Trust Service Certification Policy

SSC GDL TSCP

Version 5.1

2017

Revision History

Document Version	Document Date	Revision Details
4,2	2013.04.15	New publication
4.3	2013.05.29	OR revised version
4.4	2013.07.12	ER recommendations
5.0	2016.02.28	eIDAS revision
5.1	2017-04-29	After CAB recommendations

Table of Contents

1 INTRODUCTION

Confidence in the security of electronic services is based on Trust Service Providers (TSP) whose procedures and protective measures minimize the potential threats and risks, associated with public key infrastructure (PKI) processes and security management.

The Trust Service Certification Policy (TSCP) is a higher level document that applies to all Certification Authorities (CAs) managed by the common set of rules presented in this TSCP. A Trust Service Certification Practice Statement (TSCPS) defines how a specific TSP meets the technical, organizational and procedural requirements of this TSCP. The lower-level documentation, which due to its specific nature considered private, may be used in the daily TSP operations that detail the procedures necessary to satisfy the requirements identified in this TSCP.

This TSCP specifies a set of provisions, identifies the types of entities and applications for which it is targeted based on the requirements in ETSI standards ETSI EN 119 401, ETSI EN 119 411-1, ETSI EN 119 411-2 and ETSI TS 119 421.

This document is structured according to [RFC3647] consequently some parts are left for compatibility, although may not directly applicable for the services provided under this TSCP.

The words "MUST", "SHALL", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", "OPTIONAL" should be interpreted as described in [RFC2119].

"*No stipulation"* in this document SHOULD be treated either "*not applicable*" or "*provisions of higher level normative document apply*" depending on the context.

1.1 Overview

Each TSP MUST release its TSCPS that the information about the TSP key technical, procedural and legal conditions would presented in the appropriate way to potential customers. This information SHALL be referred in the TSCPS by name or an appropriate Object Identifier (OID)[1].

1 See ITU-T recommendation X.208 (ASN.1) or ITU-T Recommendation X.509 (ISO/IEC 8824).

Certificates issued under this TSCP SHALL contain a registered certificate policy OID, which is used to decide whether a certificate is trusted for a particular purpose. This TSCP applies to all certificates regardless of their usage unless otherwise noted.

Subscribers and *Relying parties* MUST assure themselves, by reviewing this document, the TSCPS, and other referenced documents they deem necessary, that any certificate issued or other service provided by a TSP under this TSCP is suitable for the intended use.

1.2 Document name and identification

Certificates issued in accordance with this TSCP SHALL include an OID which can be used by *Relying parties* in determining the certificates suitability and trustworthiness for a particular application. SSC OID is a concatenation of two parts – the OID anchor and object ID in the SSC OID Registry. The former is an ID assigned to SSC by an external registry. Currently SSC has been identified by two registries: IANA[2] and Lithuanian OID Registry[3].

The IANA assigned enterprise number for SSC is: 1**.3.6.1.4.1.22501.**

The National Registry enterprise ID for SSC is: **2.16.440.1.4.30003763.**

So the two OIDs used to identify this TSCP are:

1.3.6.1.4.1.22501.0.1.5.0

2.16.440.1.4.30003763.0.1.5.0

1.3 PKI participants

This section describes the types of entities that fill the roles of participants within the PKI.

1.3.1 Certification authorities

Certification authorities are the TSPs that issue certificated related to “trust services” defined in Article 3 (16) of the eIDAS Regulation. The associated TSCPS under these TSCP SHALL identify the types of TSPs and their relationship with other PKI participants.

2 Internet Assigned Numbers Authority.

3 To be approved by national authorities.

1.3.2 Registration Authorities

RAs are the entities that establish enrollment procedures for certificate applicants, perform identity verification, identification and authentication of applicants. RAs also provide other related functions that the TSP operating under this TSCP SHALL describe in its TSCPS. TSP MAY delegate or employ one or more RAs. The associated TSCPS SHALL name all delegated RAs and their relationship with one more TSPs within the PKI.

In case if the RA functions have been delegated to a third party, the TSP operating under this TSCP SHALL ensure that data is exchanged only with authorized service providers.

1.3.3 Subscribers

A *Subscriber* is an entity issued a certificate in accordance with this TSCP and who agrees to comply with the provisions of the associated TSCPS. The types of *Subscribers* and their relationship with the certificates issued by the TSP operating under this TSCP should be detailed in the TSCPS.

1.3.4 Relying parties

Relying party is any recipient of a certificate who relies on a certificate and decides to use a certificate issued under this TSCP.

1.3.5 Other participants

TSPs operating under this TSCP MAY involve other parties in provisioning of certificates and/or providing accompanying services.

1.4 Certificate usage

Certificates issued under this TSCP are identity certificates that bind subject's public key to an identity and other data in the certificate. These certificates MAY NOT necessarily convey information about the subject's role, authority, privileges or authorization to perform business functions. However they MAY contain data that indicate usage limits.

The policy defined in this TSCP applies to certificates issued to the public and place no constraints on the user community and applicability of the certificate.

1.4.1 Appropriate certificate uses

Through the use of appropriate protocols certificates can be used for server or client authentication, signature creation/verification or encryption and decryption.

1.4.2 Prohibited certificate uses

No stipulation.

1.5 Policy administration

Revisions to this TSCP is available to *Subscribers* and *Relying parties*.

1.5.1 Organization administering the document

This TSCP 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

Phone: +370.700.22722

Fax: +370.700.22715

Email: info@ssc.lt

1.5.3 Person determining TSCPS suitability for the policy

A person appointed by the Board of the company has the authority and responsibility for approving the certification practice statements.

1.5.4 TSCPS approval procedures

TSP SHALL identify which of the policies defined in the present document it adopts plus any variances it chooses to apply.

A body with final authority and responsibility reviews and evaluates how the TSCP is supported by a TSCPS. The TSP SHALL make available the TSCPS to its community[4]. Notice SHALL be given within a reasonable time to all relying parties and cross-certified TSPs of changes to this document.

1.6 Definitions and acronyms

For the purposes of the present document, the terms and definitions given in: ETSI TR 119 001, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI EN 319 421 apply.

