LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN

eID Scheme of the Principality of Liechtenstein

Notification Form for eID.li Class A

for Electronic Identity Scheme under Article 9(5) of Regulation (EU) No 910/2014

December 2022

Letter from the Prime Minister

With reference to the Opinion No. 6/2022 of the Cooperation Network on the Liechtenstein eID means "eID.li", adopted on 12 December 2022, the Principality of Liechtenstein notifies two separate eID schemes based on the eID class. This Notification Form lays out the details for the notification of one of them, eID.li class A.

The Principality of Liechtenstein 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 the Principality of Liechtenstein.

Vaduz, December 2022

REGIERUNG DES FÜRSTENTUMS LIECHTENSTEIN	**Unterzeichner**	Dr. Daniel Risch Regierungschef
	Datum/Zeit-UTC	2023-01-30T15:22:32+01:00
Prüfinformation	Signiert mit PrimeSign, einem Produkt der PrimeSign GmbH. Informationen zur Prüfung finden Sie unter http://www.signaturpruefung.gv.at	

Dr Daniel Risch
Prime Minister of the Principality of Liechtenstein

1 General information

Title of scheme	*Level(s) of assurance (low, substantial or high)*
eID.li class A	HIGH

2 Authority responsible for the scheme

Name of authority	*Postal address*	*E-mail address*	*Telephone No*
Ausländer- und Passamt APA	Städtle 38 Postfach 684 9490 Vaduz Liechtenstein	info@eid.li	+423 236 61 41

3 Information on relevant parties

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 procedure

Name of entity which manages the registration process of the unique person identification data	*Documentation References*
Ausländer- und Passamt APA (Migration and Passport Office) The APA is subordinate to the Ministry of Home Affairs, Economy and Environment. Residents of the country as well as a large portion of the workforce living abroad deal with this office on a regular basis. Its tasks include the issuance of passports and identity cards to citizens and the provisioning of permits for foreigners and cross-border commuters. The APA is also responsible for managing the lifecycle of eID.li class A.	White Paper Annex 3: Governance Annex 4: Legal Framework

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	*Documentation References*
Ausländer- und Passamt APA (Migration and Passport Office) Art. 7 (a) (i) of the eIDAS Regulation (EU) No 910/2014 applies.	White Paper Annex 3: Governance Annex 4: Legal Framework

3.3 Party operating the authentication procedure

Name of the party operating the authentication procedure	*Documentation References*
Amt für Informatik AI (Office of Information Technology)	White Paper Annex 3: Governance Annex 4: Legal Framework

3.4 Supervisory body

Name of the supervisory body	*Documentation References*
The **Ministry of Home Affairs, Economy and Environment** is the supervisory body of the Migration and Passport Office (APA), which is the issuing authority for eID.li class A. Reviews and audits to ensure compliancy and proper execution of duties are conducted according to the law, in particular "Gesetz über die Regierungs- und Verwaltungsorganisation (RVOG)".	Annex 3: Governance Annex 4: Legal Framework
The **Ministry of General Government Affairs and Finance** is the supervisory body of the Office of Information Technology, which is responsible for operating the eID infrastructure. Reviews and audits to ensure compliancy and proper execution of duties are conducted according to the law, in particular "Gesetz über die Regierungs- und Verwaltungsorganisation (RVOG)".	Annex 3: Governance Annex 4: Legal Framework
The **Security Office** reports administratively to the Office of Information Technology; however, it is fully independent when it comes to ensuring the secure and compliant delivery of digital services to the consumers, including eID.li class A. The Security Office is authorised to plan, schedule and execute independent internal and external audits at their own discretion. Audits are carried out in accordance with the audit plan of the Security Office.	Trust Framework and LoA Mapping Annex 3: Governance Annex 4: Legal Framework

