“eParaksts” Trust service policy

Prepared by:

[PUBLIC]

References:

1. [eIDAS regulation] Regulation (EU) No 910/2014 of 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
2. [ETSI EN 319 411-2] Policy and security requirements for Trust Service Providers issuing certificates Part 2 Requirements for trust service providers issuing EU qualified certificates
3. [ETSI EN 319 411-1] Policy and security requirements for Trust Service Providers issuing certificates Part 1 General requirements
4. [ETSI EN 419 211] Protection profiles for secure signature creation device
5. [CPS] Latvian state radio and television Centre Trust service provider practice statement
6. [Certificate Profile] Latvian State radio and television Centre Trust service provider certificate profiles
7. [ETSI TS 119 312] Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
8. [eID law] Electronic identification law of natural persons
9. General terms and conditions

HISTORY OF CHANGES:

Revised variant No	**Date of entry into force**	**Summary of changes**
01.0	17.05.2017	Initial version
01.1	01.08.2017	Changes regarding product details and requirements

Contents

1. Introduction

1.1. Overview

1.1.1. This document “”eParaksts” Trust service policy” defines the procedural and operational requirements that Latvian State Radio and Television Centre (LVRTC) adheres to and requires entities to adhere to when issuing and managing qualified electronic signature certificates and related certificates for authentication for “eParaksts” trust service.

1.1.2. These certificates promotes the use of electronic signatures and electronic identification of natural persons. Certificates are always issued in pairs - each "eParaksts" service contains one authentication certificate in “eParaksts mobile” mobile device key management application and a qualified electronic signature certificate in “eParakstsTX” solution and their corresponding private keys. Each private key is protected by a separate activation data – Personal Identification Number (PIN).

1.1.3. LVRTC as the TSP issuance of certificates for the "eParaksts" service is guided by [eIDAS regulation] and related standards.

1.1.4. This Policy is based on “QCP-n” policy defined in [ETSI EN 319 411-2] and NCP policy defined in [ETSI EN 319 411-1].

1.1.5. If any requirement specified in this Policy differ from the requirements specified related standards or [CPS], then the documents and requirements specified in those documents should apply in hierarchical order (first in list prevails):

1.1.5.1. [ETSI EN 319 411-2];

1.1.5.2. [ETSI EN 319 411-1];

1.1.5.3. This Policy;

1.1.5.4. [CPS].

1.1.6. This Policy is prepared in Latvian. This Policy May be translated and available in other languages. In case of Policy translation inconsistencies, Policy version in Latvian prevails.

1.1.7. The “eParaksts” service for electronic signatures described in this Policy SHALL be granted qualified status in the Trusted List of Latvia.

1.2. Document Name and Identification

1.2.1. This document is called “”eParaksts” Trust service policy”

1.2.2. This Policy is identified by OID: 1.3.6.1.4.1.32061.2.1.3.1

1.2.3. OID is composed according to the contents of the following table:

Parameter	*OID reference*
ISO	1
Identified Organization	3
DoD	6
Internet	1
Private enterprise	4
IANA registered private enterprise	1
IANA number (LVRTC)	32061
Certification service attribute	2
Type of Policy (Signature)	1
Subtype (eParaksts)	3
Version	1

1.2.4. Qualified electronic signature certificates for “eParaksts” service issued under QCP-n policy contain the following OIDs:

1.2.4.1. 0.4.0.194112.1.0 (QCP-n)

1.2.4.2. 1.3.6.1.4.1.32061.2.1.3.1 (this Policy)

1.2.5. Authentication certificates for “eParaksts” service issued under NPC policy contain the following OIDs:

1.2.5.1. 0.4.0.2042.1.1 (NCP)

1.2.5.2. 1.3.6.1.4.1.32061.2.1.3.1 (this Policy)

1.3. PKI Participants

1.3.1. Certification Authorities

1.3.1.1. Described in the Paragraph 1.3.2. of the [CPS]

1.3.2. Registration Authorities

1.3.2.1. Within this Policy, registration authority is:

1.3.2.1.1. LVRTC in order to manage “eParaksts” service and related certificates;

1.3.2.1.2. SIA “DPD Latvia” courier, acting behalf of LVRTC Registration authority;

1.3.2.1.3. Trust Services Provider’s website www.eparaksts.lv:

1.3.2.1.3.1. Submission of applications for service “eParaksts” signed with qualified electronic signature;

1.3.2.1.3.2. administration of the service “eParaksts” related certificates.