4 The TSP's user community includes: the subscribers/subjects eligible to hold certificates issued under the TSCP and any parties which MAY require relying upon those certificates.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The TSPs issuing certificates under this TSCP are obligated to post all TSP certificates issued by or to the TSP and CRLs issued by the TSP in a repository that is publicly accessible through Uniform Resource Identifier (URI) references asserted in its valid certificates.

The repositories MAY be operated by the TSP or be delegated to a third party. In the latter case, the subject TSP SHALL retain adequate control to insure that the requirements of this TSCP are met. The TSCPS SHALL document any such third-party repository relationship.

The TSCP is publicly available on the TSP's website: http://gdl.repository.ssc.lt/CP

2.2 Publication of certification information

The TSP SHALL ensure that certificates are made available as necessary to subscribers and subjects.

Upon system failure, service or other factors which are not under the control of the TSP, the TSP SHALL apply best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the TSCPS.

2.3 Time or frequency of publication

The repository information SHALL be published promptly upon issuance or acceptance by the TSP.

2.4 Access controls on repositories

No access control SHALL be applied for retrieving the TSCP, TSCPS and CRLs.

The TSP SHALL insure that appropriate access controls are in place to prevent unauthorized writing, modifying, or deleting of repository items.

3 IDENTIFICATION AND AUTHENTICATION

Certificates issued to any *Subscriber* under this TSCP SHALL have a distinguished names according to ETSI EN 319 412-2 and ETSI EN 319 412-3.

3.1 Naming

This policy does not restrict the names of Root TSPs and Issuing TSPs.

3.1.1 Types of names

Types of names SHALL be specified in the TSCPS.

3.1.2 Need for names to be meaningful

The certificates issued pursuant to this TSCP are meaningful only if the *distinguished names* can be understood by *Relying parties*.

While the issuer name in TSP certificates is not generally interpreted by *Relying parties*, this TSCP still requires use of meaningful names. The CN attribute SHOULD describe the issuer, such as:

CN= SSC GDL Class 1-2 CA

3.1.3 Anonymity or pseudonymity of subscribers

Anonymity or pseudonymity of subscribers SHALL be specified in the TSCPS.

3.1.4 Rules for interpreting various name forms

Rules for interpreting name forms shall be specified in the TSCPS.

3.1.5 Uniqueness of names

The TSP operating under this TSCP SHALL ensure that the *distinguished name* is unambiguous for all *Subjects* within the domain of the TSP.

3.1.6 Recognition, authentication, and role of trademarks

Recognition, authentication and role of trademarks SHALL be specified in the TSCPS.

3.2 Initial identity validation

The TSP, operating under his TSCP, SHALL ensure the evidence of S*ubscriber*'s and *Subject*'s identification and accuracy of their names and associated data. Where applicable, the identity validation MAY be concluded through appropriate and authorized sources. The RA SHALL ensure that certificate requests are accurate, authorized and complete according to the collected evidence or attestation.

If certificates are issued to a device or service, the TSP SHALL document the designation of a person responsible for the associated device or service.

3.2.1 Method to prove possession of private key

The registration process SHALL request the Subject to demonstrate possession of the private key. This process SHALL be specified in the TSCPS.

3.2.2 Authentication of organization identity

Authentication of organization identity SHALL be specified in the TSCPS. The TSP SHALL identify high risk certificate applications and SHALL perform additional preventive verification activity necessary to ensure that high risks requests are properly verified.

3.2.3 Authentication of individual identity

Under regular conditions, the *Subject* MUST personally appear before the RA and be visually authenticated. Exceptions MAY be made for cases when it is impossible or impractical to have the

Subject appear in person. The conditions and the requirements for authorization and approval of such requests, SHALL be specified in the associated TSCPS.

3.2.4 Non-verified subscriber information

Non-verified *Subscriber* information SHALL not be included in certificates.

3.2.5 Validation of authority

The procedure of authority validation SHALL be specified in the TSCPS.

3.2.6 Criteria for interoperation

The TSP MAY provide interoperability services to third party TSPs or application developers. The criteria for interoperation SHALL be provided in the contract between the parties. The contact provisions SHALL NOT contradict to the requirements of this TSCP.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

TSP certificate re-key SHALL follow the same procedures as initial certificate issuance.

Subject certificate re-key SHALL be specified in the TSCPS.

3.3.2 Identification and authentication for re-key after revocation

Identification and authentication of a *Subject* for re-key after revocation SHALL depend upon the revocation reason. The TSCPS SHALL specify the conditions under which this is allowed.

3.4 Identification and authentication for revocation request

Identification and authentication for revocation request SHALL be specified in the TSCPS.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The TSP SHALL have a TSCPS and procedures to address all the requirements identified in this TSCP. The TSCPS SHALL identify the obligations of all external organizations supporting the TSP operations including the applicable policies and practices. The TSP SHALL make available to *Subscribers* and *Relying parties* its TSCPS and other relevant documentation, as necessary to assess conformance to the service policy.

The TSP is not required to make all the details of its practices public.

4.1 Certificate Application

The Certificate application process MUST provide sufficient information to establish the *Subscriber*'s authorization to obtain a certificate, establish and record identity of the *Subscriber,* obtain the *Subject*'s public key to verify his/her possession of the private key for the requested certificate, verify any other information requested for inclusion in the certificate.

4.1.1 Who can submit a certificate application

Who can submit a certificate application MUST be specified in the TSCPS.

4.1.2 Enrollment process and responsibilities

Enrollment process and responsibilities SHALL be specified in the TSCPS.

4.2 Certificate application processing

TSP operating under this TSCP SHALL specify procedures to verify information in certificate applications. To prevent phishing and other fraudulent attacks the TSP operating under this TSCP SHALL identify high risk certificate applications.

4.2.1 Performing identification and authentication functions

Performing identification and authentication functions SHALL be specified in the TSCPS.

4.2.2 Approval or rejection of certificate applications

TSP SHALL disclose to Subscribers the potential reasons of application rejection.

4.2.3 Time to process certificate applications

Time to process certificate application MUST be specified in the TSCPS.

4.3 Certificate issuance

The certificate issuance shall be specified in the TSCPS.

4.3.1 TSP actions during certificate issuance

The TSP SHALL ensure that requests for certificates 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 *Subject*'s identity information.

4.3.2 Notification to subscriber by the TSP of issuance of certificate

TSPs operating under this policy MUST inform the S*ubscriber* of the generation of a certificate.

