“eParaksts karte+” Trust service policy

[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	01.07.2017.	Changes detailing products and requirements

Contents

1. Introduction

1.1. Overview

1.1.1. This document “”eParaksts karte+” 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 electronic signature certificates and related certificates for authentication for “eParaksts karte+” trust service.

1.1.2. These certificates promotes use of electronic signatures and electronic identification of natural persons. Certificates are always issued in pairs - each "eParaksts karte+" containing one authentication certificate and a qualified electronic signature certificate and their corresponding private keys. Each private key is protected by a separate activation data (PIN) and each "eParaksts karte+" has one personal unlocking code (PUK code).

1.1.3. LVRTC as TSP issuing certificates for "eParaksts karte+" service is guided by [eIDAS regulation] and related standards.

1.1.4. This Policy is based on “QCP-n-qscd” 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 to 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 language. This Policy May be translated and available in other languages. In case of Policy translation inconsistences, Policy version in Latvian language prevails.

1.1.7. The “eParaksts karte+” 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 karte+” Trust service policy”.

1.2.2. This Policy is identified by OID: 1.3.6.1.4.1.32061.2.1.5.1

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 karte+)	5
Version	1

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

1.2.4.1. 0.4.0.194112.1.2 (QCP-n-qscd)

1.2.4.2. 1.3.6.1.4.1.32061.2.1.5.1 (this Policy)

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

1.2.5.1. 0.4.0.2042.1.2 (NCP+)

1.2.5.2. 1.3.6.1.4.1.32061.2.1.5.1 (this Policy)

1.3. PKI Participants

1.3.1. Certification Authorities

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

1.3.2. Registration Authorities

1.3.2.1. Within this Policy, registration authorities are:

1.3.2.1.1. LVRTC Registration authority for managing for managing “eParaksts karte+” service and related certificates for LVRTC personnel;

1.3.2.1.2. Riga City Council acting behalf of LVRTC Registration authority and managing “eParaksts karte+” service and related certificates for Riga City Council personnel.

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

1.3.3.2. Subscribers can only be a natural person who are employees of State joint stock company “Latvia state radio and television centre” or Riga city council.

1.3.4. Relying Parties

1.3.4.1. Relaying parties are legal or natural persons who are making decisions based on “eParaksts karte+” related electronic signature or authentication certificate.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses:

1.4.1.1. “eParaksts karte+” related qualified electronic signature certificates are used for creation of Qualified 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 and compliant to [eIDAS regulation].

1.4.1.2. “eParaksts karte+” related authentication certificates are used for authentication of 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. Subscriber private key transfer to third parties.

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

1.5. Policy administration

1.5.1. Organization Administering the Document

1.5.1.1. This Policy is administrated by State Joint stock company "Latvian State Radio and Television Centre" which act as Trust service provider under those 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 enlarged.

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

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

1.6. Definitions and Acronyms

1.6.1. Definitions

Policy	Within this document – “”eParaksts karte+” Trust service policy”
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
secure cryptographic device	device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user
subject	entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

1.6.2. Acronyms

CA	Certificate authority
CRL	Certificate revocation list
NCP +	Extended 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-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD
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 Paragraph 2.1. of the [CPS]

2.2. Publication of Certification Information

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

2.3. Time or Frequency of Publication

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

2.4. Access Controls on Repositories

2.4.1. As described in 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 the 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. TSP do not offer such services.

3.1.4. Uniqueness of Names

3.1.4.1. 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. Keys are generated by Registration Authority and the keys are stored on a QSCD, proof of possession of the private key is by virtue of the trusted procedure of delivery and acceptance of the QSCD and of the corresponding certificate and key pair stored within.

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. Identity proofing and verification of natural person is based on Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015, on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of 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.

3.2.3.2. Authentication of Individual Identity applying to “eParaksts karte+” service is done by TSP.

3.3. Identification and validation for Re-Key Requests

3.3.1. Refer to Paragraph 3.2 of this Policy

3.4. Identification and validation for Revocation Request

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

3.4.1.1. Subscriber;

3.4.1.2. TSP.

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

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

3.4.4. TSP will revoke certificate after revocation application is registered by 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.

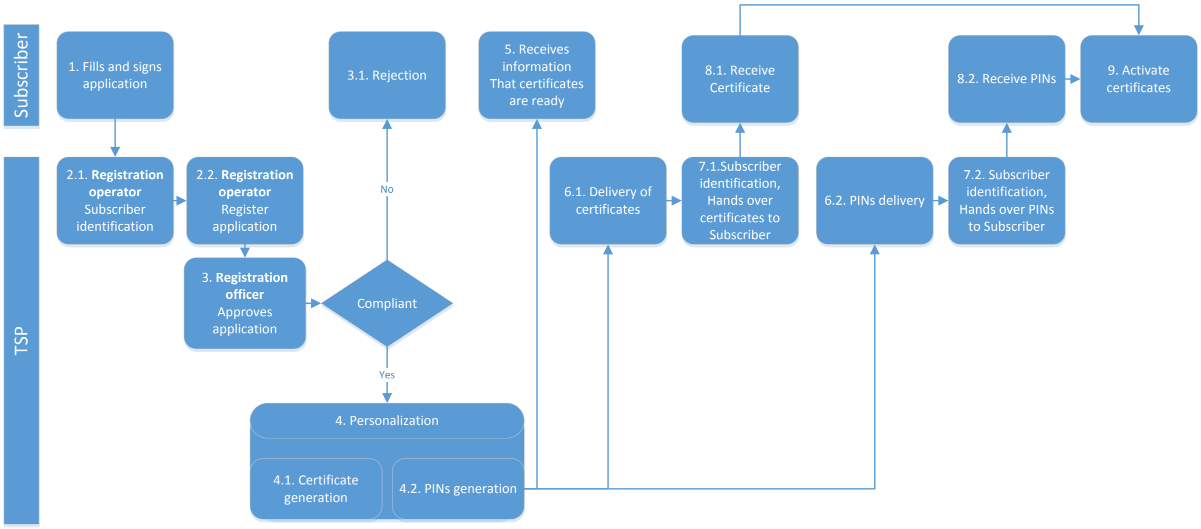
4. Certificate Life-Cycle operational requirements

