Service description

Confidential

Appendix 3

Date
May 29, 2019

Page
1 (14)

Version
1.0

Approved by
Esko Heimonen

Relation
Telia Tunnistus

Telia Tunnistus – Service Description

Contents

1 General description

Telia is an identification service provider as referred to in the legislation (Act on Strong Electronic Identification and Electronic Trust Services 617/2009, hereafter the “Identification Act”). Telia has been entered in the strong identification service register of the Finnish Communications Regulatory Authority (FICORA), and as from May 1, 2017, it has been part of the trust network referred to in the Identification Act. The trust network enables identification events performed with different identification devices to be transmitted to transaction services by means of uniform technical and administrative arrangements. Telia has concluded agreements with identification services on the transmission of identification to transmit electronic identification events to parties that trust electronic identification.

Telia Tunnistus is an identification transmission service that provides an easy solution for the customers’ needs for strong electronic identification. The customer concludes only one service agreement with Telia and is provided with several devices for strong electronic identification and a wide selection of modern ways to integrate strong identification with their web services.

The identification transmission service makes it possible to transmit strong electronic identification reliably and securely to the customer. The identification devices used for identification include

- mobile certificates, and
- online banking codes used by banks

The customer's web service can be connected to the identification according to the SAML, OpenID Connect and Tupas standards. As regards SAML and OpenID Connect interfaces, we apply FICORA’s recommendations on their use as the interface between an identification transmission service and a customer’s web service.

Telia Tunnistus is an electronic identification service that has been entered in FICORA’s register and that meets the requirements set for strong electronic identification by the Identification Act.

1.1 Terms and abbreviations

Term	Description
eIDAS	eIDAS is an EU regulation on electronic identification and trust services for electronic transactions in the internal market (910/2014).
Trust network	The trust network is a network of identification service providers that have submitted a notification to FICORA.
Mobile certificate	A mobile certificate is a service provided by Finnish mobile operators for strong electronic identification. The mobile certificate works on all mobile phones.
OpenID Connect	OpenID Connect (OIDC) is a REST-based interface on top of the OAuth 2.0 standard for sharing information related to the identification of information system users in data networks.
SAML	SAML (Security Assertion Markup Language) is an XML standard for sharing information related to the identification and authorization of information system users in data networks.

Term	Description
Identification service	An identification transmission service or a service providing an identification device.
Identification event	A chain of events where the holder of an identification device identifies him/herself in customer service (transaction service), and the transaction services uses the identification service of one or more parties to the agreement for establishing the identification or another characteristic of the identification device holder.
Identification device	An identification device is a method of strong electronic identification complying with the eIDAS regulation.
Identification transmission service	A service for transmitting strong electronic identification events to a party that trusts electronic identification.
Tupas bank code	Tupas is a service that banks have defined together for strong electronic identification of a person on the basis of their own registers.
Strong electronic identification	Strong electronic identification refers to electronic verification of identity. With strong electronic identification, consumers can securely authenticate themselves in a variety of electronic services based on eIDAS level substancial or high.

2 Trust network of identification services

The identification service providers referred to in the Act on Strong Electronic Identification and Electronic Trust Services are part of the common trust network. The members of the trust network, i.e. the identification service providers referred to in the act, include identification device providers and identification transmission service providers.

Telia Tunnistus is an identification transmission service, which serves as part of the trust network of identification services and transmits identification events to transaction and web services not belonging to the trust network. Mobile certificate is an identification device used for strong electronic identification in the trust network.

Telia Tunnistus is only available for web services within the EU.

Web services do not have right to transfer authentication outside their own domain (that is pass single-sing-on authentication).

Web services do not have right to use Telia Tunnistus for services that operate contrary to good practice.

Specific usage rules for identification device:

Mobiilivarmenne/**Elisa**: www.elisa.fi
Mobiilivarmenne/**DNA**: www.dna.fi
Mobiilivarmenne/**Telia**: www.telia.fi
OP: www.op.fi
-You are not allowed to accept payments for PSD2/RST with OP identification device when used via Finnish Trust Network.
Aktia: www.aktia.fi
Nordea: www.nordea.fi
-You are not allowed to use Nordea identification device for eIDAS international governmental services.
-Specific rules for inter portal single-sing on.