4.4 Certificate acceptance

The TSP SHALL ensure that certificates are made available as necessary to *Subscribers*, *Subjects* upon generation.

4.4.1 Conduct constituting certificate acceptance

The TSCPS SHALL specify how Subscribers accept certificates.

4.4.2 Publication of the certificate by the TSP

The TSP MUST publish its Root and Issuing TSP certificates and MAY also publish *Subject* certificates.

4.4.3 Notification of certificate issuance by the TSP to other entities

The company board MUST be notified whenever a Root TSP operating under this TSCP issues a TSP certificate.

4.5 Key pair and certificate usage

The scope of usage for a key pair SHALL be specified in the usage extensions of certificates. The TSCPS SHOULD specify specific restrictions, if any.

4.5.1 Subscriber private key and certificate usage

No stipulation.

4.5.2 Relying party public key and certificate usage

No stipulation.

4.6 Certificate renewal

Renewing means generation of a new certificate with the same *Subject distinguished name*, *public key* and other information as in an existing certificate. The existing certificate MAY or MAY NOT be revoked.

The TSP MAY issue a new certificate using the S*ubject's* previously certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the S*ubject's* private key has been compromised.

4.6.1 Circumstance for certificate renewal

TSP Certificates and OCSP responder certificates MAY be renewed if the aggregated validity of the renewed certificate does not exceed the certificate validity period.

4.6.2 Who may request renewal

TSP MAY request renewal of its own TSP certificate or OCSP responder certificate.

4.6.3 Processing certificate renewal requests

Any Root CA or Issuing CA certificate renewal[5] MUST be approved by the person appointed by the Board of SSC.

4.6.4 Notification of new certificate issuance to subscriber

The TSP MUST inform the S*ubscriber* of the renewal of certificate.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the TSP

No stipulation.

4.6.7 Notification of certificate issuance by the TSP to other

No stipulation.

5 For reasons other than re-key of the associated Root TSP certificate

4.7 Certificate re-key

Re-keying means generating new certificates with a new public key while retaining the remaining contents of the existing certificate.

The new certificate MAY have a different validity period, specify a different *CRL DP* and be signed by a different *Issuing TSP*.

The TSP SHALL ensure that requests for certificates issued to a S*ubject* who has previously been registered with the same TSP 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 attributes.

4.7.1 Circumstance for certificate re-key

Possible circumstances requiring certificate re-key might be expiration, key compromise, hardware token replacement.

4.7.2 Who may request certification of a new public key

Subscribers with a valid certificate MAY request re-key. RAs MAY request certification of a new public key on behalf of a *Subject*. For device/service certificates, the responsible person MAY request certification of a new public key.

4.7.3 Processing certificate re-keying requests

Signed re-key requests SHALL be validated before proceeding with the request processing. Re-key requests MAY also be processed using initial certificate issuance process.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the TSP

No stipulation.

4.7.7 Notification of certificate issuance by the TSP to other entities

No stipulation.

4.8 Certificate modification

Modifying a certificate means generating a new certificate that has the same or a different key and differs in one or more other fields from the old certificate.

The old certificate MAY or MAY not be revoked.

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the TSP

No stipulation.

4.8.7 Notification of certificate issuance by the TSP to other entities

No stipulation.

4.9 Certificate revocation and suspension

TSPs operating under this TSCP SHALL issue CRLs covering all unexpired certificates except for OCSP responder certificates with the *id-pkix-ocsp-nocheck* extension.

TSPs operating under this policy SHALL make public a description of how to obtain revocation information. This information SHALL be given to S*ubscribers* during certificate request or issuance, and SHALL be readily available to any *Relying party*.

Revocation requests MUST be authenticated. Requests to revoke a certificate MAY be authenticated using that certificate's associated private key.

Certificate suspension for TSP certificates is not allowed by this policy. However, the use of certificate suspension for *Subject* certificates MAY be allowed.

The TSP SHALL provide a mechanism to insure that invalidated certificates are promptly revoked. The revocation mechanism SHALL allow certificate users to obtain timely and unambiguous knowledge of the revocation status of any certificate issued by the TSP. The revocation mechanism SHALL be specified in the TSCPS.

4.9.1 Circumstances for revocation

Certificates SHALL be revoked when the private key or activation data associated with the certificate is compromised. Key compromise includes unauthorized access to private keys or

activation data, loss of private keys or activation data, stolen or destroyed keys.

4.9.2 Who can request revocation

The TSCPS SHALL identify the entities that MAY request revocation of a certificate.

The TSP SHALL also specify the manner in which a revocation request MAY be generated, and how it is processed. All revocation requests, reasons for revocation, and the resulting actions taken by the TSP SHALL be documented.

4.9.3 Procedure for revocation request

Certificate revocation request SHALL identify the certificate to be revoked, indicate the reason for revocation, and allow authentication. The process of certificate revocation SHALL be detailed in the TSCPS.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which TSP must process the revocation request

TSPs MUST revoke certificates as quickly as practical upon receipt of a proper revocation request.

Revocation requests SHALL be processed before the next CRL is published, excepting those requests received within four hours of CRL generation.

4.9.6 Revocation checking requirement for relying parties

Because use of revoked certificates MAY cause damaging consequences, the *Relying parties* are recommended to always check validity of certificates.

4.9.7 CRL issuance frequency

CRLs SHALL be issued periodically, even if there are no revocation status change. Where CRL are used as the sole means of providing revocation status information:

- every CRL SHALL state a time for next scheduled CRL issue;
- a new CRL MAY be generated before the stated time of the next CRL issue;
- the CRL SHALL be signed by the TSP or other authorized service.

The details of CRL publication SHALL be specified in the TSCPS.

4.9.8 Maximum latency for CRLs

CRLs SHALL be published as soon as possible after generation.

4.9.9 On-line revocation/status checking availability

TSPs SHALL support on-line status checking via OCSP RFC6960 where status information MUST be updated and available to relying parties within 24 hours of certificate revocation.

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

A TSP MAY also use other methods of status announcement which MUST be described in the TSCPS.

4.9.12 Special requirements re-key compromise

TSP certificate MUST be revoked within 4 hours of notification.

