participants indicated in section 1.3.5.

21 An example of evidence checked indirectly against a physical person is documentation presented for registration which was acquired as the result of an application requiring physical presence.

3.2.1 Method to prove possession of private key

If the *Subscriber* generates its own keys, he/she is required to prove possession of the private key, which corresponds to the public key in the certificate request (CSR).

For signing certificate requests, this is done by requesting the *Subject* to sign a value offered by SSC GDL CA. SSC GDL CA then validates the signature using the person's public key.

Proof of possession is not required if key generation is performed under the direct control of CA or RA.

3.2.2 Authentication of organization identity

For an organizational *Subject* evidence is provided of full name of the organizational entity and reference to a nationally recognized registration.

For a device or service operated by or on behalf of an organization, evidence is provided of identifier of the device/service by which they may be referenced, full name of the organizational entity and a nationally recognized identifier.

For certificates issued under EVCP and EVCP+ certificates verification of Applicant's Identity, including its assumed name, legal, physical and operational existence and Domain Name ownership is performed according to the requirements indicated in [CABF-EV].

3.2.3 Authentication of individual identity

If the *Subject* is a physical person with no association with a legal person, evidence is provided of full name (including surname and given names consistent with the applicable law and national identification practices), date and place of birth, reference to a nationally recognized identity document, or other attributes (e.g. biometry) which may be used to distinguish the person from others with the same name.

If the *Subject* is a physical person who is identified in association with a legal person, or organizational entity, evidence is provided of full name (including surname and given names, consistently with the applicable law and national identification practices) of the S*ubject*, date and place of birth, reference to a nationally recognized identity document, or other attributes which

may be used to distinguish the person from others with the same name, full name and legal status of the associated legal person or other organizational entity, any relevant existing registration information of the associated legal person or other organizational entity, the association of the *Subject* with the legal person or other organizational entity.

Alternative procedures, such as a PIN (Personal Identification Number) may be used for revocation using a secure connection.

3.2.4 Device authentication

If the *Subject* of certificate is a hardware device, the Applicant must provide appropriate identifying information and an acceptable proof of ownership which shall include the manufacturer assigned device/product name, serial number, device attributes to be included in the certificate, if any, and owner's contact information.

The CA shall validate that the *Applicant* is authorized to request a certificate for the device.

If the device itself provides its identification information (e.g. a certificate), the identity of the device shall be authenticated.

Additional information about device registration process can be found in section 4.

3.2.5 Service authentication

If the *Subject* of certificate is a service offered via a network, the Applicant must provide identifying information and an acceptable proof of ownership which shall include unique software or service name (e.g. DNS name), service attributes to be included in the certificate, if any, and owner's contact information.

The CA shall validate that the *Applicant* is:

(a) authorized to request a certificate for the service;
(b) the real owner owner of the service (through an appropriate reliable 3rd party database);
(c) able to demonstrate control of the domain (by manipulating DNS records and server configuration).

Additional information about service registration process can be found in section 4.

3.2.6 Non-verified subscriber information

Information about the *Subject,* including email address, is included in certificates only after it is reliably verified.

3.2.7 Validation of authority

For issuing CA certificates or signature certificates asserting organizational authority, SSC GDL CA validates the individual's authority to act on behalf of the organization. For pseudonym certificates identifying *Subjects* by their organizational roles, SSC GDL CA validates that the person has been authorized to sign on behalf of the role.

3.2.8 Criteria for interoperation

The SSC GDL PKI is designed to interoperate with other trust services for:

– *Subject* registration;

– Key material and/or certificate dissemination;

– On-line Subject authentication;

– any other mutually beneficial services.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

For re-key of S*ubscriber* certificates identity may be established through use of current valid signature certificate, provided that the identity has been reestablished through the regular registration process at least once every three years.

For re-key of device certificates, identity may be established through the use of the current signature certificate of the device or the person responsible for the device, provided that the identity is reestablished through the regular registration process at least once every three years.

3.3.2 Identification and authentication for re-key after revocation

After certificate revocation, issuance of a new certificate always requires that the *Subject* go through the initial registration process described above.

3.4 Identification and authentication for revocation request

SSC GDL CA MUST authenticate revocation requests. Authentication can be through the use of current certificate, provided that the associated private key has not been compromised.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

In general, the lifecycle of a SSC GDL CA issued certificate includes: Subject's Registration, Certificate Issuance, Certificate Usage, Certificate Revocation, Certificate Expiration, Certificate Re-issuance/Updating.

To conduct reliable Registration process the CA has implemented a verification model based on following:

1. Certificate Requester:

(a) is a natural person – holder of a valid, verifiable identification document;

(b) has been authorized to represent the *Applicant* and/or a *Subject*, where applicable;

(c) can be communicated through a publicly identifiable communication channel.

2. Certificate Applicant:

(a) is either the *Requester* or other natural/legal person with a valid, verifiable identification document;

(b) has been authorized to represent the *Subject*, where applicable;

(c) can be communicated through a publicly identifiable communication channel;

3. Certificate *Subject*:

(a) is either the *Applicant* or other natural or legal person with a valid, verifiable identification document;

(b) has relevant proof of authorization, where applicable;

(c) agrees with the terms and conditions of the certification service;

(d) can be contacted personally or communicated through a publicly identifiable communication channel.

The Registration process, which can be performed remotely or by having the Subject physically present[22], ensures reliable documentation to prevent repudiation and requires the Applicant to provide proof that:

22 using methods which provide equivalent assurance in terms of reliability to the physical presence and for which the TSP can prove the equivalence.

1. the *Subject* being registered is indeed the one entitled to the particular person;
2. the *Subject* exists under the claimed identifiers and attributes;
3. the *Subject*'s identifier is unique within a given domain.

SSC GDL CA maintains a list of documents and sources of information that have been recognized as reliable to provide acceptable proof of identity. Depending on the class of certificate, an individual shall physically present during the identity proofing or remote identity proofing can be performed, if permitted by the applicable verification procedure.

The way how a certificate is requested and an *Applicant* is verified has important security implications throughout the certificate lifecycle. In general, Registration includes:

1) acceptance of a Request to issue certificate;
2) identification of Requester and verification of his authorization in regards to the Request;
3) establishing a mutually acceptable communication channel between the Requester and RA;
4) provision of initial information (certification terms and conditions, application forms, access credentials etc.);
5) acceptance of application and all relevant documents;
6) identification of *Applicant* and verification of his authorization in regards to the Application;
7) verification of Applicant's forms of existence;
8) verification of any relationship between the *Applicant* and other persons that have significant impact to or assume responsibility for the contractual rights and obligations between the CA and *Applicant*;
9) verification of information that is requested in the *Subject* of certificate;
10) verification of other attributes (e.g. email address, domain name etc.) requested in certificate;
11) acceptance of application.

In the verification process the RA first checks the validity of information/documents provided by a *Requester* and then existence forms of other involved persons using a reliable independent source of information of its own choice.

Once the proof of identity of associated persons has been confirmed the RA verifies any other information requested in the certificate. This includes both the physical and digital assets.

For hardware devices the *Applicant* has to provide product identification information (e.g. name, serial number etc.) and proof of ownership (e.g. place of operation, shipping/delivery documents, invoice etc.). This information is cross verified through third parties, whenever possible.

For digital assets whose identifiers are maintained by third parties (e.g. email addresses, domain names etc.) the RA verifies operational existence by directly accessing/using the resource (e.g. a server) or communicating through the resource (e.g. email address) and legal existence - by obtaining independent ownership conformation from the associated registrar.

For high assurance certificates the RA requests demonstration of control over the digital asset (e.g. updating DNS records, server configuration etc.).

To sum up SSC GDL CA:

a) discloses to all *Subscribers* and *Relying parties* the terms and conditions regarding use of its services in its PKI Disclosure Statement (PDS);
b) has a management body with final authority for approving the CPS and ensuring that the CPS is properly implemented;
c) gives a notice of changes it intends to make in its CPS and makes the revised and approved CPS immediately available;
d) documents the algorithms and parameters employed.

The CA maintains a separate internal document “IDENTITY REGISTRATION FOR CERTIFICATE ISSUING AND SUBSCRIBER SUPPORT" where all identity verification related procedures have been specified at operational level. This document is subject to audit.

