# General terms and conditions of the Trust Services

[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 (hereinafter referred to as the eIDAS Regulation)
2. [CPS] Terms for provision of the Trust Services by the State Joint Stock Company "Latvia State Radio and Television Centre"
3. “eID karte” Trust service policy
4. “eParaksts” Trust service policy
5. “eParaksts karte” Trust service policy
6. “eParaksts karte+” Trust service policy
7. “eZīmogs” and “eZīmogs+” Trust service policy
8. Trust service provider time stamping policy
9. [Certificate profiles] Description of TSP issued certificate profiles

HISTORY OF CHANGES:

| Revised version No. | Enactment date | Summary of changes |
|---|---|---|
| 01.0 | 01.07.2017 | Initial version |
| 01.1 | 01.07.2017 | Detailed paragraph 3.1. 3. with relevant Trust Services and Policies<br>Added paragraph 11.8, linking this document with certificate profiles. |
| 02.0 | 01.08.2017 | Added paragraph 3.2 and reference to “eParaksts” Trust service policy |
| 03.0 | 01.02.2018 | The document is linked to the Electronic identification law of the natural persons and related Cabinet of Ministers regulations. Improved service definitions and descriptions. Throughout the document, changes are made to the new service definitions and descriptions.<br><br>Added paragraphs 3.3., 5.3., 6.1.5., 6.1.6., 10.2., 11.5.7., 11.5.8., 11.5.9., 11.9., 12.2.<br><br>Processed paragraph 9. |

| | | |
|---|---|---|
| 04.0 | 19.07.2018 | In whole document made changes according to new definition and desciptions of services.<br><br>Added paragraphs 4.7,11.10., 11.11 and chapter 11. |
| 05.0 | 17.12.2018 | Added used hardware in paragraph 12.10.2 and information about legal terms of its usage. Added additional information regarding agreement templates un paragraph 11.5. |
| 06.0 | 01.09.2019 | New “eID karte” trust service OID added in paragraph 3.1.<br>Added paragraphs 12.9.2 and 13.3 – 13.9.<br>Editorial changes have been made throughout the document. |
| 07.0 | 01.09.2019 | Added paragraph 3.4., describing new functionality of new eID cards (NFC and encryption). |
| 08.0 | 30.06.2020 | Changes regarding qualified electronic signature product details. Increased OID and trust service policy number in paragraph 3.1. Added Certificate revecotion and re-key information in paragraph 12.4. Added 6.1.7 paragrah about persons any direct or indirect discrimination. |

# TABLE OF CONTENTS

## 1. Objective and Audience

*1.1.* The general terms and conditions of the Trust and electronic identification Services are developed and approved in order to ensure uniform requirements for the beneficiaries of services and servicing provided by the trust and electronis identification services provider, in accordance with the regulatory enactments effective in the Republic of Latvia.

*1.2.* The general terms and conditions of the Trust and electronic identification Services are designed for the purpose to inform potential customers of the Trust and electronic identification service provider regarding general terms and conditions of use of the Trust and electronic identification services.

*1.3.* The general terms and conditions of the Trust and electronic identification Services shall be binding upon the Service provider and all the beneficiaries of the Trust, electronic identification and other services and servicing provided by the Trust and electronic identification services provider and the relying parties associated with the Trust and electronic identification services.

*1.4.* This document is prepared in Latvian language. This document may be translated and may be available in other languages. In case of document translation inconsistences, document version in Latvian language prevails.

## 2. Terms and Acronyms

| **Acronym, term** | **Explanation** |
|---|---|
| Subscriber | A natural or legal person who has concluded an agreement with TSP on one or more trust service or other TSP provided service or to which UPS services are provided on the basis of regulatory enactments, without concluding an agreement with the Subscriber. Includes Signatories, Creators of seals, Time stamp requestors, users of authentication certificate. |
| Relying party | A natural or legal person, who relies on the electronic identification or trust service. |
| CRL | Certificate Revocation List. |
| Laws and regulations effective in the Republic of Latvia | Include all laws and regulations effective in the Republic of Latvia. Reference to the laws and regulations effective in the Republic of Latvia shall include also international agreements binding to the Republic of Latvia and legal acts of the European Union. If the relevant law issue is governed by the legal acts of the European |

