Approved by the Management Board of the Estonian Internet Foundation and entered into force on 31.08.2021

" SUBSCRIPTION AGREEMENT AND TERMS OF USE OF THE ESTONIAN INTERNET FOUNDATION ELECTRONIC IDENTIFICATION SERVICE (eeID)"
Annex 2

DATA PROTECTION TERMS FOR AUTHENTICATION SERVICES

1. This document explains which personal data are processed in the authentication service of the Estonian Internet Foundation (hereinafter EIF) and for what purpose.

2. These data protection conditions apply to the use of the electronic identification service of the Estonian Internet Foundation.

3. The data subject (hereinafter user) is a natural person who is directed from an Estonian or foreign customer application (e.g., from an e-service) to the EIF authentication service identification (authentication).

4. Authentication data
4.1. The services process the following data about users ("authentication data"): user identification data:

- the user's authentication certificate;
- the user's personal identification code or other personal identifier;
- the user's first and last name;
- the user's date of birth;
- the user's country;
- registry code or other identifier of the legal person;
- business name of the legal person;
- the name, personal identification code, e-mail address and telephone number of the contact person of the subscribed e-service.

Authentication details:

- date and time;
- the customer application from which the user was directed to authentication;
- authentication method, in case of a bank link also the bank; in the case of a mobile ID, the mobile number;
- authentication result (authenticated or not).

4.2. Issuance of authentication data
4.2.1. Authentication data is issued to a customer application interfaced with the EIF authentication service.
4.2.1.1. In case of authentication with an ID card, mobile ID and Smart ID authentication data is sent to external services of SK ID Solutions AS in the following composition:
4.2.1.1.1. Validation confirmation service (user authentication certificate serial number);
4.2.1.1.2. MID REST API web service (user ID and mobile number);
4.2.1.1.3. Smart-ID web service (user's personal identification code).
4.2.2. Issuance of data is based on the principle of minimality of processing of personal

data. The minimum data identifying the authentication fact and identified person. For example, when authenticating with a mobile ID, the user's mobile number is not issued to customer applications interfaced with the EIF authentication services.
4.2.3. The result of the authentication (logged in or not) is visible to the user in the browser.
4.3. Encrypted channels are used to communicate with customer applications.

5. Security log
5.1. In the service, the data of authentication procedures will be logged together with personal identification data for the following purposes:
5.1.1. to detect and investigate misuse of the service, including identity theft and its attempts, as well as cyber-attacks;
5.1.2. to detect and rectify technical failures. A technical failure can be a hardware or software failure, a network connection failure, etc.;
5.1.3. to identify the causes of technical problems reported by the owners of the e-services interfaced with the services, ie the authorities;
5.1.4. to handle user inquiries (notifications of possible security issues or technical failures).
5.2. Access to the log is strictly needs-based. Only system and service operators directly involved in the operation of the service, including, where appropriate, security incident investigators, shall have access.
5.3. We also recommend logging in to the customer application for authentications. This is necessary to detect and investigate both technical failures and misuse of the service.

6. Contact persons of the interfaced authority
For the purpose of service management, the contact details of the interfaced authorities are collected.

7. Data backup
7.1. The backup process starts at least once a day. Backups of all service component data (configuration, database, logs) are stored on the same principle - 7 days / 4 weeks / 12 months.
7.2. It is possible to restore the data stored as of the days of the current week, the end of the weeks of the current month or the end of the last 12 months.

8. Issuance of security logs
The security log is issued if required by law (for example, to a law enforcement authority in criminal proceedings or to a data subject at his or her request).