4.1 Certificate Application

Before entering into a contractual relationship[23] with a *Subscriber*, SSC GDL CA informs the *Subscriber* of the terms and conditions regarding use of the certificate[24] through publicly available PKI Disclosure Statement[25].

23 Regarding contractual terms and conditions for certificates issued to the public attention is drawn to requirements of consumer legislation including implementation of Directive 93/13/EEC on unfair terms in consumer contracts.
24 If the subject is a person and not the same as the subscriber, the subject is informed of his/her obligations.
25 OID of the document: 2.16.440.1.4.30003763.0.3.1.0, 1.3.6.1.4.1.22501.0.3.1.0

SSC GDL CA collects either direct evidence, or an attestation from an appropriate and authorized source, of the identity. The procedure of *Subject's* identity verification at time of registration has been properly defined in the internal documents in accordance with national law.

SSC GDL CA ensures that the requirements of the EU and national data protection legislation have been adhered to within their registration process and SSC GDL CA's verification policy requires the capture of evidence of identity sufficient to satisfy the requirements of the intended use of the certificate.

SSC GDL CA verifies at time of registration, as specified in the internal documents in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued. Evidence of the identity is checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence[26].

If an entity other than the *Subject* is subscribing to SSC GDL CA services, then evidence is provided that the S*ubscriber* is authorized to act for the S*ubject* as identified and the certificate application form containing information about *Subject's* obligations have to be signed by both the *Subscriber* and the *Subject*. The application form provides appropriate fields that identify the roles of each participant as defined in sections 1.3.3, 1.3.5. The certificate application forms are available to *Subscribers* upon submitting initial service order form.

For EVCP and EVCP+ certificates extra verification measures are taken as defined in [CABF-EV] to ensure the Subscriber's legal[27], physical[28] and operational existence. Proof of representation and authority to act on behalf of the Applicant has to be demonstrated in order to authenticate the signatures on EVCP and EVCP+ certificate application forms[29].

SSC GDL CA records the signed agreement with the *Subscriber* including:

a) agreement to the *Subscriber's* obligations;

26 Evidence checked indirectly against a physical person is documentation presented for registration which was acquired as the result of an application requiring physical presence. Submitted evidence may be in the form of either paper or electronic documentation.

27 The RA checks that the organization is the legal holder of its name by mapping the information provided in the Extended Validation certificate application with information of official Government Registers (Legal entity DB, TAX payers DB, Social Security DB) that confirms the existence of the organization.

28 The RA checks the official postal address of the applicant along with Applicant's main business phone number.

29 In case a technical contact is also the certificate requester with no approval rights, the certificate application form has to be signed by an authorized certificate approver, whose signature has to be verified. The RA communicates with the Certificate signer by phone to ensure validity of authorization. The RA may also communicate with the Certificate signer by postal mail sent to the applicant's place of business.

b) agreement by the S*ubscriber* to use secure user device[30];

c) consent to the keeping of a record by SSC GDL CA of information used in registration[31], subject device provision, including whether this is to the *Subscriber* or to the *Subject* where they differ, and any subsequent revocation, the identity and any specific attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of SSC GDL CA terminating its services;

d) consent or refusal to publication of the certificate;

e) confirmation that the information held in the certificate is correct;

f) obligation and warranty by the *Subscriber* or a *Subcontractor* of EVCP and/or EVCP+ certificate:

- to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the private key of the associated EVCP and EVCP+ certificate and any associated access information or device, e.g. password or token;
- that it will not install and use the EVCP or EVCP+ certificate until it has reviewed and verified the accuracy of the data included in the certificate;
- to install the EVCP or EVCP+ certificate only on the server accessible at a Domain Name indicated in the certificate, and to use the EV Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement;

g) obligation and warranty to promptly request the CA to revoke the certificate, in the event that:

- any information in the SSC GDL CA issued certificate is or becomes incorrect or inaccurate;
- there is any actual or suspected misuse or compromise of the *Subscriber's* private key associated with the certificate.

h) the records identified above are retained for the period of time as indicated to the Subscriber above and as necessary for the purposes for providing evidence of certification

30 If required by the CA.
31 Including the identity of accepting the application, the identity validation method, if any, and the name of associated CA and RA, if applicable.

in legal proceedings[32].

In case the S*ubject*'s key pair is not generated by SSC GDL CA, the documented certificate request process ensures that the *Subject* has possession of the private key.

SSC GDL CA maintains a high risk application verification by checking lists of organization names that are target of phishing and other fraudulent attacks, the suspicious applications are processed with extra validation against the lists of phishing targets published by APWG[33] and other resources maintained by the CA to ensure that Applicant and the target in question are the same organization.

4.1.1 Who can submit a certificate application

For a CA certificate – an application is accepted from an authorized representative of the SSC GDL CA.

For a *Subject* certificates - an application is accepted from either the *Subject* or *Subscriber.*

For device/service certificates - an application is accepted from the responsible person of the device or service.

4.1.2 Enrollment process and responsibilities

All communications between RA and the *Subscriber* including the issuance process are authenticated and protected from modification; electronic transmission of shared secrets is protected.

For electronic communications cryptographic encryption mechanism is used.

Subscriber is responsible for providing accurate information throughout the enrollment process.

32 In case where subjects are registered through a RA in another country to where the CA is established then that RA must also apply its own country's regulations. Where some subscribers are residing in another country then contractual and other legal requirements applicable to those subscribers are also be taken into account.

33 The Anti-Phishing Work Group

4.2 Certificate application processing

The certificate application process guides and assists the *Subscriber* up to the final step of obtaining the certificate.

Application processing for EVCP and EVCP+ certificates is finished after a person other than the one who performed initial Application information verification conducts an extra cross correlation, due diligence verification and decides whether or not to issue the certificate.

4.2.1 Performing identification and authentication functions

The identification and authentication of the S*ubscriber* meets the requirements of this CPS described above.

The *Subscriber* identity authentication is a properly documented responsibility of the RA.

4.2.2 Approval or rejection of certificate applications

Conditions for application approval or rejection are specified in the *Subscriber* contract.

4.2.3 Time to process certificate applications

Certificate applications MUST be processed within three working days and a certificate MUST be issued within 5 working days since the RA verification.

4.3 Certificate issuance

Upon receiving the request, the RA verifies the identity and the authority of the *Subscriber*, the integrity of the information in the certificate request. Positive verification is followed by a request to SSC GDL CA to generate the certificate.

4.3.1 CA actions during certificate issuance

SSC GDL CA ensures that requests for certificates of a *Subject* who has previously been registered with SSC GDL CA are complete, accurate and duly authorized. This includes certificate renewals, issuing a certificate with a new subject key following revocation or prior to expiration, or update due to change to the S*ubject*'s identity information.

SSC GDL CA checks the existence and validity of the certificate to be renewed and that the information used to verify the identity and attributes of the *Subject* are still valid. If any certified names or attributes have changed, or the previous certificate has been revoked, the registration information is verified, recorded, agreed to by the subscriber.

SSC GDL CA does not issue a new certificate using the S*ubject's* previously certified public key.

The certificate issued under this CPS includes:

a) identification of SSC GDL CA and the country in which it is established;
b) the name of the *Subject*, or a pseudonym;
c) the public key which corresponds to the private key under the control of the subject[34];
d) an indication of the beginning and end of the period of validity of the certificate;
e) the identity code of the certificate;
f) the electronic signature of the issuing CA.

The QCP and QCP+ certificates issued under this CPS contain[35]:

a) an indication that the certificate is a qualified certificate;
b) the identification of SSC GDL CA and the State in which it is established;
c) the name of the signatory or a pseudonym, which is identified as such;
d) provision for a specific attribute of the signatory to be included if relevant;
e) signature-verification data which correspond to signature-creation data;
f) an indication of the beginning and end of the period of validity of the certificate;
g) the identity code of the certificate (e.g. certificate serial number);
h) the advanced electronic signature of the certification service provider issuing it;
i) limitations on the scope of use of the certificate, if applicable;

34 Certificates issued under QCP+ imply sole control by the Subject.
35 As defined in EN 319 412-5.

j) limits on the value of transactions for which the certificate can be used, if applicable[36];

k) reference to the SSC GDL CA PDS.