| | |
|---|---|
| | Union, which are directly applicable in Latvia, the Latvian law shall be applied to the extent the legal acts of the European Union permit for that. |
| LVRTC or service provider | State Joint Stock Company "Latvia State Radio and Television Centre" registration Nr. 40003011203, Address - Ērgļu iela 7, Rīga, Latvija, LV- 1012. |
| *NFC* | Near field communication technology allowing data exchange between the card and the equipement at a frequency of 13.56 MHz using eg. ISO/IEC 14443 protocol. |
| Service | Trust service defined in paragraph 3.1. of this terms and conditions. |
| Certificate | Qualified and/or unqualified certificate issued by Service provider. |
| Customer | A person who performs a payment for the person or the group of persons, which uses a secure electronic signature and/or other trust services in accordance with the terms for provision of trust services approved by the LVRTC. |
| Software | Electronic document management software created and distributed by LVRTC that provides for signing of electronic document and verification of the signed electronic documents. |
| OID | Object Identifier. |
| Parties | LVRTC TSP and Subscriber within the context of the present Terms. |
| PIN | Personal Identification number - a combination of numbers and / or letters that allows you to use the certificate only to a person with a known PIN. |
| Pricelist | Service provider’s approved Service pricelist. |
| QSCD | Qualified electronic signature/seal creation device. |
| Certificate | Qualified and/or unqualified certificate issued by TSP. |
| Services | Services associated with provision and receipt of the Trust Service. |
| Service provider | LVRTC, acting as Trust and electronic identification service provider. |

| | |
|---|---|
| Service provider's website | www.eparaksts.lv |
| Agreement | An agreement between LVRTC and the Subscriber regarding receipt of particular Trust Services. |
| Terms | The present general terms and conditions of the Trust Services. |
| Certificate revocation | Revoke certificates before the end ot their validity in case certificate is no longer applicable or required for specific use. |
| Certificate re-key | Issueing new certificates within existing services to ensure continuation of the contract. |

## 3. Relevant Trust Services and Policies

3.1. These Terms are associated with such Trust Services policies as follows:

| Service name | Policy | QSCD | Policy OID |
|---|---|---|---|
| eID karte | "eID karte" Trust service policy | Yes | 1.3.6.1.4.1.32061.2.1.2.1<br>1.3.6.1.4.1.32061.2.1.2.2 |
| eParaksts | "eParaksts" Trust service policy | Yes | 1.3.6.1.4.1.32061.2.1.3.2 |
| eParaksts karte | "eParaksts karte" Trust service policy | Yes | 1.3.6.1.4.1.32061.2.1.4.1 |
| eParaksts karte+ | "eParaksts karte+" Trust service policy | Yes | 1.3.6.1.4.1.32061.2.1.5.1 |
| eZīmogs | "eZīmogs" and "eZīmogs+" Trust service policy | No | 1.3.6.1.4.1.32061.2.2.1.1 |
| eZīmogs+ | "eZīmogs" un "eZīmogs+" Trust service policy | Yes | 1.3.6.1.4.1.32061.2.2.1.1 |
| Qualified time stamps | Trust service provider Time Stamping Policy | No | ETSI OID = 0.4.0.2023.1.1 |

3.2. Policy OIDs are described in related Policies mentioned in paragraph 3.1.

3.3. Each of the services referred to in Paragraph 3.1 consists of the:

3.3.1. qualified electronic signature certificate for the creation of a qualified or advanced electronic signature,

3.3.2. authentication certificate as a means of electronic identification for provisioning of electronic identification services.

3.4. “eID karte” service with OID – 1.3.6.1.4.1.32061.2.1.2.2 provides NFC for eID card and consists of the:

3.4.1. qualified electronic signature certificate for the creation of a qualified or advanced electronic signature,

3.4.2. authentication certificate with additional encryption functionality as a means of electronic identification for provisioning of electronic identification services and for data encryption.

## 4. General

4.1. Service provider ensures for the Subscriber the provision of Services and Servicing and the Subscriber undertakes to use the Services and Servicing received in accordance with the present Terms, [CPS], the relevant Services policy, Privacy policy as well as other binding external regulatory enactments.