4 Description of the electronic identification scheme

(a) Briefly describe the scheme including the context within which it operates and its scope	*Documentation References*
eID.li class A was released to the public in early 2020. Everyone registered in the Central Registry of Persons is entitled to obtain eID.li class A. The eID system combines identity and access management technology with mobile services. To obtain eID.li class A, natural persons identify themselves in-person at the Migration and Passport Office (APA). After successful identification, the APA activates the user's eID.li App to use their proper eID.li class A. Service providers authenticate users of eID.li class A by sending an authentication request to the eID system. The eID system takes care of the interaction with the eID.li App of the user and eventually provides an authentication response to the service provider, which contains attributes like name, family name, date of birth, and the LoA of eID.li class A, which is HIGH. Each time the eID.li App is started, it loads the user's identity data for as long as the authentication procedure lasts. No personal data is retained in the mobile device, nor in the eID.li App after it is closed or put into standby mode. The eID system allows access to services provided only by public service providers. As soon as the necessary legal basis is in place, the eID system can be expanded to also allow access to private service providers. The eIDAS node of Liechtenstein has been in operation since August 2022 and notified eID schemes of other Member States can access public services. Once eID.li class A has been notified, the node will federate it for identification and authentication with digital services from other Member States.	White Paper System Architecture Interoperability Framework Trust Framework and LoA Mapping Annex 1: Mobile App for eID.li Annex 2: Security and Privacy Annex 3: Governance Annex 4: Legal Framework

(b) Where applicable, list the additional attributes which may be provided for natural persons under the scheme if requested by a relying party	*Documentation References*
Not applicable.	n/a
(c) Where applicable, list the additional attributes which may be provided for legal persons under the scheme if requested by a relying party	*Documentation References*
Not applicable.	n/a

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:
(where applicable, information shall include the roles, responsibilities and powers of the supervising body referred to in point 3.4, and the entity to which it reports. If the supervising body does not report to the authority responsible for the scheme, full details of the entity to which it reports shall be provided).

(a) supervisory regime applicable to the party issuing the electronic identification means	*Documentation References*
See 3.4 above.	
(b) supervisory regime applicable to the party operating the authentication procedure	*Documentation References*
See 3.4 above.	

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	*Documentation References*
The law explicitly acknowledges the liability ruling specified in the eIDAS Regulation (EU) 910/2014.	Trust Framework and LoA Mapping Annex 4: Legal Framework
(b) liability of the party issuing the electronic identification means under Article 11(2) of Regulation (EU) No 910/2014	*Documentation References*
The law explicitly acknowledges the liability ruling specified in the eIDAS Regulation (EU) 910/2014.	Trust Framework and LoA Mapping Annex 4: Legal Framework
(c) liability of the party operating the authentication procedure under Article 11(3) of Regulation (EU) No 910/2014	*Documentation References*
The law explicitly acknowledges the liability ruling specified in the eIDAS Regulation (EU) 910/2014.	Trust Framework and LoA Mapping Annex 4: Legal Framework

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	*Documentation References*
The eID system is constantly monitored jointly by the provider of the mobile cloud services and the local operations centre at the AI (Office of Information Technology). If the eID system or parts thereof should be compromised, the AI would immediately shut down all eID services, then start an investigation of the cause and develop a plan for remedy. In case the Migration and Passport Office (APA) is made aware of a compromised eID.li class A, it would immediately suspend it using the APA business application. Once suspended, eID.li class A is no longer functional and can therefore no longer be used. To unblock eID.li class A, the user must identify himself in-person at the APA.	System Architecture Trust Framework and LoA Mapping Annex 1: Mobile App for eID.li

Revocation of eID.li class A is the same as suspending it permanently. eID.li class A is not available unless enabled again by the Migration and Passport Office (APA) using the APA business application.	