The EVCP and EVCP+ certificates issued under this CP contain:

Field	OID
subject:organizationName	2.5.4.10
subject:commonName[37]	2.5.4.3
subject:businessCategory	2.5.4.15
subject:jurisdictionOfIncorporationLocalityName	1.3.6.1.4.1.311.60.2.1.1
subject:jurisdictionOfIncorporationStateOrProvinceName	1.3.6.1.4.1.311.60.2.1.2
subject:jurisdictionOfIncorporationCountryName	1.3.6.1.4.1.311.60.2.1.3
subject:serialNumber	2.5.4.5
subject:streetAddress	*2.5.4.9*
subject:localityName	*2.5.4.7*
subject:stateOrProvinceName	*2.5.4.8*
subject:countryName	*2.5.4.6*
subject:postalCode	*2.5.4.17*

SSC GDL CA ensures over time the unambiguity of the DN assigned to the *Subject* of qualified certificate within the domain of SSC GDL CA[38].

The procedure of issuing the certificate has been documented and is securely linked to the key pair generation[39], associated registration, certificate renewal or update.

SSC GDL CA ensures that if it issues to the *Subject* secure user device this is carried out securely:

- Secure user device preparation securely controlled by the CA;
- Secure user device securely stored and distributed.

4.3.2 Notification to subscriber by the CA of issuance of certificate

About the issuance of certificate and its availability for delivery the *Subscriber* is informed

36 Applies to certificates issued under QCP+
37 Or *subjectAltName:dNSName*
38 Over the life time of the CA a distinguished name which has been used in an issued certificate, never be re-assigned to another entity.
39 Certificates are always issued according to the content of PKC#10 requests signed by the appropriate private key.

by RA. For device or service certificates, the RA informs the responsible person.

4.4 Certificate acceptance

The certificate issuance process includes a step when the S*ubscriber* explicitly confirms acceptance of the certificate. By accepting a certificate the *Subscriber* agrees to the terms and conditions contained in this CPS.

4.4.1 Conduct constituting certificate acceptance

The certification process provides a step in which the *Subscriber* explicitly accepts the certificate.

4.4.2 Publication of the certificate by the CA

SSC GDL CA makes no stipulation regarding publication of subscriber certificates if accepted by the *Subject* and data protection requirements are met.

4.4.3 Notification of certificate issuance by the CA to other entities

Parties involved in the certificate issuance process MAY also receive notification of a certificate's issuance.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Specific key pair and/or usage restrictions are expressed through the use of *Basic constraints*

and *Key usage*.

4.5.2 Relying party public key and certificate usage

CAs operating under this CPS issue CRLs indicating the current status of all valid certificates[40] that *Relying parties* MUST check whenever relying on a certificate.

4.6 Certificate renewal

This CA supports certificate renewal by replacing the existing certificate with a new one based on a new key pair.

4.6.1 Circumstance for certificate renewal

SSC GDL CA checks the existence and validity of the certificate to be renewed and that the information used to verify the identity and attributes of the S*ubject* are still valid.

4.6.2 Who may request renewal

Only a *Subject* or an authorized representative of the *Subject* MAY request renewal of the *Subject*'s certificate.

4.6.3 Processing certificate renewal requests

Renewal applications and procedures are generally the same as those used during the original issuance, any documents provided by the *Subscriber* MAY also be signed digitally.

4.6.4 Notification of new certificate issuance to subscriber

SSC GDL CA notifies *Subscribers* of new certificate issuance in a manner appropriate to the applicable policy requirements.

40 except OCSP responder certificates with the *id-pkix-ocsp-nocheck* extension.

4.6.5 Conduct constituting acceptance of a renewal certificate

Renewed certificates are considered accepted either explicitly upon delivery based on the written confirmation by the *Subscriber* or the *Subscriber*'s use 15 days after the certificate's renewal.

4.6.6 Publication of the renewal certificate by the CA

Renewed certificates are published in SSC GDL CA Repository based on the Subscriber's consent.

4.6.7 Notification of certificate issuance by the CA to other entities

Other entities may have also been notified of certificate issuance if involved in the issuance process.

4.7 Certificate re-key

Re-keying a certificate is the same as issuing a new certificate with a new public key while other *Subject* information in the certificate remain unchanged. The re-keyed certificate may have a different expiration period and any non-*Subject* related information in the certificate MAY also change.

4.7.1 Circumstance for certificate re-key

Up to two such renewals/re-keys may occur on-line at intervals not to exceed 25 months, without the need for the *Subject* to reappear in person. Revoked or expired certificates are not renewed.

4.7.2 Who may request certification of a new public key

Prior to the expiration of the usage period of a key pair, a *Subscriber* may request issuance of a new certificate, provided the previous certificate has not been revoked and a valid *Subscriber*

and requirement for the certificate still exists.

4.7.3 Processing certificate re-keying requests

SSC GDL CA checks the existence and validity of the certificate to be re-keyed and that the information used to verify the identity and attributes of the *Subject* are still valid.

If any certified names or attributes have changed, or the previous certificate has been revoked, the registration information is verified, recorded, agreed to by the *Subscriber*.

4.7.4 Notification of new certificate issuance to subscriber

Subscribers are notified of new certificate issuance immediately after the certificate is generated.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Re-keyed certificates are considered accepted either explicitly upon delivery based on the written confirmation by the *Subscriber* or the *Subscriber*'s use 15 days after the certificate's renewal.

4.7.6 Publication of the re-keyed certificate by the CA

Re-keyed certificates are published in SSC GDL CA Repository based on the *Subscriber*'s consent.

4.7.7 Notification of certificate issuance by the CA to other entities

Other entities may have also been notified of certificate issuance if involved in the issuance process.

4.8 Certificate modification

Certificate modification is the same as issuing a new certificate with a new public key where

any *Subject* information in the certificate MAY also change. The modified certificate MAY have a different expiration period and non-*Subject* related information in the certificate MAY also change.

4.8.1 Circumstance for certificate modification

SSC GDL CA checks the existence and validity of the certificate to be modified and that the information used to verify the identity and attributes of the S*ubject* are still valid.

4.8.2 Who may request certificate modification

Only a *Subject* or an authorized representative of the *Subject* MAY request modification of the *Subject*'s certificate.

4.8.3 Processing certificate modification requests

Modification applications and procedures are generally the same as those used during the original issuance, any documents provided by the *Subscriber* MAY also be signed digitally.

4.8.4 Notification of new certificate issuance to subscriber

SSC GDL CA notifies *Subscribers* of modified certificate issuance in a manner appropriate to the applicable policy requirements.

4.8.5 Conduct constituting acceptance of modified certificate

Modified certificates are considered accepted either explicitly upon delivery based on the written confirmation by the *Subscriber* or the *Subscriber*'s use 15 days after the modified certificate's issuance.

4.8.6 Publication of the modified certificate by the CA

Modified certificates are published in SSC GDL CA Repository based on the *Subscriber*'s consent.

4.8.7 Notification of certificate issuance by the CA to other entities

Other entities may have also been notified of certificate modification if involved in the issuance process.

4.9 Certificate revocation and suspension

SSC GDL CA ensures that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests. SSC GDL CA has documented the procedures for revocation of certificates.

The maximum delay between receipt of a revocation request and the revocation status update available to all relying parties is 48 hours[41].

Requests and reports relating to revocation[42] are processed on receipt, authenticated and checked to be from an authorized source. Such reports and requests are confirmed as required under SSC GDL CA's procedures.

The S*ubject*, and where applicable the *Subscriber*, of a revoked certificate, is informed of the change of status of the certificate. A revoked certificate is never be reinstated.

Revocation status information, is publicly and internationally available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of SSC GDL CA, SSC GDL CA makes best endeavours to ensure that this information service is not unavailable for longer than 72 hours.

SSC GDL CA supports CRL and OCSP and any updates to revocation status are available for

41 for QCP, QCP+, EVCP and EVCP+ - 24 hours.
42 e.g. due to compromise of subject's private key, death of the subject, unexpected termination of a subscriber's or subject's agreement or business functions, violation of contractual obligations.

both methods. The CA ensures sufficient resources to provide a commercially-reasonable response time for the number of certificate status queries generated by all certificates issued by the CA.

The integrity and authenticity of the status information is protected. Certificate status information is maintained at least until the certificate expires.