4.2. Service provider and the Subscriber shall enter into an agreement regarding the provision of Services (except “eID card” Service) and Servicing.

4.3. “eID karte” Service and Servicing for the Subscriber are provided on the basis of regulatory enactments, without entering into an agreement with the Subscriber.

4.4. Service provider shall ensure for the Subscriber the provision of the Services and Servicing after conclusion of the agreement or on the basis of regulatory enactments. Service provider shall ensure the provision of the Services and Servicing, if the Subscriber complies with the obligations prescribed by the present Terms, [CPS], the relevant Services policy, and the agreement concluded or the regulatory enactments, if the Services and Servicing for the Subscriber are provided on the basis of regulatory enactments.

4.5. The Subscriber commits to get acquainted and comply with the present Terms and amendments thereto, Privacy policy, [CPS], the received Service policy, as well as other information related to the receipt of the Services and Servicing published on the Service provider’s website.

4.6. In the event if any requirement of these Terms is different from the requirements specified in the agreement concluded with the Subscriber, the requirements referred

to in the Subscriber agreement, shall prevail. If the Services and Servicing are provided to the Subscriber on the basis of the regulatory enactments without entering into an agreement with the Subscriber, the Subscriber shall be bound by the present Terms.

4.7. If the Services are provided to the Subscriber upon conclusion of the Subscriber Agreement, then:

4.7.1. From the moment of signing the Agreement, the Subscriber and the Service provider are responsible for the correctness of the submitted data and the Service provider is responsible for their processing in accordance with the requirements of the Agreement and regulatory enactments;

4.7.2. After the Contract is registered in the Service provider's system, the Service provider is responsible for the production and delivery of the related Service certificates of signature/seal creation devices to the Subscriber;

4.7.3. If the Subscriber does not receive the related Service certificates or signature/seal creation devices within the term specified in the Contract due to his fault, then the Agreement shall automatically expire completely on the day following the contractual term upon which the Subscriber has to receive the related Service certificates or signature/seal creation device.

## 5. Service provider obligations

5.1. Service provider shall ensure:

5.1.1. Possibility for the Subscriber to ascertain regarding compliance of the information contained in the Certificate with data specified in the Subscriber's application (Service application form).

5.1.2. Service to be used online to add the time stamp.

5.1.3. Constantly maintenance of available and freely accessible online CRL lists in accordance with regulatory enactments effective in the Republic of Latvia.

5.1.4. Confidentiality of the the information submitted by the Subscriber, with exception of those included in the Certificate. Service provider shall be entitled to disclose the information received from the Subscriber in cases and under procedures specified in regulatory enactments effective in the Republic of Latvia to the competent governmental and municipal institutions, as well as in

other cases mentioned in the Privacy Policy, [CPS], and the related Services Policy.

5.1.5. Advice on using the Services and the Certificate through the channels provided by the assistance service available on the Service provider's website.

5.1.6. The provision of services in accordance with the requirements specified in regulatory enactments effective in the Republic of Latvia.

5.1.7. Publishing of [CPS], all the Trust Services Policies, these Terms, Privacy policy, Pricelist and Payment terms on the Service provider's website.

5.2. In cases, when Service provider generate Subscribers keys in the smart card (QSCD), Service provider immediately after the issuance of certificates shall automatically suspend the certificates issued to the Subscriber and activate them only after smart card (QSCD) issuance to subscriber.

5.3. The Service Provider informs that the Services and Servicing may be unilaterally suspended or terminated at any time for any reason or circumstances. In case of termination or termination of service, information about it is published on the Service provider's website no later than 30 days in advance.

## 6. Service provider’s rights

6.1. Service provider shall be entitled:

6.1.1. To suspend, to resume and to revoke the Certificates in cases and under procedures specified in regulatory enactments effective in the Republic of Latvia, [CPS] and related Services policies.

6.1.2. If the Customer submits a submission regarding revocation of the Certificates issued to the Subscriber (upon the Customer’s demand and paid), the Service provider shall revoke the Certificates and their renewal becomes impossible.