1.3.2.2. Registration Authorities identify applicants and, verify the documentation accrediting the circumstances appearing in the certificates, and validate and approve requests to issue, revoke and renew certificates.

1.3.3. Subscribers

1.3.3.1. The Subscriber is the subject of the certificate issued under this Policy.

1.3.3.2. Subscribers can only be a natural persons.

1.3.4. Relying Parties

1.3.4.1. Relaying parties are legal or natural persons, which shall make decisions on the basis of “eParaksts” created electronic signatures or use of associated authentication certificate..

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses:

1.4.1.1. “eParaksts” related qualified electronic signature certificates are used for creation of advanced electronic signature based on qualified signature certificate which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity.

1.4.1.2. “eParaksts” related authentication certificates are used for authentication of the Subscriber in web or other data processing systems.

1.4.2. Prohibited Certificate Uses:

1.4.2.1. The use of the Certificates issued under this Policy is prohibited for any of the following purposes:

1.4.2.1.1. Unlawful activity (including cyber-attacks and attempts to damage the certificate);

1.4.2.1.2. Issuance of new certificates and information on certificate validity;

1.4.2.1.3. Use of the electronic signature certificate for signing documents which can bring about unwanted consequences (including signing such documents during testing of the systems);

1.4.2.1.4. The use of electronic signature certificates in an automated manner;

1.4.2.1.5. The Subscriber private key transfer to third parties.

1.4.2.2. The Subscriber should not use authentication certificate to create qualified electronic signatures according to [eIDAS] requirements.

1.5. Policy administration

1.5.1. Organization Administering the Document

1.5.1.1. This Policy is administered by State Joint stock company “Latvian State Radio and Television Centre” which acts as Trust service provider under that Policy

1.5.2. Contacts

State Joint stock company "Latvia State Radio and Television Centre"

Address	Erglu street 7, Riga, LV-1012, Latvia
	Trusts service costumer support
Phone	+371 67108787
e-mail	eparaksts@eparaksts.lv
	Office
Phone	+371 67198704
e-mail	lvrtc@lvrtc.lv

1.5.3. Policy Approval Procedures

1.5.3.1. Amendments which do not change the meaning of the Policy, such as corrections of misspellings, translation and updating of contact details, are documented in the Versions and Changes section of the present document and the fraction part of the document version number shall be increased.

1.5.3.2. In the case of substantial changes, the new Policy version is clearly distinguishable from the previous ones. The new version bears a serial

number increased by one. The amended Policy along with the enforcement date, which cannot be earlier than 30 days after publication, is published electronically on the TSP website.

1.5.3.3. All amendments and the final version of this Policy are approved by board of LVRTC.

1.6. Definitions and Acronyms

1.6.1. Definitions

Certificate	public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it
"eParaksts"	Trust service provided by the TSP and contains authentication certificate in "eParaksts mobile" mobile device key management application and qualified electronic signature certificate in "eParakstsTX" solution.
Policy	Within this document – ""eParaksts" Trust service policy"
Subject	entity identified in a certificate as the holder of the private key associated with the public key given in the certificate
eParakstsTX solution	Electronic signature solution in possession of the Subscriber, where electronic signature is created in an environment provided by trust service provider and is used under the sole control of the signatory.
eParakstsTX certificate	Qualified electronic signature certificate in possession of the Subscriber used in eParakstsTX solution for creation of electronic signatures.

1.6.2. Acronyms

CA	Certificate authority
CRL	Certificate revocation list
NCP	Normalized Certificate Policy

OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PUK	Personal unblocking key
PKI	Public Key Infrastructure
RA	Registration authority
QCP-n	Policy for EU qualified certificate issued to a natural person
QSCD	Qualified electronic Signature/Seal Creation Device
TSP	Trust Service Provider – Within this document - LVRTC
RA	Registration authority

2. Publication and Repository Responsibilities

2.1. Repositories

2.1.1. As described in the Paragraph 2.1. of the [CPS]

2.2. Publication of Certification Information

2.2.1. This Policy is published on the TSP website: www.eparaksts.lv

2.3. Time or Frequency of Publication

2.3.1. As described in the Paragraph 2.3. of the [CPS]

2.4. Access Controls on Repositories

2.4.1. As described in the Paragraph 2.5. of the [CPS]

3. Identification and Authentication

3.1. Naming

3.1.1. Types of names

3.1.1.1. The Distinguished Name of any Certificate issued under this Policy SHALL be compiled in accordance with the [Certificate Profile].

