NOTIFICATION FORM FOR ELECTRONIC IDENTITY SCHEME UNDER ARTICLE 9 (5) OF REGULATION (EU) NO. 910/2014

Republic of Latvia hereby notifies the European Commission of an electronic identification scheme to be published in the list referred to in article 9 (3) of Regulation (EU) no. 910/2014, and confirms the following:

— the information communicated in this notification is consistent with the information which has been communicated to the Cooperation Network in accordance with article 7 (g) of Regulation (EU) no. 910/2014, and

— the electronic identification scheme can be used to access at least one service provided by a public sector body in **Republic of Latvia**.

Date 15.11.2018

[signed electronically]

1. GENERAL INFORMATION

Title of scheme	Level(s) of assurance (low, substantial, or high)
Latvian eID scheme: „eID karte“	high
Latvian eID scheme: „eParaksts karte“	high
Latvian eID scheme: „eParaksts karte+“	high
Latvian eID scheme: “eParaksts“	high

2. AUTHORITY/AUTHORITIES RESPONSIBLE FOR THE SCHEME

Name(s) of authority/authorities	Postal address(es)	Email address(es)	Telephone no.
Office of Citizenship and Migration Affairs (OCMA) of the Ministry of Interior of Republic of Latvia	Čiekurkalna 1. līnija 1, k-3, LV-1026, Rīga, Latvija	rigas.1.nodala@pmlp.gov.lv	+371 67209400
State join-stock company “Latvia State Radio and Television Centre” (LVRTC)	Ērgļu iela 14, Rīga, LV-1012, Latvija	eparaksts@eparaksts.lv	+371 67108787

3. INFORMATION ON RELEVANT PARTIES, ENTITIES, AND BODIES (WHERE THERE ARE MULTIPLE PARTIES, ENTITIES, OR BODIES, PLEASE LIST THEM ALL IN ACCORDANCE WITH ARTICLE 3 (2) AND (3))

3.1. Entity which manages the registration process of the unique person identification data

Name of entity which manages the registration process of the unique person identification data
Office of Citizenship and Migration Affairs – “eID karte”
State join-stock company “Latvia State Radio and Television Centre” – “eParaksts karte”, “eParaksts karte+”, “eParaksts”

3.2. Party issuing the electronic identification means

Name of the party issuing the electronic identity means and indication of whether the party is referred to in Article 7(a)(i), (ii) or (iii) of Regulation (EU) No 910/2014		
Office of Citizenship and Migration Affairs – “eID karte”		
Article 7(a)(i) ☐	**Article 7(a)(ii)** ☒	**Article 7(a)(iii)** ☐
State join-stock company “Latvia State Radio and Television Centre” – “eParaksts karte”, “eParaksts karte+”, “eParaksts”		
Article 7(a)(i) ☐	**Article 7(a)(ii)** ☐	**Article 7(a)(iii)** ☒

3.3. Party operating the authentication procedure

Name of party operating the authentication procedure
State join-stock company “Latvia State Radio and Television Centre”

3.4. Supervisory body

Name of the supervisory body
Supervisory Committee of Digital Security subordinate to the Minister of Defence

4. DESCRIPTION OF THE ELECTRONIC IDENTIFICATION SCHEME

(a) Briefly describe the scheme including the context within which it operates and its scope

There are four types of Electronic Identification Means (EIM) in Latvian eID scheme. One of them – “eID karte” is also physical identification document – Identity Card, as defined in Personal Identification Documents Law [1].

Latvian eID scheme is PKI-based solution.

In case of EIM “eID karte”, “eParaksts karte” and “eParaksts karte+” **authentication is provided in accordance with the NCP+ policy**, with authentication certificates where the private key resides in secure user's cryptographic device – smartcard. In case of EIM “eParaksts” authentication is provided in accordance with the NCP policy, with authentication certificates where the private key resides in secure key management application of user's mobile device. Identity data – the person’s first name, last name, and unique identifier (personal code) – is stored in the public key of certificate. These certificates are accessible on the smart card or in key management application of user's mobile device. Certificates of “eID karte” may also be stored in the public LDAP catalogue if user wishes it. Access to private keys for all EIMs is protected by 2 factors - PIN and possession of corresponding device (smartcard or mobile device).

Middleware of Latvian eID scheme is based on products TRUSTEDX EIDAS PLATFORM, KEYONE PKI PLATFORM and SAFELAYER MOBILE ID of Spanish corporation Safelayer Secure Communications S.A. (https://www.safelayer.com/en/).