6.1.3. Service provider alone shall be entitled to suspend or to revoke, or to preclude the use of Subscriber’s certificates in the following cases:

6.1.3.1. if the Customer or the Subscriber does not pay for the paid Services used and does not ensure fulfilment of the payment obligations in full amount within (5) five working days or within the time period prescribed by the concluded agreement, counting from the date of receipt of the

Service provider’s notification, if the Customer or the Subscriber and Service provider have entered into an agreement for the provision of paid services;

6.1.3.2. if the Customer or the Subscriber fails to comply with the obligations prescribed by the concluded agreement or by the regulatory enactments or in these Terms and fails to eliminate the breach of the obligations within (5) five working days, counting from the date of receipt of the Service provider’s notification.

6.1.3.3. In other cases, which are stipulated in the [CPS] or in the related Service Policy.

6.1.4. Service provider at its own discretion, without explaining the reasons, may refuse to issue a certificate to the Subscriber, except in the cases specified in regulatory enactments, when the issue of the certificate is obligatory.

6.1.5. Amendments to the Terms unilaterally. Such amendments enter into force on the date specified by the Service Provider's Board or its representative, but not earlier than 30 days from the placement of the relevant notice on the Service provider’s website. If the Subscriber has not submitted to the Service Provider a written notice of termination of the Agreement or refusal from the use of the Services and the Servicing until the date of such amendments, it is considered that the Subscriber has agreed to amendments to the rules for the use of the Services and the Servicing and the same shall be applicable to legal relations between the parties.

6.1.6. The Service Provider may collect and use the technical data and related information, including, but not limited to, technical information about the Subscriber's device, system and software, and peripheral devices that are periodically collected in order to facilitate the software update, the Service support and other services related to the provision of the software to a user. The Service Provider may use this information as long as it is in a form that is not personally identified and is not linked to a particular Subscriber to improve its Services and Servicing.

6.1.7. The Service Provider exercises its rights and obligations in accordance with the laws and regulations and without any direct or indirect discrimination -

regardless of a person's race, colour, sex, age, disability, religious, political or other beliefs, national or social origin, property or family status, sexual orientation or other circumstances.

## 7. Obligations of the Subscriber

7.1. By signing the agreement or applying for “eID karte” service in accordance with regulatory enactments, the Subscriber declares that they have become cognizant with terms and conditions relating to the use of the Service received, including with these Terms, Privacy policy, [CPS] and the received Services policy, which is available on the Service’s provider website.

7.2. When signing the agreement or applying for “eID karte” service in accordance with regulatory enactments, the Subscriber confirms that they undertake to follow and comply with the current version (valid version) of the terms and conditions relating to use of the Service received, including with these Terms, Privacy policy, [CPS] and received Services policy, which is available on the Service provider’s website.

7.3. Undertakes to use the Services and the Servicing received in accordance with the requirements of the concluded agreement or regulatory enactments, the present Terms, [CPS] and the received Services policy, which they recognise to be binding and enforceable in full.

7.4. Undertakes full responsibility for the loss and/or damage caused to any third party through using the received Services and/or the Servicing for illegal activities or purposes.

7.5. For receipt of the Services and the Servicing to indicate for Service provider accurate, complete and genuine information.

7.6. The Subscriber on their own resources shall ensure technical possibilities such as to be able to use the Services and the Servicing in accordance with these Terms and the concluded agreement or the regulatory enactments.

7.7. For amendments to the terms for the use of the Services and the Servicing, the Subscriber shall be notified in accordance with paragraph 6.1.5. of these Terms.

7.8. The Subscriber understands and acknowledges that provision of the trust and electronic identification services is not possible without processing of the Subscriber’s personal data. In the light of the said, when applying for the trust services or by affixing

signature to the agreement, the Subscriber agrees that the Service provider caries out processing of the Subscriber's personal data in accordance with provisions of paragraph 9 of the [CPS] and Privacy policy.

## 8. Obligations of the Relying Party

8.1. The Relying Parties must check the Certificate status of the certificates, on which they must rely or they would like to rely.

8.2. The Relying Parties can make verification of the Certificates using the latest CRL lists published on the Service provider's website or by means of the Service provider's online certificate status verification service.

8.3. Verification of the digitally signed documents has to be carried out via the online electronic document verification Service provided on the Service provider's website or the Software provided by the Service provider.