3.1.2. Need for Names to be Meaningful

3.1.2.1.1. All the values in the Subject field of a Certificate SHALL be meaningful.

3.1.3. Anonymity or Pseudonymity of Subscribers

3.1.3.1. The TSP does not offer such services.

3.1.4. Uniqueness of Names

3.1.4.1. The TSP shall not issue the certificate with an identical Subscriber's Distinguished Name to different Subscribers.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

3.2.1.1. By mobile device key container, possession of the private key is shown by the reliable procedure of generating the key pair and issuing the certificate. Procedure shall include at least the following controls:

3.2.1.1.1. The User created authentication key protection PIN;

3.2.1.1.2. Unique registration code can only be obtained upon physical or electronic identification;

3.2.1.1.3. The single use registration code can only be received to the verified mobile phone number or email specified in the application.

3.2.1.2. When the key pair is generated by registration authority and keys are stored in the HSM (QSCD) device managed by the TSP, possession of the private key is demonstrated by virtue of the reliable custody of the HSM and the trusted procedure that guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. The procedure involves at least the following controls:

3.2.1.2.1. The Subscriber must be electronically identified in the TSP website www.eparaksts.lv with "eParaksts mobile" authentication or any of the TSP issued smart cards (QSCD);

3.2.1.2.2. The Subscriber themselves must initiate request of eParakstsTX certificate;

3.2.1.2.3. Before issuance of certificate the Subscriber has to establish their own eParakstsTX key protection PIN code;

3.2.1.2.4. The Subscriber at any time on the TSP website www.eparaksts.lv may initiate regeneration of eParakstsTX keys and PIN code change.

3.2.2. Identification and validation of Organization Identity

3.2.2.1. Not applicable.

3.2.3. Identification and validation of Individual Identity

3.2.3.1. Identification and validation of individual identity should be done:

3.2.3.1.1. By the physical presence of the natural person in one of registration authorities. The natural person is identified against the Authoritative source (for example, passport);

3.2.3.1.2. By means of a certificate of a qualified electronic signature – Identity is confirmed by data in a qualified electronic signature which contains electronic time stamp;

3.2.3.2. During identification the TSP shall collect all the necessary evidence, which shall include at least the identifiable person's name, surname, personal identification number and data of presented personal identification document (for example, document type, number, issuer, issuing country).

3.2.3.3. Identification of natural persons is performed by the Registration authority and personnel in trusted roles.

3.2.3.4. Authentication of Individual Identity applying to "eParaksts" service is done by the TSP.

3.3. Identification and validation for Re-Key Requests

3.3.1. Refer to the Paragraph 3.2 of this Policy

3.4. Identification and validation for Revocation Request

3.4.1. The following may application for the end entity subscriber certificate revocation:

3.4.1.1. the Subscriber;

3.4.1.2. the TSP.

3.4.2. Application for revocation requests can be submitted via e-mail (signed with qualified electronic signature) or visiting the corresponding Registration authority.

3.4.3. The Registration authority will identify the applicant and his rights to submit an application. After successful identification, the Registration authority will register application.

3.4.4. The TSP will revoke certificate after revocation application is registered by the Registration authority.

3.4.5. Time between certificate revocation application registration and the decision to change its status information being available to all relying parties shall not exceed 24 hours.

4. Certificate Life-Cycle operational requirements

4.1. Certificate Application

4.1.1. Only signed application shall be accepted.

4.1.2. Identity validation refers to the Paragraph 3.2 of this Policy

4.1.3. Application process for receiving the “eParaksts” service:

4.1.3.1. Applicant shall complete the application on the TSP website www.eparaksts.lv or in physical presence in the registration authority.

4.1.3.2. During creation of application the TSP shall perform the following checks:

4.1.3.2.1. Verification of personal data (Subscriber's name, surname, personal identity number) against an authoritative source in case of physical presence, or against qualified signature attributes in cases where an application is signed electronically;

4.1.3.2.2. In case of physical presence, data of the presented personal identification document (type and series number of the document, period of validity, issuing country) shall be verified against an authoritative source, for example, the non-valid document register (document validity) or state resident register;

4.1.3.2.3. Verification of the communication channel, primarily by verification whether the mobile phone number specified in the application is in sole control of the applicant. The verification is carried out by sending a one-time code to the number specified in the application and by verification of the received code at the time of creating application.