Following parties are involved in the management of the Latvian eID scheme:

- **Registration and issuing authority** and provider of EIM personalisation - Office of Citizenship and Migration Affairs (for “eID karte”) and State join-stock company “Latvia State Radio and Television Centre” (for “eParaksts karte”, “eParaksts karte+”, “eParaksts”).
- **Certification Authority (CA**), a qualified trust service provider according to the eIDAS Regulation - State join-stock company “Latvia State Radio and Television Centre” with responsibility to maintain certificate lifecycle: creation, activation, suspension, and revocation.
- **Electronic Service providers** – e-government and private entities providing electronic services that are using eID scheme. Currently there are over 140 government e-services available, mainly through https://www.latvija.lv/en .

Issuance of the EIM is described in section 2.2.2. of the LoA mapping document. Technical descriptions of EIMs are provided in section 2.3.1. of the LoA mapping document.

Assurance requirements are based on the European legislation (i.e., the eIDAS Regulation, GDPR, etc.) and national legislation (i.e., the Latvian Law on Electronic Identification of Natural Persons [2], Personal Data Processing Law [3] and other national legal acts) for all parties involved. Additional normative requirements apply for the Qualified Electronic Identification Service Provider.

(b) Where applicable, list the additional attributes which may be provided for natural persons under the scheme if requested by a relying party

Not applicable.

(c) Where applicable, list the additional attributes which may be provided for legal persons under the scheme if requested by a relying party

Not applicable.

4.1. Applicable supervisory, liability, and management regime

4.1.1. Applicable supervisory regime

Describe the supervisory regime of the scheme with respect to the following:

(a) Supervisory regime applicable to the party issuing the electronic identification means

Supervisory regime is defined in Section 2 of eIDAS Regulation and in Law on Electronic Identification of Natural Persons. Pursuant to the Personal Identification Documents Law, the Ministry of the Interior[1] is responsible for overseeing the procedure for issuance of personal Identity Cards.

According to section 17 of the Law on Electronic Identification of Natural Persons, Supervisory Committee of Digital Security is acting as the supervisory authority of all operations of Electronic Identification Service Providers, including issuing of the EIM.

Rights and obligations of the Supervisory Committee of Digital Security are defined in Statutes[2] [14]. Supervisory control of the Supervisory Committee of Digital Security is performed by the Ministry of Defence of the Republic of Latvia.

(b) Supervisory regime applicable to the party operating the authentication procedure

Supervisory regime is defined in Section 2 of eIDAS Regulation and in Law on Electronic Identification of Natural Persons.

According to section 17 of the Law on Electronic Identification of Natural Persons, Supervisory Committee of Digital Security is acting as the supervisory authority of all operations of Electronic Identification Service Providers, including the authentication procedure.

4.1.2. Applicable liability regime

Describe briefly the applicable national liability regime for the following scenarios:

(a) Liability of the Member State under article 11 (1) of Regulation (EU) no. 910/2014

Latvian eID scheme is subject to European and national laws. There is full liability of the Latvian government.

(b) Liability of the party issuing the electronic identification means under article 11 (2) of Regulation (EU) no. 910/2014

According to Article 11(2) of Regulation (EU) no 910/2014 and Section 15 of Law on Electronic Identification of Natural Persons, party issuing the electronic identification means is liable for damage caused intentionally or negligently to third party due to a failure to comply with the obligations.

According to Section 12 of Law on Electronic Identification of Natural Persons, qualified identification service provider must have third party liability insurance. Issuer of EIMs “eParaksts karte”, “eParaksts karte+” and “eParaksts”, State join-stock company “Latvia State Radio and Television Centre” has liability insurance of 1 000 000 €.

(c) Liability of the party operating the authentication procedure under article 11 (3) of Regulation (EU) no. 910/2014

According to Article 11(3) of Regulation (EU) no 910/2014 and Section 15 of Law on Electronic Identification of Natural Persons any party operating the authentication procedure is liable for damage caused intentionally or negligently to third party due to a failure to comply with the obligations operating the authentication procedures.

Operator of authentication procedure State join-stock company “Latvia State Radio and Television Centre” has liability insurance of 1 000 000 €.

[1] In case of Identity Card of an employee of a foreign diplomatic or consular representation accredited in Latvia, Ministry of Foreign Affairs is responsible.
[2] Statutes of the Supervisory Committee of Digital Security (in Latvian only), https://likumi.lv/ta/id/286009-digitalas-drosibas-uzraudzibas-komitejas-nolikums

4.1.3. Applicable management arrangements

Describe the arrangements for suspending or revoking of either the entire identification scheme or authentication, or their compromised parts.