## 9. Force Majeure

9.1. In the event of impossibility of obligations or duties imposed by any of the parties by force majeure circumstances such as, but not limited to, magnetic storms, floods, earthquakes, acts of public authorities and administrations, or other similar circumstances or events which the parties could not foresee and did not comply with the control of the parties , each party as far as possible strives to ensure fulfillment of its obligations, but if this is not possible, the parties shall be released from liability for non-compliance during force majeure circumstances.

9.2. A party whose obligations or obligations are obstructed by force majeure shall notify the other party immediately by written notice of such occurrence. The Service provider may make the notification by publishing the corresponding notice on the Service provider's website in accordance with Paragraph 11.9.1 of these Terms.

9.3. The burden of proving proof of force majeure lies with the party to which it refers, except when the fact of force majeure is well known.

## 10. Price and Settlement Procedure

10.1. Fee for use of the Services and the Servicing supplied and provided by Service provider to the Subscriber, shall be determined in accordance with the Service provider approved Pricelist, which is published on the Service provider's website. No

fees are charged for the Services and Servicing, which must be provided free of charge by the Service provider in accordance with the regulatory enactments. The Service provider may charge fees for additional Services and Servicing provided additionally to the Services provided under regulatory enactments, which are provided free of charge.

10.2. The payment order is published on the Service provider's website.

10.3. Notification shall be provided to the Subscriber regarding changes in Pricelist and Payment rules of the Services and the Servicing at 30 (thirty) days in advance, through publication by the Service provider of the relevant information on the Service provider's website. If the Subscriber, before the date of entry into force of such changes in Pricelist or Payment rules of the Services and the Servicing, has not submitted a written notification to the Service provider regarding termination of the agreement or refusal from the use of the Services and the Servicing, it shall be considered that the Subscriber has agreed to changes in Pricelist and/or Payment rules of the Services and the Servicing and these shall be applicable to legal relations between the Parties.

## 11. Electronic identification rules

11.1. "eID card", "eParaksts", "eParaksts card" and "eParaksts card +" trust services include electronic identification mean of a natural person.

11.2. The Service Provider provides electronic identification of natural persons using the Service Provider's electronic identification platform.

11.3. The electronic identification platform for natural persons is available only from the websites of electronic service providers where electronic platform providers have integrated the platform.

11.4. The electronic identification platform provides electronic identification of natural persons and the transfer of authenticated physical person data to the electronic service provider who requested the electronic identification of the natural person.

11.5. Samples of trust and electronic identification service application contracts are available on the Service Provider's website https://www.eparaksts.lv/en/about_us/repository/contract_templates.

11.6. The use of all electronic identification means is protected by a PIN.

11.7. Access to the private key is protected by a PIN code and stored in a secure medium (smart card chip or software container / mobile phone security chip on mobile phone).

11.8. The set of data protection for physical persons provided by the service provider is described in the CPS and these controls are audited annually.

11.9. All communication between the Subscriber, the Service Provider and the electronic service provider requesting the Subscriber Identification is encrypted (SSL is used).

11.10. Possible risks:

11.10.1. Subscription must be aware and understand that when transferring a carrier containing its electronic identification means (smart card or mobile device) as well as the PIN code of its electronic identification means to third parties, these persons may request and receive electronic services on behalf of the Subscriber, as a result of which the Customer may incur civil liability or arise liability, disciplinary liability, administrative liability or criminal liability.

11.10.2. Only licensed and official software should be used on mobile devices.

11.10.3. The reinstallation of a mobile device operating system on an unlicensed or functionally restricted (rooted or jailbraked) versions poses serious security risks, including, but not limited to, the use of electronic services and the protection of data stored on a mobile device.

11.10.4. When using any digital technology, including software, there is a risk that new vulnerabilities may be discovered so far that may make the Services unsafe. Therefore, the Subscription must follow the software updates and always use the latest officially approved version.

11.10.5. If use smartcards, the risk is caused by the device that is connected to the card. The subscriber should always make sure that the computer to which the smart card is connected is clean from malicious software, has an antivirus program installed, and that the Subscription identifies in a trusted source.

## 12. Other Provisions

12.1. The Subscriber agrees that the Service provider shall be entitled to verify the accuracy of the Subscriber’s data, including obtaining the Subscriber’s personal data from the registries of national importance and to track the Subscriber’s personal data changes,

but it does not impose any obligation for the Service provider to make appropriate changes to the certificate.