A revocation request may be authenticated on the basis of a verifiable digital signature or by a signed request. Revocations can be made at the request of the S*ubject*, the S*ubscriber* or other authorized persons.

4.9.1 Circumstances for revocation

SSC GDL CA revokes the certificate:

a) upon the *Subject's* or *Subscriber's* request;

b) when the control on the private key is lost;

c) when the incorrect data was submitted;

d) in accordance with the limitations indicated in the certificate;

e) when the *Subject* become incapable or died;

f) when the *Subject* violated the agreement or any other relevant legal regulation;

g) other cases in line with governing law.

For *Subscribers* using SSCD tokens revocation is optional if all the following conditions are met:

- the revocation reason was not "*key compromise*";
- the associated private key can not be exported;
- the token was returned to CA and it was initialized, formatted or destroyed promptly upon delivery;
- the token has been protected from unauthorized use within the period between surrender and initialization, formatting or destruction.

- In all other cases, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

h) The *Subscriber* indicates that the original EVCP and/or EVCP+ certificate request was not authorized and does not retroactively grant authorization;

i) The CA obtains reasonable evidence that the EVCP and or EVCP+ certificate has been misused;

j) The CA receives notice or otherwise becomes aware that a court or arbitrator has revoked *Subscriber's* right to use the domain name indicated in the EVCP and/or EVCP+ certificate, or that the *Subscriber* has failed to renew its domain name;

k) The CA receives notice or otherwise becomes aware of a material change in the information contained in the EVCP and/or EVCP+ certificate;

l) A determination, in the CA's sole discretion, that the EVCP and or EVCP+ certificate was not issued in accordance with the terms and conditions of [CABF-EV];

m) The CA determines that any of the information appearing in the EVCP and/or EVCP+ Certificate is not accurate;

n) The CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the EVCP and EVCP+ certificate;

o) The CA's right to issue EVCP and or EVCP+ certificates expires or is revoked or terminated, unless the CA makes arrangements to continue maintaining the CRL/OCSP Repository;

p) The private key of the CA's Root Certificate used for issuing that EVCP and/or EVCP+ certificate is suspected to have been compromised;

q) The CA receives notice or otherwise becomes aware that a *Subscriber* has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the CA's jurisdiction of operation;

r) An *Application Software Supplier* has requested revocation;

s) The certificate was used to sign or distribute malware, code that was downloaded without user consent.

4.9.2 Who can request revocation

These include:

- the *Subject* or the *Subscriber*;
- the issuing CA,
- authorized organization or law enforcement officials.

Revocation requests are promptly forwarded to SSC GDL CA or RA following suspicion or detection of a compromise or any other event necessitating revocation.

4.9.3 Procedure for revocation request

Application for certificate revocation MUST identity the Subject and explain the reason of revocation.

SSC GDL CA requests authentication of the applicant or confirmation of the revocation from an out-of band communication (e.g., phone, fax, email, in person). An authenticated application will always result in certificate revocation.

Applications submitted by third parties are investigated by SSC GDL RA within 24 hours after receipt and a decision is being made based on: the authentication of applicant, nature of the revocation reason and relevant legislation. Appropriate revocation applications will result in certificate revocation.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

Revocation requests received within two hours of CRL generation are processed before the

following CRL is published.

4.9.6 Revocation checking requirement for relying parties

Revocation checking is a decision to be made by *Relying parties*, based on risk assessment, responsibility, and evaluating the consequences of revoked certificate use.

4.9.7 CRL issuance frequency

CRLs are published not later than the next scheduled update. CAs issue CRLs at least once a week and the *nextUpdate* time in the CRL may be no later than 168 hours after the CRL generation.

4.9.8 Maximum latency for CRLs

CRLs are published promptly as they are generated but not later than 2 hours following the generation. CRLs are generated no later than the time indicated by *nextUpdate* of the current CRL.

4.9.9 On-line revocation/status checking availability

All SSC GDL CA issued certificate status information is available via CRL.

Online certificate status checking is available for certificates issued under QCP, QCP+, EVCP and EVCP+ policies.

4.9.10 On-line revocation/status checking requirements

Prior to relying on any SSC GDL CA issued certificate, relying parties MUST check the validity of the certificate[43].

43 See section "Revocation checking requirement for relying parties", 4.9.6 .

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

SSC GDL CA will use appropriate methods to inform its Subscribers and Relying parties about any SSC GDL CA private key compromise. The decision is being made by the SSC GDL CA shall be based on either a confirmed evidence of private key compromise or according to high probability of such a vulnerability.

4.9.13 Circumstances for suspension

Not applicable.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

SSC GDL CA provides a certificate status service using CRL or OCSP. The OCSP service available for the types of certificates indicated in "On-line revocation/status checking availability", 4.9.9 .

4.10.1 Operational characteristics

Availability and location of the CRL and OCSP services can be defined by verifying the Crl DP URL and AIA extensions.

4.10.2 Service availability

SSC GDL CA CRL and OCSP services are internationally available 24 x 7.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

SSC GDL CA Subscribers may end their service subscriptions in accordance with the provisions of appropriate service Agreement as indicated in Section 9 below.

4.12 Key escrow and recovery

Not applicable.

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

Physical security controls have been implemented to control access to SSC GDL CA hardware and software.

Physical access to SSC GDL CA personnel computers are limited to those performing one of the assigned roles. Access control is provided by keeping SSC GDL CA computers and related equipment in a locked room with access only available to those personnel.

Any persons entering the certificate generation, subject device provision and revocation management areas shall not be left for any significant period without oversight by an authorized person.

Security checks for SSC GDL CA facility are provided on a regular basis. The security check includes visual verification that cryptographic devices/tokens are securely stored if not in use, that the doors and locks are properly secured, and that there have been no attempts at forceful entry.

SSC GDL CA facility provides storage for backup and distribution media in a manner sufficient to prevent loss, tampering, or unauthorized use of the stored information. Backups are kept both for data recovery and for the archival of important information. At least one copy of backup material is stored at a location apart from the primary facility, with equivalent security, to permit restoration in the event of a disaster to the primary facility. Backup media is adequately protected from access by unauthorized personnel.

Sensitive data is stored in a way that prevents being revealed through re-use of storage objects (e.g. deleted files) by unauthorized users.

For the RA the only mandatory physical security control is the use of a lockable file cabinet or other repository for storing records of end entity registration requests.

5.1.1 Site location and construction

SSC GDL CA maintains three different locations for its core CA system, CA and RA

operations and provide robust protection against unauthorized access to the overall PKI infrastructure as the three components function independently from each other.

5.1.2 Physical access

The physical access controls for CA equipment ensures that no unauthorized access to the hardware is permitted and monitored for unauthorized intrusion at all times. Access to critical CA components including the cryptographic module requires at least two persons. Activation data stored separately from the cryptographic module. A security check of workstations used to administer SSC GDL CAs verifies if door locks, vent covers are functioning properly and the area is secured against unauthorized access.

The RA implements physical access controls to reduce the risk of equipment tampering.

5.1.3 Power and air conditioning

SSC GDL CA maintains appropriate power and air conditioning infrastructure to ensure the stability of its CA services.

5.1.4 Water exposures

SSC GDL CA ensures that its CA services are protected from water exposures.

5.1.5 Fire prevention and protection

SSC GDL CA ensures that its CA services are protected with reliable Fire prevention and protection infrastructure.

5.1.6 Media storage

SSC GDL CA stores its media so as to protect them from accidental damage and unauthorized physical access. Backups are created according to predefined schedules and are stored in a location separate from the primary facility. Media management procedures ensure protection against obsolescence and deterioration of media within the period of time that records

are retained.

5.1.7 Waste disposal

SSC GDL CA ensures that information storage media before being disposed is always destroyed.

5.1.8 Off-site backup

Data and system backups are performed and stored off-site once per week.

5.2 Procedural controls

5.2.1 Trusted roles

A trusted role is the one that can introduce security problems. These functions form the basis of trust for the entire PKI. Two approaches have been taken to ensure that these roles reliably carried out: the person filling the role is properly trained and is trustworthy; the roles are distributed among more than one person, so that malicious activity would require collusion. The primary trusted roles employed at SSC GDL CA and RA locations involve the following responsibilities:

1. Information System Security Supervisor – is responsible for the implementation of the SP;
2. Administrators – are authorized to install, configure and maintain SSC GDL CA trustworthy systems;
3. CA Operators – are responsible for operating SSC GDL CA trustworthy systems on a day-to-day basis;
4. RA Operators: are responsible for verification and approving end entity Certificate generation, revocation or suspension;
5. System Auditor – is authorized to view audit logs of SSC GDL CA system.