EIMs in Latvian eID scheme may be revoked or suspended. Arrangements for suspending or revoking the Latvian EIMs are described in sections 2.2.3., “Suspension, revocation, and reactivation”, and 2.4.1., “General provisions”, clause 5 of the LoA mapping document.

4.2. Description of the scheme components

Describe how the following elements of Commission Implementing Regulation (EU) 2015/1502 (1) have been met in order to reach a level of assurance of an electronic identification means under the scheme the Commission is being notified of:

4.2.1. Enrolment

(a) Application and registration

Application and registration are described in section 2.1.1. of the LoA mapping document.

(b) Identity-proofing and verification (natural person)

Identity-proofing and verification (natural person) is described in section 2.1.2. of the LoA mapping document.

(c) Identity-proofing and verification (legal person)

Latvian eID scheme is used only for identification of natural persons; therefore, this is not applicable.

(d) Binding between the electronic identification means of natural and legal persons

Latvian eID scheme is used only for identification of natural persons; therefore, this is not applicable.

4.2.2. Electronic identification means management

(a) Electronic identification means characteristics and design (including, where appropriate, information on security certification)

Electronic identification means characteristics and design are described in section 2.2.1. of the LoA mapping document.

(b) Issuance, delivery, and activation

Issuance, delivery, and activation is described in section 2.2.2. of the LoA mapping document.

(c) Suspension, revocation, and reactivation

Suspension, revocation, and reactivation is described in section 2.2.3. of the LoA mapping document.

(d) Renewal and replacement

Renewal and replacement are described in section 2.2.4. of the LoA mapping document.

4.2.3. Authentication

Describe the authentication mechanism, including the terms of access to authentication by relying parties other than public sector bodies:

Authentication in Latvian eID scheme is managed by LVRTC e-identification platform. The LVRTC e-identification platform is conform to OAuth 2.0 standard, defined in Internet Engineering Task Force

RFC6749, and it uses Authorization Code flow[1]. LVRTC e-identification platform consists of Authorization Server and Resource Server (Identity provider).

OAuth2 provides secure delegated access, allowing relaying party application (a client) to access resources on a resource server on the behalf of a user, without the user sharing their authentication credentials with the client. In first step client requests Authorization Code from Authorization Server. This request is approved by user. Then client acquires an Access Token with limited usage scope from Authorization Server. Afterwards client requests identity data of user form Resource Server by using this Access Token. Whole communication is TLS protected.

Steps of authorization flow are described below:

- ***Terms of access to authentication***
  To use the LVRTC e-identification platform API, each relying party must register its client application within the LVRTC e-identification platform. During registration process the client_id, client_secret (password) and corresponding API Access Key are created. According to the OAuth 2.0 specification, this key is used in all API requests by client.
- ***Authorization Code request***
  In Latvian eID scheme, the user wanting to use a client application that requires authentication is redirected to Authorization server of EIPS LVRTC and is presented with a browser screen to choose Electronic Identification Means. If user chooses smartcard based EIM ("eID karte", "eParaksts karte" or "eParaksta karte+"), browser plugin should be installed. If user chooses EIM "eParaksts", mobile phone with "eParaksts mobile" application containing authentication certificate is required. After entering PIN user is authenticated by using public/private key of certificate. Validity of certificate is checked against OCSP. By authentication user authorizes issue of Authorization Code by Authorization Server. This code is sent to server side of client application.
- ***Issue of Access Token***
  In next step client (server side) requests Access Token from Authorization Server by providing Authorization Code.
- ***Resource request***
  In last step client (server side) requests a resource – identification data of user – from Resource Server by using Access Token. After validation of Access Token resource is returned to client.

LVRTC e-identification platform is built on base of TrustedX eIDAS Platform (https://www.safelayer.com/en/products/trustedx-eidas-platform) by Safelayer. This is a Web services platform for integrating identification, authentication and electronic signatures. It combines authentication, single sign-on (SSO), identity federation and authentication trust level management functionality. Different authentication methods including PKI, SMS/email One-time passwords and mobile authentication are provided. It provides REST Web services API that is implemented via the OAuth 2.0/OpenID Connect and SAML and can be used through HTTP protocol.