Danskebank: www.dankebank.fi
Handelsbanken: www.handelsbanken.fi
POP-Pankki: www.poppankki.fi
Säästöpankki: www.sp.fi
OmaSP: www.omasp.fi
Ålandsbanken: www.alandsbanken.fi

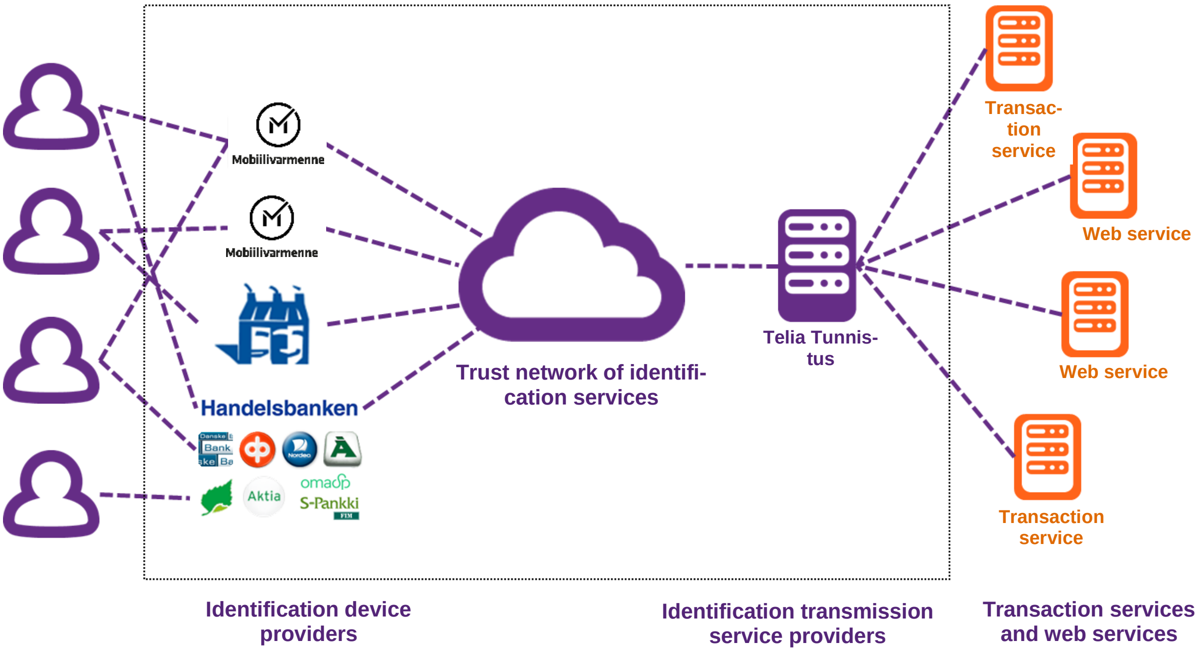
Mobiilivarmenne
Mobiilivarmenne
Handelsbanken
Aktia
omasp
S-Pankki
Trust network of identifi-cation services
Telia Tunnis-tus
Transac-tion service
Web service
Web service
Transaction service
Identification device providers
Identification transmission service providers
Transaction services and web services

Figure 1. Trust network of identification services

3 Description of the identification service

The customer’s transaction service is technically connected to the identification transmission server of the Telia Tunnistus service according to the service agreement.

Before the introduction of the service, the operation of the technical connection of the customer's transaction service is tested in Telia's test environment. When the connection of the transaction service has been approved, it is connected to the production environment of the service.

Strong electronic identification devices granted by identification device providers are used for the identification of transaction service users in identification events of the trust network. The holder of the identification device (the person) is a natural person or a legal person to whom the identification device provider has granted an identification device based on an agreement.

The identification device provider issues strong electronic identification devices and provides its identification device to the identification transmission service provider to be transmitted in the trust network. An identification device may also be granted even if the identification device provider does not have an identification service of their own, e.g. electronic ID granted by the authorities.

Telia Tunnistus is connected to the customer’s service utilizing strong electronic identification over an interface separately agreed on.

When the transaction service has been technically connected to the transmission service, the customer can send an identification request for the identification of the person, and this request is further transmitted to the identification service whose identification device is used for identifying the person in question.

The person accepts the identification request in a manner that depends on the identification device, e.g. with a PIN or the like. When the PIN or a similar code entered has been accepted, the identification message sent by the identification service is accepted on the identification device, and the person accepts the transaction he/she has made in the customer’s transaction service. When using and accepting transactions in the customer’s transaction service, the person is responsible for these transactions and their consequences.

The person can reject or refuse to accept an identification request. In this case, Telia Tunnistus notifies the customer of the failure of the identification request, i.e. on the rejection of the request.

The service launches strong electronic identification by sending an identification request through the interface. Telia Tunnistus transmits the identification request to an identification service providing strong electronic identification agreed on with the customer.