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	*Documentation References*
The supporting documentation provided with this notification contains a detailed description of the enrolment process.	White Paper System Architecture Trust Framework and LoA Mapping Annex 1: Mobile App for eID.li Annex 2: Security and Privacy Annex 3: Governance
(b) Identity proofing and verification (natural person)	*Documentation References*
The supporting documentation provided with this notification contains a thorough description of the procedures for identity proofing and verification for natural persons. For eID.li class A, the user must identify himself in-person at the Migration and Passport Office (APA). eID.li is then labelled "class A" in the Central Registry of Persons by the APA, indicating that the necessary requirements as specified under the eIDAS Regulation assurance level HIGH are met.	White Paper Trust Framework and LoA Mapping Annex 3: Governance
(c) Identity proofing and verification (legal person)	*Documentation References*
Not applicable.	
(d) Binding between the electronic identification means of natural and legal persons	*Documentation References*
Not applicable.	

4.2.2 Electronic identification means management

(a) Electronic identification means characteristics and design (including, where appropriate, information on security certification)	*Documentation References*
The eID.li App is protected by strong authentication that includes up to three authentication factors from different categories: "you have" (possession of the mobile device), "you know" (password) and, optionally, "you are" (biometrics). The supporting documentation provided with this notification contains a thorough description of the design of the eID.li App, how it is used and the security of the eID system as a whole. The password policy does not allow to set easy-to-guess passwords and prevents brute force attacks. The eID.li App uses hardware-backed keystore, and it does not run on mobile devices with known vulnerabilities or on rooted, jailbroken devices.	White Paper System Architecture Trust Framework and LoA Mapping Annex 1: Mobile App for eID.li Annex 2: Security and Privacy Annex 3: Governance
(b) Issuance, delivery and activation	*Documentation References*
Issuance: The eID.li App is the control tool for the eID.li class A, and it is available for free on iOS version 13.0 and above, and Android 8 and above. Delivery and activation: The Migration and Passport Office (APA) has full control over the activation status of eID.li class A. Authorised personnel at	White Paper System Architecture Trust Framework and LoA Mapping

the APA can suspend or activate eID.li class A using the APA business application. When the status is set to active for the first time, this is the moment when eID.li class A is finally "delivered".	Annex 1: Mobile App for eID.li
(c) Suspension, revocation and reactivation	*Documentation References*
The Migration and Passport Office (APA) is always in control of the activation status of eID.li class A. It can suspend or activate eID.li class A using the APA business application. Revocation of eID.li class A is the same as suspending it permanently. eID.li class A is not available unless the status is set to active again using the APA business application. Suspension and revocation services are available 24/7.	White Paper System Architecture Trust Framework and LoA Mapping Annex 1: Mobile App for eID.li
(d) Renewal and replacement	*Documentation References*
The eID.li App is not eID.li class A, but a controlling tool for it, and no personal data is stored in the app or on the mobile device. Thus, eID.li class A cannot get lost, but control over the eID.li App can. The personal data provided with eID.li class A in an identification is up to date at all times. If a user's personal data in the Central Registry of Person changes, this has immediate effect on eID.li class A, hence there is no need to renew or replace eID.li class A. The eID.li App is regularly updated, and the cryptographic keys are regularly renewed as well.	White Paper System Architecture Trust Framework and LoA Mapping Annex 1: Mobile App for eID.li Annex 2: Security and Privacy

4.2.3 Authentication

Describe the authentication mechanism including terms of access to authentication by relying parties other than public sector bodies	*Documentation References*
The supporting documentation provided with this notification contains a thorough description of the authentication mechanism. The eID system is technically ready to serve non-public, private relying parties. However, the legal basis to release the eID system to the private sector has yet to be enacted. Until then, eID.li class A is available for E-Government services only.	White Paper System Architecture Trust Framework and LoA Mapping Annex 1: Mobile App for eID.li

4.2.4 Electronic identification means management

Describe the management and organisation of the following aspects:

(a) General provisions on management and organisation	*Documentation References*
The Migration and Passport Office (APA) is the issuer of eID.li class A, while the AI (Office of Information Technology) is responsible for operating the eID infrastructure. Both offices act on behalf of the State Government and their duties are defined by the law. The E-Government Law and E-Government Ordinance specifiy the goals, duties, and range of applicability of eID.li.	White Paper Trust Framework and LoA Mapping Annex 3: Governance Annex 4: Legal Framework
(b) Published notices and user information	*Documentation References*
A description of the purpose and scope of eID.li, regardless of class, is provided in the law. A description of the eID system services, the applicable restrictions, and limitations, as well as the terms and conditions are provided in the eID.li App and on the official website. The terms and conditions must be accepted upon enrolment by the user in the eID.li App.	Trust Framework and LoA Mapping Annex 5: End User Terms and Conditions

(c) Information security management	*Documentation References*
Each time a new service is developed, integrated, or deployed, a risk assessment is carried out, and measures are specified to mitigate risks and identify residual risks. When the service is undergoing change, the risks are reassessed to consider the potential for new security requirements. All those principles have been applied and continue to be applied to the eID system. In addition, proven information security standards for the management and control of security risks are employed.	Trust Framework and LoA Mapping Annex 2: Security and Privacy Annex 3: Governance
(d) Record keeping	*Documentation References*
Data is retained for auditing and to ensure proper execution of the life cycle processes of eID.li class A in accordance with the law.	Trust Framework and LoA Mapping
(e) Facilities and staff	*Documentation References*
Procedures are in place to ensure that staff and subcontractors are sufficiently trained, qualified, and experienced in the skills needed to execute the roles they fulfil. There is sufficient staff to adequately operate the eID system services according to the quality requirements and security policy. All facilities used for providing the service are continuously monitored for, and protected against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service. Facilities used for providing the service ensure that access to areas holding or processing personal or sensitive information or cryptographic material is limited to authorised staff or subcontractors.	Trust Framework and LoA Mapping Annex 2: Security and Privacy
(f) Technical controls	*Documentation References*
Technical controls are in place to mitigate the security risks of the services and to protect confidentiality, integrity, and availability. All communications between the components of the eID system and to outside entities, like service providers, are encrypted. As far as the eID system is concerned, key generation and distribution are fully integrated into the eID.li App and keys for authentication and encryption are stored in the secure area of the mobile device. Access to keys and certificates that are used to protect communication between the components of the eID system are kept in highly secured areas and they are only accessible to authorised personnel. Procedures for security incident management and response have been defined and implemented. It is confirmed that all media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.	Trust Framework and LoA Mapping Annex 2: Security and Privacy Annex 3: Governance
(g) Compliance and audit	*Documentation References*
The Security Office is authorised to plan, schedule and execute independent internal and external audits at their own discretion. In accordance with the audit plan of the Security Office, audits of the eID system are performed on a regular basis.	Trust Framework and LoA Mapping Annex 2: Security and Privacy Annex 3: Governance

4.3 Interoperability requirements

Describe how the interoperability and minimum technical and operational security requirements under Commission Implementing Regulation (EU) 2015/1501 (1) 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.	*Documentation References*
The Interoperability Framework specifies the design and implementation of the eIDAS node and how it meets the interoperability requirements under Commission Implementing Regulation (EU) 2015/1501.	Interoperability Framework

If the user identifies or authenticates himself in a cross-border context with other Member States, the eIDAS node specifies the assurance level of eID.li class A as HIGH. To mitigate any potential risk associated with biometrics, the eIDAS node federates eID.li class A only if the user is providing consent using the PIN or password, but not biometrics.	

4.4 Supporting documents

List here all supporting documentation submitted and state to which of the elements above they relate. Include any domestic legislation which relates to the electronic identification provision relevant to this notification. Submit an English version or English translation whenever available.	*Documentation References*
The supporting documentation consists of the documents listed on the right. The relevant laws are mentioned throughout the documentation and can be consulted at any time using the information in Annex 6: References and Glossary.	White Paper System Architecture Interoperability Framework Trust Framework and LoA Mapping Annex 1: Mobile App for eID.li Annex 2: Security and Privacy Annex 3: Governance Annex 4: Legal Framework Annex 5: End User Terms and Conditions Annex 6: References and Glossary