Personnel has no access to the trusted functions until any necessary checks are completed.

5.2.2 Number of persons required per task

At least two persons present and actively aware of the current operation while following operations are performed:

- bypassing OS protections - in the case of unexpected system malfunctions;
- copying/replacement of storage drives or system media;
- system restore from a backup;
- Root or Issuing CA key-pair generation, revocation, backup/recovery.

Administrators do not issue certificates to subscribers.

Certificate issuance by the Root CAs is a multi-person operation performed by authorized individuals whose roles have been defined in the Key Generation ceremony documentation.

The persons involved are sufficiently trained in IT, PKI, security requirements and understand the implications of the operation they are performing or witnessing.

5.2.3 Identification and authentication for each role

In accordance with usual practices for positions of this sensitivity.

5.2.4 Roles requiring separation of duties

SSC GDL CA supports these three distinct roles:

- CA Administrator;
- System Administrator;
- Information System Security supervisor.

No role separation controls are stipulated for RA.

The person who removes audit logs from SSC GDL CA system is different from the personnel who, in combination, command SSC GDL CA signature key.

5.3 Personnel controls

SSC GDL CA employs personnel[44] possessing the knowledge[45], experience and qualifications necessary to the job function. Appropriate sanctions are applicable to personnel violating CA policies or procedures.

Trusted roles, on which the security of SSC GDL CA service is dependent, are clearly identified.

CA personnel have job descriptions determining position sensitivity based on the duties, background screening, employee training and awareness. Personnel exercises administrative and management processes according to CA's security management procedures.

All CA personnel in trusted roles is free from conflict of interest.

SSC GDL CA ensures that individuals performing RA tasks have been trained in the operation of RA software and in the registration policies and practices.

5.3.1 Qualifications, experience, and clearance requirements

Persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, and MUST be citizens of one of EU member state.

5.3.2 Background check procedures

SSC GDL CA ensures that employees appointed to trusted roles have passed a background check prior approving such person to act in a trusted role. Each candidate must appear in-person before an authorized CA employee who verifies candidate's identity using government issued identity document (passports and/or e-ID).

44 Personnel employed by CA include individual personnel contractually engaged in performing functions in support of the CA's services. Personnel who may be involved in monitoring the CA services need not be CA personnel.

45 CA personnel is able to fulfill the requirement of "*expert knowledge, experience and qualifications*" through formal training and credentials, actual experience, or a combination of the two. This includes regular, at least every 12 months, updates on new threats and current security practices.

The identity verification includes: employment history, education, references, social security number, places of residence and criminal background. All checks cover the last five years interval. SSC GDL CA shall not appoint to trusted roles any person who is known to have a conviction for a crime or other offense. The candidate is asked to provide past convictions and turned down in case of refusal.

5.3.3 Training requirements

CA, RA and TSA personnel receives training in the following areas:

- CA and RA security procedures and principles;
- Authentication and verification policies and procedures;
- CA and RA PKI software;
- Disaster recovery and business continuity procedures;
- potential threats to the validation process;
- other applicable recommendations and guidelines.

Training period shall last three month and is provided by senior employees of CA and/or RA. SSC GDL CA maintains records of training and what level of training was completed.

RA personnel performing validation tasks must have the knowledge and skills to perform validation duties before being granted validation privileges[46].

5.3.4 Retraining frequency and requirements

Significant changes to SSC GDL CA or RA operations have a awareness plan.

5.3.5 Job rotation frequency and sequence

SSC GDL CA ensures that any changes in its personnel will have no impact on the performance of the CA services.

46 after passing an internal examination on the principles of validation presented in [CABF-BR] and [CABF-EV]).

5.3.6 Sanctions for unauthorized actions

SSC GDL CA maintains appropriate administrative sanctions to personnel violating relevant requirements, policies and procedures.

5.3.7 Independent contractor requirements

The employment policy and personnel requirements maintained by SSC GDL CA is equally applicable to all contractors.

5.3.8 Documentation supplied to personnel

The Documentation supplied to SSC GDL CA personnel includes:

- Certificate Policies, Certificate Practice Statements, Relying Party Agreements, Privacy Policy, PKI Disclosure Statement;
- Relevant technical and operational documentation to support duties and functions of the personnel;
- Records of all internal trainings and corresponding achievement levels are maintained on individual basis.

5.4 Audit logging procedures

Automatic audit log files are maintained by all applications supporting the functionality of SSC GDL CA. The log files ensure the traceability of any certificate life cycle event to a corresponding person.

5.4.1 Types of events recorded

Each audit record includes the following: the type of event, the date and time the event occurred, a success/failure indicator of certificate signing or revocation, the identity of the role that caused the event.

A message from any source requesting an action by SSC GDL CA is an auditable event. The corresponding audit record MUST also include message date and time, source, destination, and contents.

5.4.2 Frequency of processing log

Audit logs are automatically preprocessed and reviewed periodically for any evidence of suspicious activity and following each important operation.

5.4.3 Retention period for audit log

Audit logs MUST be retained for at least seven years.

5.4.4 Protection of audit log

CA system configuration and procedures ensure that only authorized people archive or delete security audit data. Procedures have been implemented to protect archived data from deletion or destruction before the end of the security audit data retention period.

5.4.5 Audit log backup procedures

A backup of the incremental information copies is maintained daily. A full backup copies of are maintained on a weekly basis.

5.4.6 Audit collection system (internal vs. External)

The audit log collection system is an internal process. Automated audit processes are invoked at system/application start-up.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

SSC GDL CA performs routine self-assessments of security controls according to internal procedures.

5.5 Records archival

5.5.1 Types of records archived

The archive records have been sufficiently detailed to determine the proper operation of SSC GDL CA and the validity of any certificate issued by SSC GDL CA. The following data is being recorded for archive: CA accreditation, CP, CPS, Subscriber Agreement templates, System/device/application configuration, changes and updates to system or configuration, *Subject* key generation, Certificate signing requests (CSR), all certificates issued, Revocation requests, receipt and acceptance of certificates, Subscriber agreements, receipt of tokens, CRLs published, changes to the audit parameters (frequency, type of events audited), attempts to delete or modify the audit logs, CA and *Subject* key generation, the export of private keys, the approval or rejection of a certificate status change request, appointment of an individual to a *trusted role,* destruction of cryptographic modules, all certificate compromise notifications, violations of SP, CP or CPS.

5.5.2 Retention period for archive

The retention period for archive data is 10 years.

5.5.3 Protection of archive

Protection of archive data is maintained by the means of digital signing and time stamping technologies.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

The archive data is periodically checked to ensure the integrity and readability of the information. Archive verification is performed by an automatic procedure under the control of a personnel with trusted role.

5.6 Key changeover

Each Root and Issuing CA has a single signing key with which they perform all CA signing functions. CAs may not issue certificates that extend beyond the expiration dates of their own certificates and public keys; therefore, their certificate validity periods are longer than those for users. To minimize the consequences of expired CA certificate, those keys are changed before the expiration of SSC GDL CA certificate. Only the new key is used for CA signing purposes from that time. The older, but still valid, CA certificate are available until all of the subscriber certificates signed under it have also expired.

5.7 Compromise and disaster recovery

In case of a CA key compromise, SSC GDL CA's certificate according to internal procedure will have to be revoked (if possible), SSC GDL CA installation re-established from the beginning by first re-establishing SSC GDL CA equipment and re-issuing SSC GDL CA certificate, then re-issuing all cross-certificates and all subscriber certificates.

If, due to the disaster, SSC GDL CA keys are compromised, or there is reasonable suspicion that compromise may have been possible during the disaster or subsequent activities, then SSC GDL CA will have to be re-built as in the case of key compromise, above.

All breaches or suspected breaches of CA integrity or security are reported promptly to the designated authorities.

5.7.1 Incident and compromise handling procedures

SSC GDL CA has established procedures to ensure that it notifies the competent supervisory body and other relevant third parties such as providers of software or systems relying on the trust service, data protection authorities of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein.