4.2.4. Management and organisation

Describe the management and organisation of the following aspects:

(a) General provisions on management and organisation

General provisions are described in section 2.4.1. of the LoA mapping document.

(b) Published notices and user information

Published notices and user information are described in section 2.4.2. of the LoA mapping document.

(c) Information security management

[1] https://tools.ietf.org/html/rfc6749#section-4.1

Information security management is described in section 2.4.3. of the LoA mapping document.

(d) Record-keeping

Record-keeping is described in section 2.4.4. of the LoA mapping document.

(e) Facilities and staff

Facilities and staff are described in section 2.4.5. of the LoA mapping document.

(f) Technical controls

Technical controls are described in section 2.4.6. of the LoA mapping document.

(g) Compliance and audit

Compliance and audit are described in section 2.4.7. of the LoA mapping document.

4.3. Interoperability requirements

Describe how the interoperability and minimum technical and operational security requirements under Commission Implementing Regulation (EU) 2015/1501 (2) are met. List and attach any document that may give further information on compliance, such as the opinion of the Cooperation Network, external audits, etc.

How the Latvian eID scheme meets the interoperability and minimum technical and operational security requirements under Commission Implementing Regulation (EU) 2015/1501 is described in IF mapping document.

4.4. Supporting documents

List of all supporting documentation is submitted and states to which of the elements above they relate. Includes any domestic legislation, which relates to the electronic identification provision relevant to this notification. Submit an English version or English translation whenever available.

List of Notification documents

1. Level of assurance mapping document “LoA mapping: Mapping of the characteristics of the Latvian eID scheme to the eIDAS Level of Assurance”
2. Interoperability mapping document “IF mapping: Fulfilment of interoperability requirements according to (EU) 2015/1501”

List of national legislation related to the electronic identification in Latvia

1. Personal Identification Documents Law, https://likumi.lv/ta/en/en/id/243484
2. Law on Electronic Identification of Natural Persons, https://likumi.lv/ta/en/en/id/278001
3. Personal Data Processing Law (in Latvian only), https://likumi.lv/ta/id/300099-fizisko-personu-datu-apstrades-likums
4. Regulation regarding personal identification documents, https://likumi.lv/ta/en/en/id/244720
5. Regulation on the technical and organizational requirements of a qualified and qualified enhanced-security electronic identification service provider and its service (in Latvian only), https://likumi.lv/ta/id/293654-noteikumi-par-kvalificeta-un-kvalificeta-paaugstinatas-drosibas-elektroniskas-identifikacijas-pakalpojuma-sniedzeja-un-ta
6. Regulation on the information to be specified in the security description of information systems, equipment and procedures for the provision of qualified or qualified enhanced-security electronic identification services (in Latvian only), https://likumi.lv/ta/id/293652-noteikumi-par-kvalificeta-vai-kvalificeta-paaugstinatas-drosibas-elektroniskas-identifikacijas-pakalpojuma-sniegsanas-informacijas

List of EISP LVRTC documents

7. General terms and conditions of the Trust Services, LVRTC, https://www.eparaksts.lv/download/1_1_Noteikumi_GTAC_EN_03%20(1)_03042018_083445.pdf
8. Certificate Practice Statement, LVRTC (in Latvian only), https://www.eparaksts.lv/download/1_3_Noteikumi_CPS_LV_03_14052018_084304.pdf.
9. "eID karte" Trust service policy, LVRTC, https://www.eparaksts.lv/download/1_4_2_Politika_eID_EN_01_2_03042018_080133.pdf
10. "eParaksts karte" Trust service policy, LVRTC, https://www.eparaksts.lv/download/1_4_4_Politika_eParaksts_karte_EN_01_03_16042018_104313.pdf
11. "eParaksts karte+" Trust service policy, LVRTC, https://www.eparaksts.lv/download/1_4_5_Politika_eParaksts_karte+_EN_01_2_16042018_104345.pdf
12. "eParaksts" Trust service policy, LVRTC, https://www.eparaksts.lv/download/1_4_3_Politika_eParaksts_EN_01_02_03042018_080221.pdf
13. Security description of electronic identification of physical persons, LVRTC (in Latvian only), https://www.eparaksts.lv/download/LVRTC_Drosibas_aparaksts_LV-01_00_13112018_082140.pdf
14. E-IDENTIFICATION PROVISIONING PLATFORM (EISP). DEVELOPER GUIDE, LVRTC, https://www.eparaksts.lv/download/2017_Developer_Guide_LVRTC_v0.8_02082018_103848.pdf