4.1. Certificate Application

4.1.1. Only signed application SHALL be accepted.

4.1.2. Identity validation refer to Paragraph 3.2 of this Policy

4.1.3. Enrollment process:


Subscriber
TSP
1. Fills and signs application
2.1. Registration operator Subscriber identification
2.2. Registration operator Register application
3. Registration officer Approves application
Compliant
No
Yes
3.1. Rejection
4. Personalization
4.1. Certificate generation
4.2. PINs generation
5. Receives information That certificates are ready
6.1. Delivery of certificates
7.1.Subscriber identification, Hands over certificates to Subscriber
8.1. Receive Certificate
6.2. PINs delivery
7.2. Subscriber identification, Hands over PINs to Subscriber
8.2. Receive PINs
9. Activate certificates

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. 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 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. In case, where TSP generates subject’s keys in QSCD, QSCD containing subject’s private key SHALL be securely delivered to the registered subject.

4.4. Certificate acceptance

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

4.4.2. TSP SHALL publish general terms and conditions in TSP web page www.eparaksts.lv

4.4.3. The TSP SHALL record the signed agreement with the subscriber.

4.5. Key Pair and Certificate Usage

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

4.5.2. Subscriber SHALL follow 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. 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. The TSP SHALL check the existence and validity of the certificate to be renewed and that the information used to verify the identity and attributes of the subject are still valid.

4.6.2. If any of the TSP terms and conditions has changed, these shall be communicated to the subscriber and agreed by singing new agreement.

4.6.3. The TSP SHALL issue a new certificate using the subject'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 subject's private key has been compromised nor that the certificate has been revoked due to any other security breach.

4.7. Certificate Re-Key

4.7.1. Certificate re-key process are done in accordingly to 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.

4.8. Certificate Modification

4.8.1. Certificate modification can be done only after subscriber’s identification accordingly to 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. TSP SHALL revoke certificates in a timely manner based on authorized and validated certificate revocation requests.

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

4.9.2.1. Received and validated revocation application;

4.9.2.2. The subject's or 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 breaches its 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 Paragraph 3.4. of this Policy.

4.9.4. Notification SHALL be send to subscriber about certificate revocation when 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. TSP provides revocation status information via published CRLs or OCSP service with availability defined in Paragraph 2.1. of the [CPS].

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

4.11. End of Subscription

4.11.1. When it expires or when 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 Paragraph 5.1. of the [CPS]

5.2. Procedural Controls

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

5.3. Personnel Controls

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

5.4. Audit Logging Procedures

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

5.5. Records Archival

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

5.6. Key Changeover

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

5.7. Compromise and Disaster Recovery

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

5.8. CA Termination

5.8.1. Described in 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 minimum algorithm and key length recommendations defined in [ETSI TS 119 312].

6.1.2. Keys for qualified electronic signature certificates issued under QCP-n-qscd SHALL be generated only in QSCD.

6.1.3. Keys are generated by the TSP, the keys SHALL be handed over to the Subscriber in person or using a courier in sealed envelope.

6.1.4. 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. Keys for qualified electronic signature certificates on QSCD for “eParaksts karte+” service issued under policy QCP-n-qscd SHALL be generated on a device certified in accordance with [eIDAS regulation] and [ETSI EN 419 211].

6.2.2. Subscribers is responsible for his/her private key security and management.

6.2.3. The subscriber is responsible for he’s PIN code and smart card retention only under his control. It is prohibited to transfer smart card and / or PIN codes to a third party.

6.2.4. Subscriber has the responsibility to immediately revoke their certificates, if the Subscriber PIN codes and / or smart card is lost or there is reasonable suspicion that the certificates are to be used without the Subscriber's knowledge and consent.

6.2.5. PIN requirements:

6.2.5.1. for authentication key – at least 4 digits;

6.2.5.2. for signature key – 6 digits;

6.2.6. PUK should contain at least – 6 digits.

6.3. Other Aspects of Key Pair Management

6.3.1. The validity period of Subscriber certificates is up to five (5) years.

6.4. Activation Data

6.4.1.1. Subscriber keys is generated by the TSP, activation codes (PIN and PUK codes) SHALL be handed over in person to the Subscriber.

6.4.2. Subscribers should protect their private key activation data (PIN and PUK codes).

6.5. Computer Security Controls

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

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

6.6. Life Cycle Technical Controls

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

6.6.2. No Conditions for subscribers

6.7. Network Security Controls

6.7.1. TSP life cycle technical controls are described in Paragraph 6.7. of the [CPS].

6.7.2. No provisions for 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 Paragraph 8. of the [CPS]

9. Other business and legal matters

9.1. Fees

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

9.2. Financial Responsibility

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

9.3. Confidentiality of Business Information

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

9.4. Privacy of Personal Information

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

9.5. Intellectual Property Rights

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

9.6. Representations and Warranties

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

9.7. Disclaimers of Warranties

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

9.8. Limitations of Liability

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

9.9. Indemnities

9.9.1. Described in 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, TSP ensures customer and stakeholder awareness.

9.11. Individual Notices and Communications with Participants

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

9.12. Amendments

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

9.14. Governing Law

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

9.15. Compliance with Applicable Law

9.15.1. Described in 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.