4.1.3.3. The TSP may perform additional verifications and monitoring of changes in submitted data against authoritative registries.

4.1.3.4. Applicant shall choose application signing type – either physical presence in RA or by DPD courier or electronically with a qualified electronic signature.

4.1.3.5. The Subscriber must submit a signed application.

4.2. Certificate application processing

4.2.1. All applications and applicants shall be verified by Registration authority.

4.2.2. All applications shall be processed by registration operator and approved by registration officer.

4.2.3. The TSP shall refuse to issue a Certificate if the Certificate request does not comply with the technical requirements set in the applicable agreements.

4.2.4. If the TSP refuses to issue a Certificate, an entity that requested certification shall be notified.

4.2.5. All applications will be processed by the TSP in accordance with the applicable laws and agreements.

4.3. Certificate issuance

4.3.1. The TSP SHALL take measures against forgery of certificates, and in cases where the TSP generates the subject's key pair, guarantee confidentiality during the process of generating such data.

4.3.2. The procedure of issuing the certificate SHALL be securely linked to the associated registration, certificate renewal or rekey, including the provision of any subject-generated public key.

4.3.3. All certificates are issued according to [Certificate profiles].

4.3.4. "eParaksts mobile" authentication certificate issuing process:

4.3.4.1. The Subscriber shall download and install "eParaksts mobile" key management application in their mobile device;

4.3.4.2. Following the application validation and approval, the Subscriber receives a generated QR code containing a unique registration code and user name, as well as separately unique registration code and user name for

the cases when it is not possible for the user with a mobile device to scan QR code:

4.3.4.2.1. In the case of physical presence – personnel of the Registration Authority will show to the Subscriber the generated QR code and a unique registration code with the Subscriber's user name.

4.3.4.2.2. At the TSP website – the generated QR code and unique registration code with the Subscriber's user name will be shown to the Subscriber.

4.3.4.3. The Subscriber opens the "eParaksts mobile" mobile device key management application creates their own PIN code,

4.3.4.4. After entry of the PIN code, scanning of their generated QR code or enters the received unique registration code and their user name,

4.3.4.5. After entry of the QR code or the unique registration code, and user name a single use registration code is sent to the phone number (communication channel) specified in the application and verified,

4.3.4.6. The received single use registration code must be entered in the "eParaksts mobile" mobile device key management application,

4.3.4.7. After verification of the single use code (upon successful result), a key pair is generated and an appropriate certificate issued.

4.3.4.8. The Subscriber must activate "eParaksts mobile" mobile device key management application (finish onboarding process) within five (5) minutes after receipt of the unique registration code.

4.3.5. eParakstsTX qualified electronic signature certificate issuing process:

4.3.5.1. The Subscriber after receipt of "eParaksts mobile" authentication certificate authenticate the TSP website by using "eParaksts mobile" authentication or any smart cards (QSCD) issued by the TSP;

4.3.5.2. The Subscriber selects to generate eParakstsTX certificate;

4.3.5.3. After making the choice, the Subscriber creates a new PIN code for eParakstsTX keys, thereafter eParakstsTX keys are generated and a new certificate issued.

4.4. Certificate acceptance

4.4.1. Before entering into a contractual relationship with the Subscriber, the TSP shall inform the Subscriber of the general terms and conditions.

4.4.2. The TSP shall publish general terms and conditions on the TSP web page www.eparaksts.lv

4.4.3. The TSP shall record the Subscriber's signed agreement.

4.5. Key Pair and Certificate Usage

4.5.1. Main certificate usage is described in the Paragraph 1.4. of this Policy.

4.5.2. The Subscriber shall follow the Subscriber obligations provided in agreement, general terms and conditions, this Policy and [CPS].

4.5.3. All subject keys should be generated using a key length and algorithm as specified in [ETSI TS 119 312].

4.5.4. The Subscriber shall 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:

4.5.4.1. the subject's private key has been lost, stolen, potentially compromised;

4.5.4.2. control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons;

4.5.4.3. or inaccuracy or changes to the certificate content, as notified to the Subscriber or to the subject.