5.7.2 Computing resources, software, and/or data are corrupted

In case of any computing resource, software irregularities including the cases of data corruption the SSC GDL CA acts in accordance with its disaster recovery plan.

5.7.3 Entity private key compromise procedures

In case of SSC GDL CA private key compromise (or suspected to be compromised): the CA shall performs appropriate investigation procedures and decide whether the CA certificate need be revoked. If confirmed, all Subscribers will be notified at the earliest communication opportunity and a new CA key pair shall be generated or an alternative SSC GDL CA shall be used to further generate subscriber certificates.

5.7.4 Business continuity capabilities after a disaster

SSC GDL CA maintains a disaster recovery plan that will restore its operations based on predefined priorities, the highest priority will be given to restore the functionality of status checking services and SSC GDL CA Repository.

5.8 CA or RA termination

In the event of SSC GDL CA termination the Issuing CA certificate shall be revoked and the CA shall disseminate email and web site notice to all *Subscribers, Subjects, Application Software Suppliers* and cross certified entities prior to the termination. The CA shall also:

a) stop issuing certificates according to present CPS;

b) archive all audit logs and other records;

c) destroy all associated private keys;

d) transfer archived records to an authorized entity as defined by the Laws of jurisdiction;

e) notify the customers to delete all trust anchors representing the EV CA and take care about their

applications.

In the event if no authorized entity exists SSC GDL CA will:

a) transfer those functions to a reliable third party and preserve all relevant records;

b) revoke all unexpired certificates on a date as specified in the notice and publish final CRLs;

c) destroy all private keys.

SSC GDL has made insurance arrangements to cover the costs associated with fulfilling these requirements in case it becomes bankrupt or is unable to cover the costs.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

SSC GDL CA issuing certificates under this CPS ensures that SSC GDL CA key generation is undertaken in a physically secured environment by personnel in trusted roles and in accordance with the approved CA key generation ceremony.

6.1.1 Key pair generation

SSC GDL CA ensures that:

a) CA-generated *Subject* keys are generated using an algorithm recognized by industry;
b) CA-generated S*ubject* keys are of a key length and for use with a public key algorithm which are recognized by industry[47];
c) CA-generated *Subject* keys are generated and stored securely before delivery to the *Subject*;
d) the S*ubject's* private key is delivered to the *Subject* in a manner such that the secrecy and integrity of the key is not compromised;
e) preparation is securely controlled by SSC GDL CA[48].

Where the SSCD has associated user activation data, the activation data is securely prepared and distributed separately from the secure signature-creation device[49].

6.1.2 Private key delivery to subscriber

SSC GDL CA's delivery procedure is accomplished in a way that ensures that the correct tokens and activation data are provided to the correct *Subscribers*. Accountability for the location and state of the token is maintained until the S*ubscriber* accepts it.

SSC GDL CA maintains a record of acknowledgment of receipt of the token by the S*ubscriber*.

47 Guidance on algorithms and their parameters according to TS 102 176-1.
48 Applies to QCP+ certificates.
49 Separation may be achieved by ensuring distribution of activation data and delivery of SSCD at different times, or via a different route.

6.1.3 Public key delivery to certificate issuer

Where key pairs are generated by the *Subscriber* or RA, the public key and the *subscriber's* identity information MUST be delivered securely to SSC GDL CA for certificate issuance. The delivery mechanism binds the S*ubscriber's* verified identity to the public key. The cryptography used to achieve this binding is as strong as SSC GDL CA keys used to sign the certificate.

6.1.4 CA public key delivery to relying parties

When a CA updates its signature key pair, SSC GDL CA distributes the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate or in cross-certificates.

Installing a self-signed certificate onto tokens delivered to relying parties via secure mechanisms:

a) the certificate is installed onto the token during the S*ubscriber's* visit to the RA or in accordance with the section 6.1.2;
b) the certificate is installed onto the token when the RA generates the S*ubscriber's* key pair, which is then delivered to the *Subscriber* in accordance with section 6.1.2;
c) distribution of self-signed certificates through a software vendor[50] or trusted lists.

6.1.5 Key sizes

Industry recommended cryptographic algorithms and key lengths ensure that the issued certificates confirms the electronic signature during the period of validity.

6.1.6 Public key parameters generation and quality checking

SSC GDL CA public key parameters are defined in accordance with the appropriate ETSI, FIPS and other reliable sources[51] of information.

50 Includes Operating systems, browsers and other popular applications.
51 ECRYPT II Yearly Report on Algorithms and Key sizes, Katholieke Universiteit Leuven, 2012

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

User certificates with sscAuthenticationPolicy OID assert only the *digitalSignature* bit. Digital signature certificates may assert either the *digitalSignature or nonRepudiation*[52] bit.

CA certificates are used only for signing Subject certificates and CRLs and assert the *keyCertSign* bit. CA certificates with the subject public key to verify CRLs assert the *cRLSign* bit.

CA certificates with subject public key to verify OCSP responses assert the *digitalSignature* and/or *nonRepudiation* bits.

Device certificates to be used for digital signatures assert the *digitalSignature* bit. Device certificates may assert the *nonRepudiation* bit.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

SSC GDL CA HSMs have FIPS 140-2 Level 3 and/or EAL 4 security compliance certificate. The HSMs are handled, stored and checked strictly according to manufacturer's documentation. .

6.2.1 Cryptographic module standards and controls

No stipulation.

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

SSC GDL CA Private Key cryptographic operations are managed by internally documented multi-person procedures that provision a multilayer approach to access the Private key and the relevant operational environment. SSC GDL CA Key storage, the Root Key and Issuing key material are always protected through 3 of 5.

6.2.3 Private key escrow

SSC GDL CA does not escrow its signature keys or *Subscriber* private keys used for encryption.

6.2.4 Private key backup

SSC GDL CA private signature keys are backed up under the same control as the original signature key and stored off-site. Backup copies of SSC GDL CA private signature are protected in

52 Also known as contentCommitment.

the same manner as the original.

6.2.5 Private key archival

SSC GDL CA doesn't archive Private Key materials.

6.2.6 Private key transfer into or from a cryptographic module

When transferred into or outside the signature-creation device SSC GDL CA private signing key are protected in a way that ensures the same level of protection as provided by the signature creation device:

a) SSC GDL CA private signing key is backed up, stored and recovered only by personnel in trusted roles in a physically secured environment.
b) Backup copies of SSC GDL CA private signing keys are subject to the same level of security controls as the keys currently in use.

6.2.7 Private key storage on cryptographic module

SSC GDL CA Private Keys are stored on FIPS 140-2 level 3 certified devices.

6.2.8 Method of activating private key

The Private keys activation is based on the HSM manufacturer's methodology and internally developed and maintained multi-person, multilayer protection mechanisms.

6.2.9 Method of deactivating private key

SSC GDL CA personnel private keys may be deactivated after each procedure, logging-off the system.

SC GDL CA ensures that an activated HSM is not not left unattended or otherwise available to unauthorized access. Only predefined SSC GDL CA personnel activity may lead to Private Key signing. Private keys are transferred to the HSM only when appropriate CA is operational.

6.2.10 Method of destroying private key

When it is necessary, CA destroy the private keys in the order which reasonably ensures that there are no residue left, which may be used to the reproduction of the key. In respect of the computer cryptographic module, CA uses the "*zeroisation function*" and other appropriate measures in order to ensure the appropriate CA key destruction.

6.2.11 Cryptographic Module Rating

See 6.2.7 .

6.3 Other aspects of key pair management

6.3.1 Public key archival

Not applicable.

6.3.2 Certificate operational periods and key pair usage periods

Key pair's activity period is the same as the period of validity of the related certificate, except that private keys may continue to be used for decryption, and public keys may continue to be used for signature verification.

Subscriber signature private keys have the same usage period as their corresponding public key.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data generation and installation is performed in accordance with SSC GDL CA's Key Generation Ceremony documentation. The activation data is stored on smart cards that are grouped into three separately stored packets.

6.4.2 Activation data protection

The activation data and media are protected from disclosure by a combination of physical

storage, cryptographic and physical access control mechanisms.

6.4.3 Other aspects of activation data

Effective use of activation data is conditioned by the availability of at least two out of three separately stored activation data media packages.