12.2. The Subscriber shall give permission for inclusion of their personal data in the Certificate, in the case of which use the data shall become available (published) to third parties. The Subscriber shall give permission to the Service provider to the processing of personal data in accordance with the [CSP] and Privacy policy.

12.3. The Subscriber shall give permission for use of their personal data that are necessary for the purposes of the provision of the Services and the Servicing to the Subscriber. The Service provider shall use the Subscriber's data only for the purposes of provision of the Services and the Servicing in accordance with Privacy policy.

12.4. Certificate renewal and re-key procedure:

12.4.1. Certificate revocation are described in paragraph 4.9 of the Trust Service eParaksts policy.

12.4.2. Subscriber under an existing contract with the re-key of old certificate shall not be considered as grounds for termination of the contract.

**12.5. Time limits for storage of the log files**

12.5.1. Log files are archived and stored for at least 10 (ten) years without any data loss.

**12.6. Liability limits**

12.6.1. The Service provider's liability amount and limits are prescribed by paragraph 9. of [CPS]. The Service provider's liability is limited and on each case shall not exceed the amount referred to in paragraph 9. of [CPS].

12.6.2. The Service provider is not responsible for the loss and/or damage caused to the Subscriber if the Subscriber has incurred such loss amd/or damage by intent or due to negligence.

12.6.3. The Service provider is not responsible for the damage and/or losses caused to the Subscriber if the Subscriber violates the provisions of the agreement and/or the present Terms.

12.6.4. The Service provider shall be held responsible only for the loss which, intentionally or due to negligence, has caused to any natural or legal person because the Service provider has failed to comply with regulatory enactments effective in the Republic of Latvia in accordance with the provisions laid down

therein. The Service provider is not responsible for the loss, if it is proved that the loss has been incurred without any intention or negligence on behalf of the Service provider.

12.6.5. The Service provider shall not assume any responsibility for the content, amount and execution of the transaction for performance whereof a certificate issued by Service provider is used. The Subscriber or the Customer may limit the use of the certificate through suspension or revocation thereof.

12.6.6. In order to secure against financial responsibility, the Service provider has purchased and manages appropriate insurance policy.

12.6.7. The Service Provider does not assume any responsibility for the actions of the Subscriber, which are carried out through the use of trust or electronic identification services, and their consequences.

12.6.8. The Service provider does not assume any responsibility whatsoever for the use of the public information contained in the Subscriber Certificate by Third parties.

12.6.9. The Service Provider is not responsible for the accuracy and correctness of the data included in the document and its visual representation, which is made up of the Subscriber, as well as on the conclusions, assumptions and decisions made by third parties and / or transactions using the data included in the visual representation of the document.

12.6.10. The Service provider is not liable for damage and / or losses caused to the Subscriber, if the Service Provider unilaterally suspends or terminates the provision of any Service or Service for any reason or circumstances.

**12.7. Procedure for resolution of disagreements**

12.7.1. If a dispute occurs arising out of or related to the Service provider provision procedures or associated agreements or contracts before launching the proceedings, the parties involved in the dispute must endeavour to resolve the dispute or opinion differences through acting in good faith by means of negotiations between the Parties.

12.7.2. If the Parties involved in the dispute fail to resolve the dispute through negotiation within one (1) month from the emergence of a dispute, the Parties agree to apply to the courts. The disputes shall be adjudicated by the Riga

City Vidzeme Suburb Court (first instance) of the Republic of Latvia in Latvian pursuant to the regulatory enactments effective in the Republic of Latvia. The disputes are not examined by the court of arbitration.

**12.8. Frequency and conditions of the conformity audit**

12.8.1. The conformity assessment body is carrying out conformity assessments of the Service provider and it`s provided Services in compliance with the regulatory enactments effective in the Republic of Latvia.

12.8.2. Extraordinary conformity assessment in the Service provider is carried out in the cases where the Service provider makes substantial changes to the Service provider management or information systems or it is required by the supervisory body in accordance with the regulatory enactments effective in the Republic of Latvia.