4.6. Certificate Renewal

4.6.1. Certificate renewal is not allowed.

4.7. Certificate Re-Key

4.7.1. Certificate re-key process is done in according to the Paragraphs 3.2., 4.1., 4.2., 4.3. and 4.4. of the [CPS].

4.7.2. In the case of certificates Re-Key old certificates are revoked.

4.7.3. Only the Subscriber can request certificates for "eParaksts mobile" mobile device key container and eParakstsTX re-key. It can be requested only when the Subscriber is authenticated on the TSP webpage using high level authentication means.

4.7.4. “eParaksts” service related certificate re-key process is identical as mentioned in the paragraphs 4.3.4. and 4.3.5. of this Policy.

4.8. Certificate Modification

4.8.1. Certificate modification can be done only after the Subscriber’s identification accordingly to the Paragraph 3.2. of the [CPS].

4.8.2. If any certified names or attributes have changed or contains an errors, incorrect certificate shall be revoked, the registration information shall be verified, recorded, agreed to by the Subscriber in accordance with this Policy.

4.9. Certificate Revocation and Suspension

4.9.1. The TSP shall revoke certificates in a timely manner based on authorized and validated certificate revocation requests.

4.9.2. The TSP shall revoke certificates if any of the following events occur:

4.9.2.1. Receives and validates revocation application;

4.9.2.2. The subject's or the TSP CA private key has been compromised or if the subject or a third party has misused the data.

4.9.2.3. When a legal or administrative order has been issued to this effect.

4.9.2.4. Change in the data supplied in order to obtain the certificate or modification in the circumstances verified for certificate issuance

4.9.2.5. One of the parties does not fulfil their obligations.

4.9.2.6. An error is detected in the certificate issuance procedure, either because one of the prerequisites has not been satisfied or due to technical problems during the certificate issuance process

4.9.2.7. Technical failure in the issuance and/or distribution of certificates or associated documentation.

4.9.2.8. Three months have elapsed from the time the certification is requested to time it is collected.

4.9.3. Requestors of revocation and available channels for processing revocation applications refer to the Paragraph 3.4. of this Policy.

4.9.4. Notification SHALL be sent to the Subscriber about certificate revocation when the TSP revokes a certificate.

4.9.5. Any relaying party can check certificate status via published CRLs or OCSP service provided by TSP.

4.10. Certificate Status Services

4.10.1. The TSP provides revocation status information via published CRLs or OCSP service with availability defined in the Paragraph 2.1. of the [CPS].

4.10.2. The revocation status information is publicly and internationally available.

4.11. End of Subscription

4.11.1. When it expires or when it has been revoked, the certificate is not valid for use.

4.12. Key Escrow and Recovery

4.12.1. Key escrow is not allowed.

5. Facility, management, and operational controls

5.1. Physical Controls

5.1.1. Described in the Paragraph 5.1. of the [CPS]

5.2. Procedural Controls

5.2.1. Described in the Paragraph 5.2. of the [CPS]

5.3. Personnel Controls

5.3.1. Described in the Paragraph 5.3. of the [CPS]

5.4. Audit Logging Procedures

5.4.1. Described in the Paragraph 5.4. of the [CPS]

5.5. Records Archival

5.5.1. Described in the Paragraph 5.5. of the [CPS]

5.6. Key Changeover

5.6.1. Described in the Paragraph 5.6. of the [CPS]

5.7. Compromise and Disaster Recovery

5.7.1. Described in the Paragraph 5.7. of the [CPS]

5.8. CA Termination

5.8.1. Described in the Paragraph 5.8. of the [CPS]

6. Technical security controls

6.1. Key Pair Generation

6.1.1. The subject keys must be generated pursuant to a minimum algorithm and key length recommendations defined in [ETSI TS 119 312].

6.1.2. When the Subscriber generates keys for “eParaksts mobile” authentication certificate, they should be generated in the mobile device key container in possession of the Subscriber.

6.1.3. Qualified electronic signature certificates are issued only in accordance with the QCP-n policy.

6.1.4. eParakstsTX certificate keys are generated by LVRTC, the keys are generated in the environment ensured by the Trust service provider and signatory is the only one who has sole control over their signature creation environment and its associated certificate.

6.1.5. eParakstsTX keys are stored in HSM device which is configured in accordance with the guidelines for a secure signature creation device.