6.5 Computer security controls

SSC GDL CA operating under this CPS ensures that its system access is limited to properly authorized individuals:

a) controls has been implemented to protect SSC GDL CA's internal network domains from unauthorized access including access by subscribers and third parties;

b) sensitive data is protected against unauthorized access, modification and is not exchanged over unsecured networks;

c) effective administration of user[53] access maintains system security, including user account management, auditing and timely modification or removal of access;

d) access to information and application system functions is restricted in accordance with the access control policy;

e) SSC GDL CA system provides sufficient computer security controls for the separation of trusted roles including the separation of security administration and operation functions;

f) CA personnel is properly identified and authenticated before using critical applications;

g) CA personnel is accountable for their activities;

h) Certificate generation and revocation management has a documented structure which safeguards impartiality of operations.

Dissemination and revocation status management application enforces access control on attempts to add or delete certificates and modify other associated information.

6.5.1 Specific computer security technical requirements

The following specific computer security requirements are applicable to SSC GDL CA system:

53 CA and RA operators, administrators and auditors

- each user authenticated before obtaining to SSC GDL CA system or applications;
- users have privileges appropriate to their assigned roles;
- audit records are generated and archived for all transactions;
- enforce domain integrity boundaries for security critical processes;
- support recovery from key or system failure.

6.5.2 Computer security rating

SSC GDL CA PKI system has been evaluated to be compliant with the the industry requirements to trustworthy systems.

6.6 Life cycle technical controls

6.6.1 System development controls

The development requirements for SSC GDL CA system are:

SSC GDL CA use software has been developed under a documented specification;

The dedicated infrastructure for SSC GDL CA operations and the system development have been effectively separated;

SSC GDL CA operation supports multiple CAs;

Proper care is being taken to prevent malicious software attacks.

6.6.2 Security management controls

The configuration of SSC GDL CA system have been documented. There is a mechanism for detecting unauthorized modification to the software or configuration. SSC GDL CA periodically verifies the integrity of the software.

6.6.3 Life cycle security controls

The system resources are monitored so that projections of future capacity requirements ensured

by availability of adequate processing power and storage.

6.7 Network security controls

Access to SSC GDL CA system is protected by firewalls that limit services allowed to and from SSC GDL CA system to perform CA functions. Protection of CA equipment is provided against known network attacks. All unused network ports and services are turned off. Network software present on SSC GDL CA equipment is the only necessary to the functioning of SSC GDL CA application.

6.8 Time-stamping

SSC GDL CA asserted times are accurate to within one minute.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Profiles of X.509 certificates issued under this CPS confirm to the specifications of [RFC5280] , additional profile requirements apply depending on the Class of certificate and applicable policy OID indicated in the Subject certificate.

The *Subject* certificate profiles issued under this CPS are defined in separate documents under the following OIDs:

Class of certificate	Types of certificates	Profile OID
Class 1	All	1.**3.6.1.4.1.22501.9.1.3.0** **2.16.440.1.4.30003763.9.1.3.0**
Class 2	All	1.**3.6.1.4.1.22501.9.2.3.0** **2.16.440.1.4.30003763.9.2.3.0**
Class 3	All	1.**3.6.1.4.1.22501.9.3.3.0** **2.16.440.1.4.30003763.9.3.3.0**
Class 4	All	1.**3.6.1.4.1.22501.9.4.1.0** **2.16.440.1.4.30003763.9.4.1.0**

The certificate profiles are available to *Subscribers*, *Subjects, Relying parties* and other persons upon request.

The profiles of EVCP and EVCP+ certificates are available in the documents containing Class 2 and Class 3 certificate profiles listed in the table above.

7.1.1 Version number(s)

SSC GDL CA issued certificates are X.509 Version 3 compliant.

7.1.2 Certificate extensions

See table in section 7.1.

7.1.3 Algorithm object identifiers

The algorithm OIDs used in the SSC GDL CA issued certificates are:

Algorithm	OID
sha-1WithRSAEncryption	1.2.840.113549.1.1.5
sha256WithRSAEncryption	1.2.840.113549.1.1.11
id-RSASSA-PSS	1.2.840.113549.1.1.10

7.1.4 Name forms

See table in section 7.1.

7.1.5 Name constraints

SSC GDL CA may issue certificates with name constraints.

7.1.6 Certificate policy object identifier

See table in section 7.1.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

See table in section 7.1.

7.1.9 Processing semantics for the critical Certificate Policies extension

See table in section 7.1.

7.2 CRL Profile

The CRL profiles issued under this CPS are defined in a separate document with the following OID:

1.3.6.1.4.1.22501.9.5.2.0

2.16.440.1.4.30003763.9.5.2.0

The CRL profiles are available to *Subscribers*, *Subjects, Relying parties* in the Repository:

http://gdl.repository.ssc.lt/CRLprofile

7.2.1 Version number(s)

SSC GDL CA CRLs comply with [RFC5280] Version 2 profile.

7.2.2 CRL and CRL entry extensions

See section 7.2 above.

7.3 OCSP profile

See section 7.2.

7.3.1 Version number(s)

See section 7.2.

7.3.2 OCSP extensions

See section 7.2.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

SSC GDL CA has a compliance audit mechanism in place to ensure that the requirements of this CPS are being implemented and enforced.

8.1 Frequency or circumstances of assessment

To gain confidence that the policy requirements specified in [ETSITS101042], [ETSI101456], and [ETSI102023] are appropriately applied an independent annual assessment may be required to assure that the service provider meets the policy requirements relating to its services.

8.2 Identity/qualifications of assessor

The certification body of TÜV Informationstechnik GmbH (FRG) is accredited by "DAkkS Deutsche Akkreditierungsstelle GmbH" according to DIN EN 45011 for the scope IT security product certification. The certification body performs its certification on the basis of:

"Zertifizierungsschema für Zertifikate des akkreditierten Bereichs der Zertifizierungsstelle der TÜV Informationstechnik GmbH", version 1.2 as of 2011-01-28, TÜV Informationstechnik GmbH

8.3 Assessor's relationship to assessed entity

SSC GDL CA has selected an Auditor/Assessor completely independent from the CA based on internationally accepted transparent tender arrangements.

8.4 Topics covered by assessment

The audit ensures that SSC GDL CA and its RAs comply with all the requirements of the current versions of SSC GDL CP and this CPS. All aspects of the CA/RA operation are subject to compliance audit inspections.

8.5 Actions taken as a result of deficiency

In case if an assessment reports any material noncompliance with applicable law, the SSC GDL CA CP/CPS, or any other obligations relevant to the CA services, SSC GDL CA shall develop an action plan to cure such noncompliance.

8.6 Communication of results

The assessment report has to be presented to the SSC GDL CA's Policy Authority for resolution of any deficiency through an appropriate action plan.

9 OTHER BUSINESS AND LEGAL MATTERS

Business and legal matters of the certification services provided by SSC GDL CA under this CPS have been classified as and presented in separate documents as shown in the following table:

CA Service Agreement	Document OID
Individual Subscriber's Agreement	1.3.6.1.4.1.22501.8.3.1.0 2.16.440.1.4.30003763.8.3.1.0
Organizational Subscriber's Agreement	1.3.6.1.4.1.22501.8.3.2.0 2.16.440.1.4.30003763.8.3.2.0
OCSP Service Agreement	1.3.6.1.4.1.22501.8.3.3.0 2.16.440.1.4.30003763.8.3.3.0
Time-stamp Service Agreement	1.3.6.1.4.1.22501.8.3.4.0 2.16.440.1.4.30003763.8.3.4.0
On-line Authentication Service Agreement	1.3.6.1.4.1.22501.8.3.5.0 2.16.440.1.4.30003763.8.3.5.0
Relying Party Agreement	1.3.6.1.4.1.22501.8.3.7.0 2.16.440.1.4.30003763.8.3.7.0

9.1 Fees

9.1.1 Certificate issuance or renewal fees

SSC GDL CA operating under this CPS publishes certificate issuance, renewal and modification fees on its web site.

9.1.2 Certificate access fees

SSC GDL CA reserves the right to charge a reasonable fee for access to its certificate database.