4.9.13 Circumstances for suspension

TSP MAY provide a certificate suspension service. Unlike the revocation, suspension allows to re-enable the certificate. The expiry date of suspended certificate remains unchanged.

4.9.14 Who can request suspension

In case, if the TSP offers the certificate suspension service, the TSP MUST accept the *Subscriber's* request to suspend the validity of the certificate.

4.9.15 Procedure for suspension request

The TSP SHALL authenticate the person requesting certificate suspension.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

No stipulation.

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

No stipulation.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

TSP private keys SHALL never be escrowed.

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The TSP SHALL ensure that administrative and management procedures are applied and adequate to recognized best practice[6].

The TSP SHALL retain responsibility for all aspects of its operations, whether or not functions are outsourced. Responsibilities of third parties SHALL be clearly defined by the TSP and appropriate arrangements to ensure that third parties are bound to implement controls required by the TSP.

The information security infrastructure necessary to manage the security within the TSP SHALL be maintained at all times. Any changes that will impact on the level of security provided SHALL be approved by the TSP management body.

TSP's security policy (SP) SHALL be documented[7], implemented and maintained including the security controls and operating procedures for TSP facilities, systems and information assets. The TSP SHALL ensure that the system components are secure and correctly operated, with acceptable risk of failure:

- the integrity of TSP components and information SHALL be protected against viruses, malicious and unauthorized software;
- incident reporting and response procedures SHALL be employed in such a way that damage from security incidents and malfunctions SHALL be minimized;
- procedures SHALL be established and implemented for all trusted and administrative roles that impact on the provision of services.

6 The TSP SHALL carry out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. The risk assessment SHALL be regularly reviewed and revised (ISO/IEC 27001, ISO/IEC 27002). The TSP SHALL ensure that its assets, including information assets, receive an appropriate level of protection, SHALL maintain an inventory of all information assets and assign a classification consistent with the risk assessment.

7 The security policy SHOULD identify all relevant targets, objects and potential threats and the safeguards required to avoid or limit the effects of those threats, consistent with the risk assessment. It SHOULD describe the rules, directives and procedures regarding how the specified services and the associated security assurance are granted in addition to stating policy on incidents and disasters.

Where security measures and controls required by this TSCP are already in place as part of existing TSP practice, appropriate documents SHALL be cited in the TSCPS either by their names or OIDs.

5.1 Physical controls

All the physical control requirements specified in this TSCP apply to Root CAs, Issuing CAs and all TSP and RA information system workstations except where specifically noted.

The CA issuing certificates under this TSCP SHALL ensure that physical access to critical services is controlled and risks related to physical and environmental security[8] minimized:

- physical access to facilities concerned with sensitive services[9] SHALL be limited to properly authorized individuals;
- controls SHALL be implemented to avoid loss, damage or compromise of assets and interruption to business activities;
- controls SHALL be implemented to avoid compromise or theft of information and information processing facilities.

The certificate generation, *Subject* device provisioning and revocation management SHALL be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data, persons entering this physically secure area SHALL not be left for any significant period without oversight by an authorized person. The facilities SHALL have physical barriers around the certificate generation, subject device preparation and revocation management services. No parts of the premises can be shared with any other organization.

Physical and environmental security controls SHALL be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The TSP's physical and environmental SP for systems concerned with certificate generation, subject device preparation and revocation management services SHALL address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities structure collapse,

8 Guidance according to ISO/IEC 27002.

9 Sensitive services are those identified through the TSP's risk assessment.

plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

Controls SHALL be implemented to protect against equipment, information, media and software relating to the TSP services being taken off-site without authorization.

5.1.1 Site location and construction

The location and construction of the facility housing the TSP's equipment, as well as sites housing TSP's workstations used to administer the TSP, SHALL be consistent with facilities for high-value, sensitive information.

5.1.2 Physical access

The physical access controls SHALL ensure that no unauthorized access to the hardware is permitted.

If the facility is not continuously attended, the last person to depart SHALL initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3 Power and air conditioning

The TSP SHALL have backup capability sufficient to finish any pending actions, and record the state of the equipment automatically before a shutdown caused by lack of power or air conditioning.

The repository SHALL be provided with uninterrupted power sufficient for at least of 8 hours operation in the absence of commercial power.

5.1.4 Water exposures

TSP equipment SHALL be installed on elevated floors with no danger of exposure to water.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

All media SHALL be handled securely in accordance with requirements of the information classification scheme.

Media containing sensitive data SHALL be securely disposed of when no longer required. Media used within the TSP systems SHALL be securely handled to protect media from damage, theft, unauthorized access and obsolescence.

5.1.7 Waste disposal

Media and documentation with sensitive data that are no longer needed SHALL be destroyed in a secure manner.

5.1.8 Off-site backup

Data and system backups sufficient to recover from failure SHALL be made on a periodic schedule and described in the TSCPS.

5.2 Procedural Controls

The TSP SHALL use trustworthy systems and products that are protected against modification[10].

An analysis of security requirements SHALL be carried out at the design and requirements specification stage of any systems development project undertaken by the TSP or on behalf of the TSP to ensure that security is built into TSP systems. Change control procedures SHALL be applied

10 The risk assessment carried out on the TSP operation SHOULD identify its critical components requiring trustworthy systems and the levels of assurance required. Requirements for the trustworthy systems ensured using systems conforming to a suitable protection profile, defined in accordance with ISO/IEC 15408.

for releases, modifications and emergency software fixes of any operational software.

These security operations SHALL be separated from other operations:

- TSP operational procedures and responsibilities;
- secure systems planning and acceptance;
- protection from malicious software;
- backups;
- network management;
- active monitoring of audit logs, event investigation and follow-up;
- media handling and security;
- data and software exchange.

These operations SHALL be managed by trusted personnel, but, MAY actually be performed by, non-specialist, operational personnel under supervision.

5.2.1 Trusted Roles

The TSP operating under this TSCP SHALL identify trusted roles in its TSCPS.

5.2.2 Number of persons required per task

The TSP operating under this TSCP SHALL identify critical operations requiring two or more persons[11] in its TSCPS.

5.2.3 Identification and authentication for each role

All TSP roles SHALL require two factor authentication before anyone being permitted to perform any actions set forth for that role.