6.1.6. Allowed key usage flags SHALL be set as described in the [Certificate Profile]

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. The Subscribers is responsible for their private key security and management.

6.2.2. Activation of private key is done by PIN. The Subscriber’s in “eParaksts mobile” mobile device key management application can choose to enable the comparison of fingerprints instead of PIN input.

6.2.3. The Subscriber’s are responsible that their PIN code and mobile device are only under their control. It is prohibited to transfer the PIN codes and/or the use of mobile device to a third party.

6.2.4. The Subscriber shall be held responsible for keeping their PIN code and mobile device only under their control. It shall be prohibited to transfer the PIN codes and/or the use of mobile device to a third party.

6.2.5. The Subscriber has the responsibility to immediately revoke their certificates, if the Subscriber PIN codes and / or mobile device is lost or there is

reasonable suspicion that the certificates are to be used without the Subscriber's knowledge and consent.

6.2.6. PIN requirements:

6.2.6.1. for authentication key – at least 4 digits;

6.2.6.2. for signature key – 6 digits;

6.3. Other Aspects of Key Pair Management

6.3.1. The validity period of the Subscriber certificates is up to three (3) years.

6.4. Activation Data

6.4.1. Subscribers should protect their private key activation data.

6.5. Computer Security Controls

6.5.1. The TSP computer security controls are described in the Paragraph 6.5. of the [CPS].

6.5.2. The Subscribers is responsible for applying reasonable protections on their devices and equipment.

6.6. Life Cycle Technical Controls

6.6.1. The TSP life cycle technical controls are described in the Paragraph 6.6. of the [CPS]

6.6.2. No Conditions for the subscribers

6.7. Network Security Controls

6.7.1. The TSP network security controls are described in the Paragraph 6.7. of the [CPS].

6.7.2. No provisions for the subscribers.

6.8. Time-Stamping

6.8.1. Not in the scope of the present document

7. Certificate, CRL, and OCSP profiles

7.1. Certificate Profile

7.1.1. Certificate SHALL be compliant with the profile defined in the [Certificate Profile].

7.2. CRL Profile

7.2.1. CRL SHALL be compliant with the profile defined in the [Certificate Profile].

7.3. OCSP Profile

7.3.1. The OCSP responses SHALL be compliant with the profile defined in the [Certificate Profile].

8. Compliance audit and other assessment

8.1.1. Described in the Paragraph 8. of the [CPS]

9. Other business and legal matters

9.1. Fees

9.1.1. Described in the Paragraph 9.1. of the [CPS]

9.2. Financial Responsibility

9.2.1. Described in the Paragraph 9.2. of the [CPS]

9.3. Confidentiality of Business Information

9.3.1. Described in the Paragraph 9.3. of the [CPS]

9.4. Privacy of Personal Information

9.4.1. Described in the Paragraph 9.4. of the [CPS]

9.5. Intellectual Property Rights

9.5.1. Described in the Paragraph 9.5. of the [CPS]

9.6. Representations and Warranties

9.6.1. Described in the Paragraph 9.6. of the [CPS]

9.7. Disclaimers of Warranties

9.7.1. Described in the Paragraph 9.7. of the [CPS]

9.8. Limitations of Liability

9.8.1. Described in the Paragraph 9.8. of the [CPS]

9.9. Indemnities

9.9.1. Described in the Paragraph 9.9. of the [CPS]

9.10. Term and Termination

9.10.1. This Policy SHALL remain in force until it is replaced by the new version or when it is terminated due to CA termination or when the service is terminated and all the Certificates therefore become invalid.

9.10.2. In the event of Termination, the TSP ensures customer and stakeholder awareness.

9.11. Individual Notices and Communications with Participants

9.11.1. Described in the Paragraph 9.11. of the [CPS].

9.12. Amendments

9.12.1. Described in the Paragraph 1.5.3. of this Policy.

9.12.2. OID SHALL change when the scope of this Policy will change or when a new type of Certificate will occur.

9.13. Dispute Resolution Provisions

9.13.1. Described in the Paragraph 9.13. of the [CPS].

9.14. Governing Law

9.14.1. Described in the Paragraph 9.14. of the [CPS].

9.15. Compliance with Applicable Law

9.15.1. Described in the Paragraph 9.15. of the [CPS].

9.16. Miscellaneous Provisions

9.16.1. No provisions.

9.17. Other Provisions

9.17.1. No other provisions.