12.9. Certificate profiles for Services defined in paragraph 3.1. of those Terms are described in annexes of [Certificate profiles].

**12.10. Notifications**

12.10.1. All notifications or other documents sent to a party must be delivered by post, electronic mail or to the addresses specified in the Agreement. If the notice or document is addressed or is being transferred to all Subscribers or to all Subscribers of a particular Service, the Service provider may publish relevant information on the Service provider’s website and it is deemed that by such publication the Service provider has notified in writing each Subscriber or each particular service Subscribers.

12.10.2. Notifications about the certificate status changes will be sent to the communication channel specified in the Subscriber's application and official electronic address, if the person has an activated official electronic address account.

12.11. Software and equipment used in the provision of services.

12.11.1. Service provider uses certified manufacturer Safelayer Secure Communications S.A. for providing reliability and electronic identification services. software produced:

12.11.1.1. KeyOne PKI Platform Certification for Lifecycle Certification;

12.11.1.2. TrustedX eIDAS platform electronic identities services;

12.11.1.3. MobileID eSignature Mobile provision service and application;

12.11.1.4. TrustedX Electronic signature service to create an electronic signature in the infrastructure of LVRTC.

12.11.1.5. Electronic identification service based on oAuth2.0 and OpenID protocols.

12.11.2. Service provider for reliability and electronic identification is using the following equipment to provide services:

12.11.2.1. Software involved in providing identification service is located on virtual machines witch uses the IBM System x3550 M4, IBM System x3650 M4 and Cisco UCSCC220-M4S.

12.11.2.2. Security devices nShield are used to encrypt data - Connect 1500+ and nShield 500e F3 PCI-Express.

12.11.3. All equipment is owned by LVRTC and all software is purchased and has all required licenses for legal use.

12.12. Service availability and system recovery.

12.12.1. The Service Provider ensure that unplanned interruptions in the provision of reliability and electronic identification services do not exceed as defined in [CPS] 2.1. (Including through accident prevention and system renewal).

## 13. Warranties

13.1. The Service provider guarantees that certificates issued to the Subscriber are generated under the State Joint Stock Company “Latvia State Radio and Television Centre” Service provider Root Certification authority.

13.2. Excerpts from the Service provider’s Certification authority certificates are publicly available on the Service provider's website www.eparaksts.lv

13.3. The Service provider does not warrant that its published apps, including mobile apps or Services will run on any device (smartphone, tablet, computer, etc.) with any operating system or version of it.

13.4. Apps, including mobile apps, or Services provided by Service provider, may contain third-party software and middleware that may be incompatible and may not work with older devices as well as newer devices with certain devices operating system or version of it.

13.5. To use an app issued by Service provider, including a mobile app, or a Service, a Subscriber or Relying party may need a compatible device with a particular operating system or version of it. The features of apps, including mobile apps, issued by Service provider, or Services may vary depending on the device, operating system, or versions of it.

13.6. For up-to-date information on supported devices, operating systems, and the minimum required technical performance of your device, please visit the Service provider's webpage.

13.7. If third-party software or middleware included in an app, including a mobile app, issued by the Service provider is not technically supported by a third party software manufacturer for a particular operating system or version, the Service Provider does not guarantee its operation on that particular operating system or version of it.

13.8. The service provider does not maintain or be responsible for third-party software and middleware included in the apps issued by the Service provider and does not guarantee their operation on all devices and all versions of the operating system. The Service provider shall not be responsible for the performance of third-party software and middleware included in the apps issued by the Service provider and the operation of assisted devices and operating systems or versions thereof.

13.9. By using an application provided by a Service Provider with third party software or middleware, the Subscriber shall take all risks and responsibility for its compatibility with the Subscriber Device operating system independently and independently.

## 14. Contact Information

*State Joint Stock Company "Latvia State Radio and Television Centre"*

| | |
|---|---|
| ***Address*** | Ērgļu iela 14, Rīga, LV-1012 |
| ***Trust and electronic identification service helpdesk*** | |
| ***Phone*** | +371 67108787 |
| ***e-mail*** | eparaksts@eparaksts.lv |
| ***Office*** | |
| ***Phone*** | +371 67198704 |

| | |
|---|---|
| ***e-mail*** | lvrtc@lvrtc.lv |