5.2.4 Roles requiring separation of duties

A TSP operating under this TSCP SHALL separate these three roles: Information system

11 to be presented and be aware of the nature of current operations.

security supervisor, System Administrator and the TSP Administrator.

Separation of duties SHALL be acceptable with the condition that the resilience to insider attack is strong and the roles identified in the TSCPS.

5.3 Personnel Controls

The TSP operating under this TSCP SHALL ensure that personnel and hiring practices enhance and support the trustworthiness of the TSP's operations.

TSP personnel in sensitive positions SHALL be appointed in writing and have received proper training in the performance of their duties.

5.3.1 Qualifications, experience, and clearance requirements

The requirements governing the qualifications, experience and clearance of individuals who operate, manage, oversee, and audit the TSP SHALL be set forth in the TSCPS.

5.3.2 Background check procedures

TSP personnel SHALL, at a minimum, pass a background investigation covering the following areas: employment, education, place of residence, Law enforcement and references.

The period of investigation MUST cover at least the last five years for each area, excepting the residence check which MUST cover at least the last three years.

Regardless of the date of award, the highest educational degree SHALL be verified.

5.3.3 Training requirements

TSP and RA personnel SHALL receive comprehensive job training.

5.3.4 Retraining frequency and requirements

Personnel responsible for PKI roles SHALL be made aware of changes in the TSP operation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

The TSP SHALL take administrative and disciplinary actions against personnel who have performed unauthorized actions involving the TSP, RA operating under this TSCP, appropriate TSCPS or other defined procedures.

5.3.7 Independent contractor requirements

Contractors fulfilling *trusted roles* are subject to all personnel requirements stipulated in this TSCP.

5.3.8 Documentation supplied to personnel

Each role SHALL be provided with documentation explaining applicable duties and procedures.

5.4 Audit logging procedures

Audit log files or reports SHALL be generated for all events relating to the security of the TSP.

5.4.1 Types of event recorded

The types of event recorded SHALL include all operating system level security events and TSP/RA application events. The TSCPS or an internal TSP document SHALL detail the types of events.

5.4.2 Frequency of processing log

Review of the audit log verifying that the log has not been tampered with and then briefly inspecting all log entries SHALL be required every week. In case of suspicious events more thorough investigation SHALL be arranged.

5.4.3 Retention period for audit log

The audit logs SHALL be retained on-site for at least 6 months.

5.4.4 Protection of audit log

The TSP SHALL implement procedures that protect audit logs from destruction prior to the end of the audit log retention period.

The off site storage MUST be a safe and secure location that is separate from the location where the audit logs were generated.

5.4.5 Audit log backup procedures

Audit logs and audit summaries SHALL be backed up at least monthly. A copy of the audit log SHALL be sent off-site on a monthly basis.

5.4.6 Audit collection system (internal vs. external)

Audit collection systems SHALL be configured so that security audit data is protected against loss.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessment

Audit logs SHALL be monitored or reviewed regularly to identify evidence of malicious activity.

5.5 Records Archival

Records concerning certificates include registration information and information concerning significant TSP environmental, key management and certificate management events.

The TSP SHALL ensure that all relevant information concerning the operation of services is recorded for a defined period of time, in particular for the purpose of providing evidence for the purposes of legal proceedings.

5.5.1 Types of records archived

No stipulation.

5.5.2 Retention period for archive

The minimal retention period for achieve is 10 (ten) years.

5.5.3 Protection of archive

No unauthorized user SHALL be permitted to write to, modify, or delete the archive. Archive media SHALL be stored in a safe, secure storage facility.

5.5.4 Archive backup procedures

TSP systems data necessary to resume TSP operations SHALL be backed up and stored in

safe places suitable to allow the TSP to timely go back to operations in case of incident/disasters[12].

Back up and restore functions SHALL be performed by the relevant trusted roles[13].

5.5.5 Requirement for time-stamps of records

TSP archive records SHALL be automatically time-stamped as they are created.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key Changeover

The TSP SHALL ensure that TSP private signing keys are not used beyond the end of their life cycle. All copies of the TSP private signing keys SHALL be destroyed or rendered unusable at the end of their life cycle.

5.7 Compromise and disaster recovery

Business Continuity ensures that the TSP services are quickly and securely restored in case of system failure. Following services MUST withstand a single failure, and continue uninterrupted operations: Dissemination Service, Revocation Management Service, Revocation Status Service.

The TSP SHALL ensure in the event of a disaster, including compromise of its private

12 In line with ISO/IEC 27002, clause 10.5.1: *Back-up copies of essential information and software SHOULD be taken regularly. Adequate back-up facilities SHOULD be provided to ensure that all essential information and software can be recovered following a disaster or media failure. Back-up arrangements SHOULD be regularly tested to ensure that they meet the requirements of business continuity plans.*

13 If risk analysis identifies information requiring dual control for management, for example keys, then dual control SHOULD be applied to recovery.

signing key or trust service credentials, operations are restored as soon as possible. In particular, the TSP SHALL define and maintain a continuity plan to enact in case of a disaster[14].

In the case of compromise the TSP SHALL as a minimum provide the following undertakings:

a) inform all subscribers and other entities with which the TSP has agreements or other form of established relations, among which Relying parties and TSPs;

b) indicate that certificates and revocation status information issued using this TSP key MAY no longer be valid;

c) when a TSP is informed of the compromise of another TSP, any TSP certificate that has been issued for the compromised TSP, is revoked.

SHOULD any of the algorithms, or associated parameters, used by the TSP or its *Subscribers* become insufficient for its remaining intended usage then the TSP SHALL:

- inform all *Subscribers* and *Relying parties* with whom the TSP has agreement or other form of established relations. In addition, this information SHALL be made available to other relying parties;
- revoke any affected certificate.

5.7.1 Incident and compromise handling procedures

The TSP SHALL act in a timely and coordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents SHALL be reported as soon as possible after the incident.

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

When computing resources, software, and/or data are corrupted, TSPs operating under this TSCP SHALL:

- Before returning to operation, ensure that the system's integrity has been restored;
- If the TSP signature keys are not destroyed, TSP operation SHALL be

14 Other disaster situations include failure of critical components of a TSP system, including hardware and software.

reestablished, giving priority to the ability to generate CRL within the issuance schedule;

➢ If the TSP signature keys are unusable, TSP operation SHALL be reestablished as quickly as

➢ possible, giving priority to the TSP key recovery or generation of a new TSP key pair.

