16.5.2024

Annex 3, Terms of Delivery for Identification Service Usage Rights, Elisa Corporation – Service description of the Trust Network Interface

The Mobile Certificate is a service for companies offering e-commerce services that allows them to reliably verify the identity of their customers, regardless of the service channel.

Using Elisa's Trust Network Interface, the identification broker service can integrate Mobile Certificate into its own service and offer service providers the opportunity to improve their customer service – making it easier to identify customers online, over the phone and in person.

Mobile Certificate enables authentication, login, retrieval of additional information, electronic approval and signatures.

The service provided by Elisa uses the Mobile Certificate, developed in cooperation between Finnish teleoperators, which is a service that can be added to SIM cards or existing DNA, Elisa and Telia Finland phone subscriptions and which acts as an electronic identification means as defined in the relevant legislation.

Mobile Certificate enables strong legal identification of Varmenne users from all teleoperators.

It enables the implementation of new electronic services and improves the usability and security of existing services:

- **Identification:** For internet services on PCs and mobile phones, the user can be identified, for example, when logging in to a service. Identification can also be easily and reliably performed in various telephone services and customer service situations.

- **Approval and signatures:** Electronic signatures can be used to approve transactions and orders and to confirm orders. Confirming a document with an electronic signature eliminates the need for physical presence and allows for increased productivity through reduced paper handling.

1 Content of the service

Mobile Certificate is a SaaS service used over the internet. When a service provider needs to identify a customer, an Identification Broker Service Provider's system sends an identification request to the Mobile Certificate service. Elisa's service receives the request and forwards the identification request to the service of the operator whose service the user in question has joined. After the user confirms the identification request, information about the identification is forwarded to the Identification Broker Service Provider. If the user's certificate is blacklisted, information about this will be returned to the Identification Broker Service Provider.

Elisa's Mobile Certificate service for Identification Broker Service Providers consists of the following service components:

- **Legislation-compliant strong electronic identification:** Service providers can reliably identify their customers using Elisa's identification service. The service can be used, for example, for logging in to online and telephone services, identifying a person during a call, and approving various transactions that require identification.

- **Approval and signatures:** Service providers can ask their users to electronically sign some content using their mobile phone by sending a signature request. The service can be used in both online and telephone services, for example in contracts and agreements entered into over the telephone and changes to such contracts and agreements, or for orders and payment confirmations that take place in the service.

- **OIDC interface (strong electronic identification):** Identification service in accordance with Traficom Regulation M72B and Traficom Recommendation 213/2023S. An identification interface designed for use in a web browser, where the browser is used to identify a user in an external identification service, and finally the reference information is returned to the transaction service, which is used to retrieve the actual personal data. Data transfer takes place using encrypted connections.

- **ETSI interface ("Identify Your Customer" and "Approval and Signature" services):** An interface in line with the ETSI TS 102 204 specification, the functionality of which is described in the FiCom application guide, which complements the ETSI standards. The interface is connected with an encrypted XML interface. The mobile signature is returned to the service provider as a signature message in PKCS#7 format.

- **Elisa Lisätieto interface ("Identify Your Customer" and "Establish Customer Relationship" services):** An encrypted REST HTTP interface through which service providers can define the additional information attributes they want. The response message is in either XML or JSON format, in accordance with the service provider's request.

The properties and operation of the interfaces are detailed in the relevant technical specifications.

2 Conditions and limitations

The Identification Service Provider implementing the Trust Network Interface must be a strong electronic identification provider registered with Traficom.

When using the ETSI interface or the Elisa Lisätieto interface in accordance with the FiCom specifications, the Identification Service Provider is responsible for the service provider's obligations as laid out in the FiCom specifications.

In other respects, the Identification Service Provider is responsible for the obligations assigned in Elisa's contracts and agreements, the law, regulations and regulations from Traficom.

Each party is responsible for the protection and security of its own services and the correctness of the information it stores.

Purposes and limitations of the service:

- Legislation-compliant strong electronic identification: The service is intended for the identification of natural persons using a mobile certificate. The use of the identification service for other purposes is prohibited without separate agreement. The storage and use of personal data transmitted in the identification service is limited by the terms and conditions of the service and by the identification principles implemented by the issuers of the identification means.

3 Service delivery

The Identification Service Provider uses the order form to order the service, and at the same time, commits to the terms of use of the identification and signature service.

1. The service provider fills out the order form for the Trust Network Interface service provided by Elisa.
    - The order form specifies e.g. service components and, if necessary, interfaces
        - OIDC interface
        - Identify Your Customer service (Single authentication)
        - Electronic Initial Identification (Chaining)
        - Approval and Signature service
    - The agreement also specifies the information to be transmitted:
        - The current identification options are:
            - Electronic Unique Identification Number (SATU)
            - Personal identity code (HETU)
    - The terms of the agreement limit the use of name and identification information provided by Elisa.

2. Elisa or a technical platform provider acting on behalf of Elisa supplies the service provider with the necessary connection keys:
    - The information is delivered using a secure method to the customer's contact person named in the contract.

3. The necessary communication connections are opened:

- The security of message traffic between the parties is guaranteed by methods that meet Traficom's requirements.

3.1 Delivery time

Elisa delivers the order confirmation to the service provider, which shows the delivery time and content of the order, as well as the price of the service. When the interface chosen by the service provider has been opened for the customer, the customer is notified that the service is available.

The delivery time of the service is at least four (4) weeks, unless otherwise agreed with the customer.

4 Use of the service

Elisa only handles the identification of the customer as described in this service description. Elisa is not responsible for the binding nature or content of any legal transaction between a customer and the service provider.

Each party is responsible for the protection and security of their own services and the correctness of the information they store.

Customers using Mobile Certificate for identification are responsible for ensuring that their Mobile Certificate and its security codes do not fall into the hands of others, makes sure that the identification service returns the identification information to the service provider, and must accept the transmission of the identification.

4.1 Service levels

The service includes the basic service level. The response and resolution times for the basic service level and any available special service levels with their response and resolution times are described in the table below.

Service levels exceeding the basic service level must be agreed separately in the agreement.

Service level category	Service response time category	Response time	Resolution time
P0V8h basic service level	P0: business days: Mon–Fri, 8 am – 4 pm	Target: 8 h	Target: 24 h

Response and resolution times are counted only during the times specified in the service response time category.

The precise content and application of the service levels are described in more detail in the Elisa SLA service description. The customer-specific service level is specified in the offer and is agreed upon in the delivery agreement concluded with the customer.

5 Pricing

The price of the service is specified in the separate price list annexed to the agreement.

6 Terms and conditions

The terms and conditions of the service and its delivery are specified in the document “Terms of Delivery for Identification Service Usage Rights, Elisa Corporation”.