9.1.3 Revocation or status information access fees

Up to 10 OCSP requests per day is processed free of charge, for higher volume OCSP requests a Relying party MUST contact SSC GDL CA for commercial service terms and conditions[54].

54 Applicable to QCP and QCP+

9.1.4 Fees for other services

SSC GDL CA reserves the right to charge a reasonable fee for any other services.

9.1.5 Refund policy

According to the provisions of applicable Service Agreement presented in Section 9 .

9.2 Financial responsibility

SSC GDL CA maintains reasonable sufficient financial resources to support its operations and fulfill its duties under this CPS.

9.2.1 Insurance coverage

SSC GDL CA maintains Commercial Liability insurance according to the requirements set by the legislation of the European Union and Government of Lithuania.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

SSC GDL CA will cover a direct damage caused by its fault made to its customers within the limit of its liability.

9.3 Confidentiality of business information

See section 9 above.

9.3.1 Scope of confidential information

All *Subject*/*Subscriber* information collected by CA under this CPS is confidential and can not be revealed without the consent of *Subscribers* and *Subjects* except where permitted by the applicable legislation.

Information about SSC GDL CA's PKI design including all CA/RA applications, overall system architecture and principles of work considered confidential. Following information is not publicly available:

- all applications submitted to CA;
- requests for certificate;
- private keys (if any) and corresponding recovery data;
- all audit records;
- *Force majeure* planning;
- disaster recovery plans;
- security provisions for hardware/software control;
- all technical and technological aspects of certification ans registration processes;
- any business and service performance data except as provided by law.

9.3.2 Information not within the scope of confidential information

All *Subject* data presented in a certificate is considered public. Information presented by SSC GDL CA's certificate status services is also considered public.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

SSC GDL CA is a registered data controller with the State personal data controller's` register,

the registration number is P-3069.

9.4.1 Privacy plan

SSC GDL CA's privacy policy can be found here: https://gdl.repository.ssc.lt/pp

9.4.2 Information treated as private

Subject information about an individual that is not included in the certificate or CRL profiles is considered private.

9.4.3 Information not deemed private

Any personal or organizational data included in certificates, CRLs are not considered private.

9.4.4 Responsibility to protect private information

SSC GDL CA and *Subscribers* shall protect the confidentiality of private information with the same degree of care that it exercises in respect to its own information.

9.4.5 Notice and consent to use private information

SSC GDL CA MAY use private information with the Subject's consent or in accordance with the applicable law.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

All information referenced in this CPS under the name of or in association with the *SSC GDL CA* name is property of the organization indicated in section 1.5.2 . The organization may have other trade and service marks that have not been registered, but shall remain its intellectual property. All SSC GDL CA issued certificates are exclusive property of the CA. *Subscribers* and *Relying parties* are permitted to reproduce and otherwise use the certificates on a non-exclusive basis. SSC GDL CA as the issuer of certificates reserves exclusive right to revoke any certificate at any time and at its sole discretion.

9.5.1 Certificates and CRLs

No stipulation.

9.5.2 CP/CPS

All rights reserved by the authors of CP and CPS.

9.5.3 Trademarks

No stipulation.

9.5.4 Signature creation data

All Root and Issuing CA key pairs and corresponding Certificates, are the property of SSC GDL CA.

9.6 Representations and warranties

SSC GDL CA by issuing EVCP and EVCP+ certificates makes the EV Certificate Warranties to *Subscribers*, *Subjects*, *Application Software Suppliers* and *Relying parties* that it has followed the requirements of [CABF-EV] in issuing, managing and verifying the accuracy of EVCP and EVCP+ certificates.

9.6.1 CA representations and warranties

See section 9 above.

9.6.2 RA representations and warranties

See section 9 above.

9.6.3 Subscriber representations and warranties

See section 9 above.

9.6.4 Relying party representations and warranties

Relying party representations and warranties are subject to RPA available in the SSC GDL CA Repository.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

See section 9 above. In addition, in no event SSC GDL CA shall be liable for any or all of the following:

- Indirect, incidental or consequential damages;
- Loss of data or profits;
- Death or personal injury;
- Liability arising as a consequence of exceeding the limitations of monetary value indicated in the certificate;
- Liability arising as a consequence of hardware and software used by a *Subscriber*.
- Liability arising as a consequence of Private key compromise.

9.8 Limitations of liability

See section 9 above.

9.9 Indemnities

See section 9 above.

9.10 Term and termination

9.10.1 Term

See section 9 above.

9.10.2 Termination

See section 9 above.

9.10.3 Effect of termination and survival

See section 9 above.

9.11 Individual notices and communications with participants

Individual notices and communications related to SSC GDL CA CPS are accepted by the service contact points indicated in SSC GDL CA PDS.

9.12 Amendments

9.12.1 Procedure for amendment

See section 9 above. In addition, revisions may be made to this CPS with changing the modification part of the document version. SSC GDL CA maintains procedures that ensure that this CPS is not amended and/or published without proper authorization by the SSC GDL CA Policy Authority.

9.12.2 Notification mechanism and period

See section 9 above.

9.12.3 Circumstances under which OID must be changed

Any changes in applicable certificate policy OIDs indicated in section 1.2 will result in publication of revised version of this CPS.

9.13 Dispute resolution provisions

Any claims or disputes need to be notified directly to SSC GDL CA. The CA will attempt to resolve the dispute in a mutually acceptable manner before resorting to any dispute resolution mechanism and in the case if the parties in conflict can't resolve the dispute it will be solved in a Lithuanian national court. For more detailed info see section 9 above.

9.14 Governing law

See section 9 above.

9.15 Compliance with applicable law

See section 9 above.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

See section 9 above.

9.16.2 Assignment

See section 9 above.

9.16.3 Severability

See section 9 above.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

See section 9 above.

9.16.5 Force Majeure

See section 9 above.

9.17 Other provisions

No stipulation.

10 REFERENCES

10.1 Normative References

The documents below contain requirements which, if applicable to a specific certificate type, constitute provisions of this CPS. For an updated CP version the edition of referenced document that is earlier than date of update applies.

[CWA14167-1] CEN CWA 14167-1, Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.

[ETSITS101042] Policy requirements for certification authorities issuing public key certificates (Normalized level only).

[ETSIEN319411-3] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates.

[ETSI101456] ETSI TS 101 456 Policy, Requirements for Certification Authorities Issuing Qualified Certificates.

[ETSIEN319411-2] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.

[ETSI102023] ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities

[CABF-NCSSR] Network and Certificate System Security Requirements, CA/Browser Forum, 2012

[CABF-BR] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum, 2013

[CABF-EV] EV SSL Certificate Guidelines Version, CA/Browser Forum, 2012

[CENSSCD] CWA 14169 Secure Signature Creation Devices EAL4+.

[ALGO] ETSI SR 002 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures.

[SSC_CP] SSC GDL CA Certificate Policy

10.2 Informative References

[LT-PDP-LAW] The law on Personal data protection of Lithuanian Republic No. I-1444, 1st February 2008.

[LT-ES-LAW] The law on Electronic signature of the Republic of Lithuanian No. VIII-1822, 11th July 2000, (changed 6th June 2002 no. IX-934)

[CWA14172-3] CWA 14172-3: EESSI Conformity Assessment Guidance - Part 3: Trustworthy Systems Managing Electronic Signatures.

[RFC3647] RFC3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices.

[RFC2119] RFC 2119, Key words for use in RFCs to Indicate Requirement Levels. March 1997.

[RFC2560] RFC 2560, Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol, OCSP, June 1999.

[RFC5280] RFC 5280, Internet X.509 Public Key Infrastructure: Certificate and CRL Profile.Certificates for

[Dir1999/93/EC] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[RFC2510] Internet X.509 Public Key Infrastructure Certificate Management Protocols, Adams, S. Farrell, March 1999.

[RFC2822] RFC 2822, Internet Message Format, IETF, 2001

[ETSI TS 101 862] Qualified Certificate Profile, DTS/SEC-004003

[RFC3039] RFC3039, Internet X.509 Public Key Infrastructure Qualified Certificates Profile, Santesson, et al.).

[CC] Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408-1:1999, ISO/IEC 15408-2:1999, ISO/IEC 15408-3:1999.

[SSCGDLRPA] SSC GDL CA Relying Party Agreement

[SSC_PDS] SSC GDL CA PKI Disclosure Statement.