5.7.3 Entity private key compromise procedures

The TSP's business continuity plan[15] SHALL address the compromise or suspected compromise of a TSP's private signing key as a disaster and the planned processes SHALL be in place.

Following a disaster the TSP SHALL, where practical, take steps to avoid repetition of a disaster[16].

5.7.4 Business continuity capabilities after a disaster

TSPs operating under this TSCP SHALL have recovery procedures to reconstitute the TSP as soon as possible. In the case of the TSP installation is physically damaged and the TSP signature key is destroyed, the designated national authority SHALL be notified and the TSP SHALL take whatever action it deems appropriate.

5.8 TSP or RA termination

Operation of the TSP or RA MAY be terminated for convenience, contract expiration, re-organization, or other non-security related reasons. In this case, the TSP SHALL attempt to notify all *Subjects* and *Relying parties* of the termination. Certificates MAY continue to be considered valid at the discretion of the *Relying party*.

15 Or "Disaster recovery plan".

16 Guidance procedures according to ISO/IEC 27002.

The designated authority MUST be notified immediately of the intent to terminate an operating TSP.

The TSP SHALL ensure that potential disruptions to *Subscribers* and *Relying parties* are minimized as a result of the cessation of the TSP operation. Before the TSP terminates its operation the following procedures SHALL be executed:

a) the TSP SHALL inform all *Subscribers* and other entities with which the TSP has agreements or other form of established relations;

b) the TSP SHALL terminate authorization of all subcontractors to act on behalf of the TSP;

c) the TSP SHALL transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period;

d) TSP private keys, including backup copies, SHALL be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.

In addition regarding the requirement:

➢"*the TSP shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP operation for a reasonable period*" this SHALL apply to registration and revocation status information for their respective period of time as indicated to the S*ubscriber* and *Relying party*;

➢"*The TSP shall state in its practices the provisions made for termination of service*" this SHALL also include the handling of the revocation status for unexpired certificates that have been issued.

6 TECHNICAL SECURITY CONTROLS

This section contains provisions for CAs, RAs, *Subjects* and the corresponding technical controls.

The TSP SHALL ensure that cryptographic device throughout its life-cycle is not tampered with during shipment. The TSP SHALL ensure that private signing keys stored on the cryptographic hardware are destroyed upon device retirement.

Where security measures and controls are already in place as part of existing TSP, these policies SHALL be cited in the TSCPS.

6.1 Key Pair Generation & Installation

Every Issuing CA SHALL have its own signing key pair.

Subscribers MAY generate their own key pairs or have their key pairs generated by a CA, RA, or other authorized person, provided that the all relevant requirements of this TSCP are met.

6.1.1 Key pair generation

The TSP key generation SHALL be carried out within one of the following devices:

a) meets the requirements identified in either CEN Workshop Agreement 14167-2 or CWA 14167-3 or CWA 14167-4;

b) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408, or equivalent security criteria.

The TSP key generation SHALL be performed according to a documented key generation ceremony using an algorithm and key length recognized by industry and witnessed by the TSP"s Qualified Auditor in order to observe the process and the controls over the integrity and confidentiality of the Root CA Key Pairs produced. A video of the entire key generation ceremony will be recorded for auditing purposes.

6.1.2 Private key delivery to subscriber

Private keys MAY be delivered electronically or MAY be delivered on a HSM. In all cases, the following requirements MUST be met:

Personnel generating a *Subject* signing key SHALL not retain any copy of the key after to the subscriber. The private key MUST be protected from activation, compromise, or modification during the delivery process. The S*ubscriber* SHALL acknowledge receipt of the private key.

6.1.3 Public key delivery to certificate issuer

TSP public keys SHALL be protected against modification or substitution during delivery to the certificate user. The TSCPS SHALL specify the mechanism for delivery.

6.1.4 TSP public key delivery to relying parties

The TSP SHALL ensure that the integrity and authenticity of the TSP public key and any associated parameters are maintained during its distribution to relying parties. TSP public keys SHALL be made available to relying parties in a manner that assures the integrity of the TSP public key and authenticates its origin.

6.1.5 Key sizes

Certificates issued under this TSCP SHALL contain RSA or elliptic curve public keys with the industry recommended key sizes.

6.1.6 Public key parameters generation and quality checking

No stipulation.

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

The use of a specific key MAY be constrained by the *KeyUsage* extension and all certificates SHALL include a critical key usage extension if applicable.

Public keys that are bound into subscriber certificates SHALL be used only for signing or encrypting, but not both.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The TSP certificate signing keys SHALL only be used within physically secure premises. The Subject private keys SHALL never be made available to any party other than the subject.

6.2.1 Cryptographic module standards and controls

TSPs that issue certificates under QCP+ SHALL use a FIPS 140 Level 3 or higher validated hardware cryptographic module according to COMMISSION IMPLEMENTING DECISION 2014/148/EU amending Decision 2011/130/EU establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

The TSP private signing key SHALL be held and used within a secure cryptographic device which: meets the requirements identified in ISO/IEC 19790[17] or one of the following: CEN Workshop Agreement 14167-2, CWA 14167-3, CWA 14167-4 or is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 or equivalent security criteria.

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

17 level 3 or higher. Demonstrated conformance to FIPS PUB 140-2 level 3 is considered as fulfillment of this requirement.

A single person SHALL not be permitted to activate or access any HSM the TSP private signing key. TSP signature keys MAY be backed up only under two-person control. Access to TSP signing keys backed up for disaster recovery SHALL be under at least two-person control. The names of the parties used for two-person control SHALL be maintained on a list that SHALL be made available for inspection during compliance audits.

6.2.3 Private key escrow

The TSP SHALL not hold subject private keys once they have been delivered to the subject, if the subject's key is to be used for electronic signatures with the meaning of [Directive 1999/93/EC].

The TSP operating under this TSCP SHALL never escrow its private keys.

6.2.4 Private key backup

Backup procedure SHALL be presented in the TSCPS.

6.2.5 Private Key archival

TSP and subscriber private signatures keys SHALL not be archived.

6.2.6 Private key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private key storage on cryptographic module

The TSP SHALL ensure that TSP private keys remain confidential, maintain their integrity and are not used beyond the end of their life cycle.

6.2.8 Method of activating private key

For digital signature certificates the subscriber MUST be authenticated to the

cryptographic token before the activation of the associated private key. Cryptographic modules that have been activated SHALL not be available to unauthorized access.

6.2.9 Method of deactivating private key

After use, the cryptographic module SHALL be deactivated either via log-out or automatically after a period of inactivity.

6.2.10 Method of destroying private key

Individuals in trusted roles SHALL destroy private keys when they are no longer needed.

Subscribers SHALL either surrender their cryptographic module to TSP personnel for destruction or destroy[18] their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are revoked.

6.2.11 Cryptographic Module Rating

According to section 6.2.1 .

6.3 Other aspects of Key Pair Management

6.3.1 Public key archival

Certificate archival requirements SHALL apply.

6.3.2 Certificate operational periods and key pair usage periods

The Root and Issuing CA key pair validity SHALL not be longer than 20 years. The *Subject* key pair operational period SHALL not exceed 5 years.

18 According to cryptographic module manufacturer's documentation.

The maximum usage period for OCSP responders operating under this TSCP SHALL be 5 years.

6.4 Activation Data

6.4.1 Activation data generation and installation

If the activation data MUST be transmitted, it SHALL be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module. Subscriber activation data MAY be user-selected.

6.4.2 Activation data Protection

Activation data SHALL be protected from disclosure by a combination of cryptographic and physical access control mechanisms.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

The TSP SHALL require each user to identify him/herself and be successfully authenticated before allowing any action on behalf of that user or role. Re-authentication MUST be mandatory after log-out. Authentication data, where used, MUST be unique and not reused.

6.5.1 Specific computer security technical requirements

Mandatory computer security controls specified below SHALL ensure that the TSP operations are performed according to this TSCP:

- access authentication;

- security audit;
- separation of roles/duties for sensitive functions;
- recovery mechanism for keys and the TSP system.

Any communications between a trusted role and the TSP SHALL be authenticated and protected.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

The system development controls SHALL be specified in the TSCPS.

6.6.2 Security management controls

TSP operating under this TSCP SHALL use System Access Control functions that control use of all sensitive objects of the TSP system by authorized persons only. System Access Control MAY be provided either, by the underlying operating software, or directly by the actual component itself. Access rights to specific TSP objects are determined by the owner of the object based on the identity of the subject attempting the access.

6.6.3 Life cycle security ratings

No stipulation.

6.7 Network security controls

The TSP SHALL ensure that network components are kept In a physically secure environment and

their configurations periodically audited for compliance with the requirements specified by the TSP.

Continuous monitoring and alarm facilities SHALL be provided to enable the TSP to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

6.8 Time-stamping

The TSP SHALL ensure that its network is synchronized to an official time source. This requirement is separate from the time-stamping service requirements of the TSP.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

Certificates issued under this TSCP SHALL conform to the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile.

X.509 v3 certificates contain the identity and attribute data with applicable extensions. All certification paths start from a trust anchor. A trust anchor is a Root TSP that a user trusts based on out-of-band knowledge.

More detailed information about X.509 certificates can be found in Recommendation X.509 and [RFC5280].

Profiles of certificates issued under this TSCP SHOULD be presented in the TSCPS.

7.1.1 Version number

The TSP SHALL issue X.509 v3[19] certificates.

7.1.2 Certificate extensions

Rules for certificate extensions SHALL be presented in the TSCPS.

7.1.3 Algorithm object identifiers

Rules for algorithm OIDs SHALL be presented in the TSCPS.

7.1.4 Name forms

Name forms SHALL be presented in the TSCPS.

19 The version value equal to 2.

7.1.5 Naming constraints

The TSPs MAY assert name constraints in TSP certificates.

7.1.6 Certificate policy object identifier

Certificate policy OIDs SHALL be presented in the TSCPS.

7.1.7 Usage of Policy Constraints extension

The TSPs MAY assert *Policy Constraints* in TSP certificates.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL Profile

TSPs use CRLs to publish the revocation of a subject's certificate. The CRLs are stored in the Repository and are checked by relying parties to verify their status. The content of a CRL identify the issuer, the date the current CRL was generated, the date by which the next CRL will be generated, and the revoked users' certificates.

7.2.1 Version number(s)

The TSPs SHALL issue X.509 Version two CRLs.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

The OCSP signing certificate profile SHALL be presented in the TSCPS.

7.3.1 Version number(s)

The TSP operating under this TSCP SHALL use version 1.

7.3.2 OCSP extensions

Critical OCSP extensions SHALL not be used.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

TSPs operating under this TSCP SHALL have a compliance audit mechanism. This TSCP does not impose a requirement for any particular assessment methodology, however the TSP conformance SHALL be checked on a regular basis and whenever major change is made to the TSP operations.

For the TSP time-stamping services the TSA SHALL apply requirements in ETSI EN 319 421.

8.1 Frequency or circumstances of assessment

TSPs and RAs operating under this policy SHALL be subject to a periodic compliance.

8.2 Identity/qualifications of assessor

The compliance auditor MUST perform compliance audits as a regular business activity and MUST be certified according to ETSIEN319403.

8.3 Assessor's relationship to assessed entity

The compliance auditor SHALL be a private firm that is independent from the TSP being audited.

8.4 Topics covered by assessment

A conformant TSP SHALL demonstrate that:

a) it meets SSC GDL TSP obligations and warranties as defined by the TSCP;

b) it has implemented controls which meet the requirements on TSP practices;.

c) it has made available its TSCPS and other relevant documentation to subscribers and relying parties;

d) it has documented the algorithms and parameters employed.

8.5 Actions taken as a result of deficiency

When the auditor finds a discrepancy between the requirements of TSCP or the stipulations in the TSCPS and the operation of the TSP, the following actions SHALL be performed:

The compliance auditor SHALL note the discrepancy;

The TSP will propose a remedy, including expected time for completion.

Depending upon the nature and severity of the discrepancy, and the time required for correction, the TSP MAY decide to temporarily halt operation of the TSP or RA.

8.6 Communication of results

An Audit Report SHALL be provided to the TSP.

9 OTHER BUSINESS AND LEGAL MATTERS

The purpose of this section is to provide the obligations of the parties, and the provisions on liability and the financial/economic issues. In addition, there is the confidentiality section, describing the distinction between confidential information and publicly available and disseminated information. There also stated principles of verification of the TSP activities.

The terms and conditions made available to relying parties SHALL include a notice in order to identify under which conditions is reasonably to rely upon a service:

a) verify the validity, suspension or revocation of the certificate using current revocation status information;

b) take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or the terms and conditions;

c) take any other precautions prescribed in agreements or elsewhere.

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Fees are applied for issuing and renewal of certificates. In any case, fees MUST be clearly set out in the TSCPS.

9.1.2 Certificate access fees

TSPs operating under this policy MAY charge additional fees for access to certain classes or types of certificates it issues.

9.1.3 Revocation or status information access fees

TSPs operating under this TSCP MUST not charge additional fees for revocation and/or CRL access.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage

This TSCP contains no financial limits on the use of certificates issued by CAs under this policy, except QCP-n and QCP-l certificates. Subscribers and Relying parties, SHALL determine what financial limits, if any, they wish to impose for certificates they use.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

No stipulation.

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

The information in the SSC GDL TSP issued certificates and publicly available information in the CRL lists is not considered confidential. If a certificate is terminated, the reasons MAY be given in the certificate revocation list. Date of validity and reason for revocation of certificate are not confidential. In any case, under normal conditions, no other certificate-related information SHALL be undisclosed.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

9.4.1 Privacy plan

The TSPs operating under this TSCP SHALL have a "Privacy and personal data processing statement" to protect personally identifying information from unauthorized disclosure which will be implemented in accordance with the requirements of applicable Law of the Republic of Lithuania.

9.4.2 Information treated as private

TSPs operating under this TSCP SHALL protect all subscriber personally identifying information from unauthorized disclosure. Records of individual transactions MAY be released upon request of any subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by TSPs operating under this policy SHALL not be released except as required by law.

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

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

No stipulation.

9.5.1 Certificates and CRLs

No stipulation.

9.5.2 TSCP/TSCPS

No stipulation.

9.5.3 Trademarks

No stipulation.

9.5.4 Signature creation data

No stipulation.

9.6 Representations and warranties

9.6.1 TSP representations and warranties

The TSP SHALL meet its claims as given in its terms and conditions including the availability and accuracy of its service. The TSP SHALL ensure that all requirements on TSP are implemented as applicable to the selected TSCP. The TSP has the responsibility for conformance with the procedures prescribed in this policy, even when the TSP functionality is performed by third parties.

9.6.2 RA representations and warranties

An RA that performs registration functions SHALL comply with the stipulations of this TSCP.

9.6.3 Subscriber representations and warranties

The TSP SHALL oblige the subscriber[20] to address all the following obligations:

a) accurate and complete information is submitted to the TSP in accordance with the requirements of this TSCP;

b) the key pair is only used in accordance with any limitations notified to the subscriber;

c) reasonable care is exercised to avoid unauthorized use of the subject's private key;

d) subject keys are generated using an algorithm indicated in the applicable TSCPS;

e) a key length and algorithm[21] is used according to the requirements of the applicable TSCPS[22];

f) use the *Subject*'s private key for cryptographic functions within the secure user device only;

g) if the certificate policy requires use of an QSCD[23], only use the certificate with electronic signatures or electronic seals created using such a device;

h) notify the TSP without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:

- the subject's private key has been lost, stolen;
- the subject's private key has been potentially compromised or control over the *Subject*'s private key has been lost due to compromise of activation data or other reasons;
- inaccuracy or changes to the certificate content;
- following compromise, the use of the subject's private key has to be immediately and permanently discontinued;

i) in the case of being informed about issuing TSP's certificate has been compromised, ensure that the certificate is not used by the subject;

j) permit the processing and storage of personal data.

20 If the subject and subscriber are separate entities, the subscriber SHALL make the subject aware of those obligations applicable to the subject.

21 Guidance on algorithms and their parameters according to ETSI TR 119 001, ETSI TR 119 300.

22 If the subscriber or subject generates the key pair for electronic signatures the subject's private key SHOULD have been maintained under the subject's sole control.

23 Applies to QCP-l, QCP-n.

9.6.4 Relying party representations and warranties

The terms and conditions made available to relying parties SHALL include a notice that if it is to reasonably rely upon a certificate, it SHALL:

a) verify the validity, suspension or revocation of the certificate using current revocation status information[24];

b) take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or the terms and conditions supplied;

c) take any other precautions prescribed in agreements or elsewhere.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

TSPs operating under this policy MAY not disclaim any responsibilities described in this TSCP.

9.8 Limitations of liability

The TSP SHALL specify any disclaimers or limitations of liability in accordance with applicable laws.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

This TSCP becomes effective when approved by the authorized person appointed by the Board of the TSP.

24 There MAY be a delay of up to 1 day in disseminating revocation status information.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

The requirements of this TSCP remain in effect through the end of the archive period for the last certificate issued.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

The Board of TSP SHALL review this TSCP at least once every year. Corrections, updates, or changes to this TSCP SHALL be publicly available.

Suggested changes to this TSCP SHALL be communicated to the contact in section 1.5.2 and MUST include a description of the change, a change justification, and contact information of the person requesting the change.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

These rules SHALL be construed in accordance with the Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and legislation of the Republic of Lithuania.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should one section of this TSCP is incorrect or invalid, the other sections of this TSCP SHALL remain in effect until the TSCP is updated.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.

10 REFERENCES

10.1 Normative References

The documents below contain requirements which, if applicable, constitute provisions of this TSCP. For an updated TSCP version the edition of referenced document that is earlier than date of update applies.

[eIDAS] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[ETSI TR 119 001] Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations

[ETSI EN 319 401] Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[ETSI EN 319 411-1] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[ETSI EN 319 411-2] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

[ETSI EN 319 412-2] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

[ETSI EN 319 412-3] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

[ETSI EN 319 421] Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

[ETSI EN 319 412-4] Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations.

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

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

[CABF-EV] CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates.

[ETSIEN319403] Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

10.2 Informative References

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

[ETSI TR 119 300] Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for Cryptographic Suites.

[ETSI TS 119 312] Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[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.

[RFC6960] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

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

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