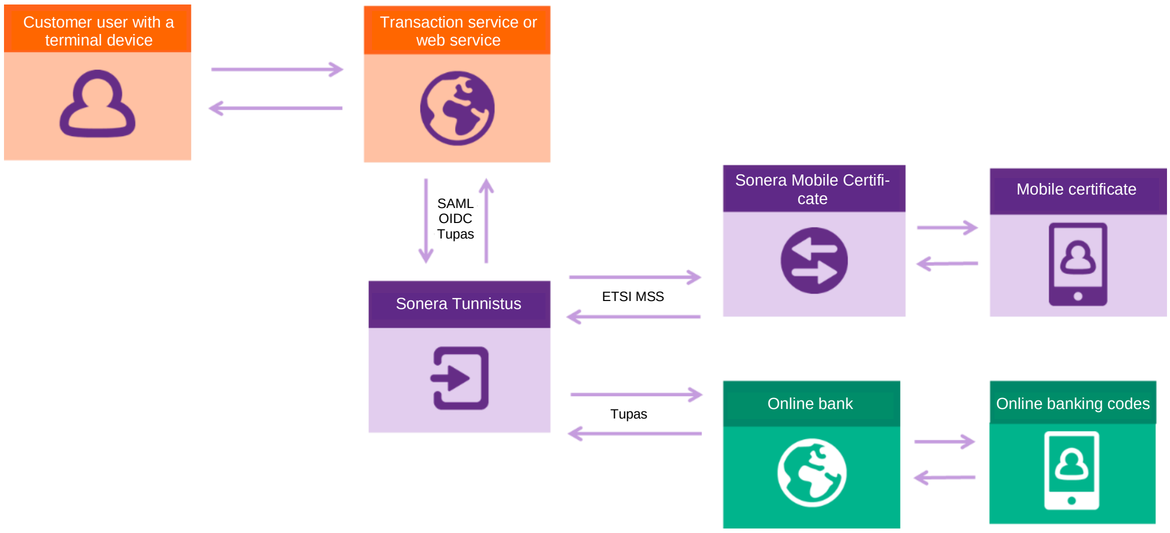
Customer user with a terminal device
Transaction service or web service
SAML
OIDC
Tupas
Sonera Tunnistus
ETSI MSS
Sonera Mobile Certificate
Mobile certificate
Tupas
Online bank
Online banking codes

Figure 2. Electronic identification in the trust network

3.1 Identification devices

Identification device refers to a method of strong electronic identification that can be used to verifiably identify a person using the service. Telia Tunnistus transmits a request for strong electronic identification to the provider of the selected identification device.

Telia Tunnistus enables strong electronic identification of a person by means of the following identification devices.

Identification device	Description
Mobile certificate	A person can perform strong electronic identification by means of a mobile certificate. The identification device providers of mobile certificate are Finnish operators.
Banking code	A person can perform strong electronic identification by means of a banking code provided by his/her own bank. The identification device providers of banking codes are Finnish banks.

The assurance level of the mobile certificate and banking code identification devices and services transmitted in the service is ‘substantial‘ according to the eIDAS regulation.

Telia is entitled to add and remove identification devices and services used in the service on the basis of the agreements valid at any given time.

3.2 Identification transmission methods

In identification transmission, the information on strong electronic identification is transmitted to the customer’s service. Telia Tunnistus provides several interfaces for the transmission of strong electronic identification.

Interface	Description
SAML	Information on an identification event is transmitted in messages complying with the SAML standard. It is also possible to apply FICORA’s recommendations for the use of an SAML interface in the interface configurations.

OpenID Connect	Information on an identification event is transmitted in messages complying with the OpenID Connect standard. It is also possible to apply FICORA’s recommendations for the use of an OpenID Connect interface in the interface configurations.
Tupas	Information on an identification event is transmitted by emulating the interface configurations of the Tupas standard.

3.3 Dialog page for selecting the identification method

Telia Tunnistus provides a dialog page to be connected to the customer's service to allow the service user to select the identification method that best suits him/her. If Telia and the customer have agreed only on the use of mobile certificate, the dialog page for selecting the identification method is not needed. In that case, identification is directed automatically to the Telia Tunnistus service and the use of mobile certificate.

Method	Description
Web link	The customer’s service has a “Login” link to the Telia Tunnistus service dialog page for selecting the identification method.
The dialog page is inserted in IFrame.	The Telia Tunnistus service dialog page for selecting the identification method is inserted in the website of the customer's service by means of the *IFrame* technology.
Dialog page directly in the service	The selected identification methods are embedded in the customer’s service. The customer’s service then determines in the identification request which identification device is used for the user’s strong identification.

As regards the web link, a *Login* link is added to the customer’s service (in the figure *customer.service.*fi). When a person clicks on the link, he/she moves to the Telia Tunnistus service (in the figure *tunnistus.telia*.fi) dialog page for selecting the identification method.

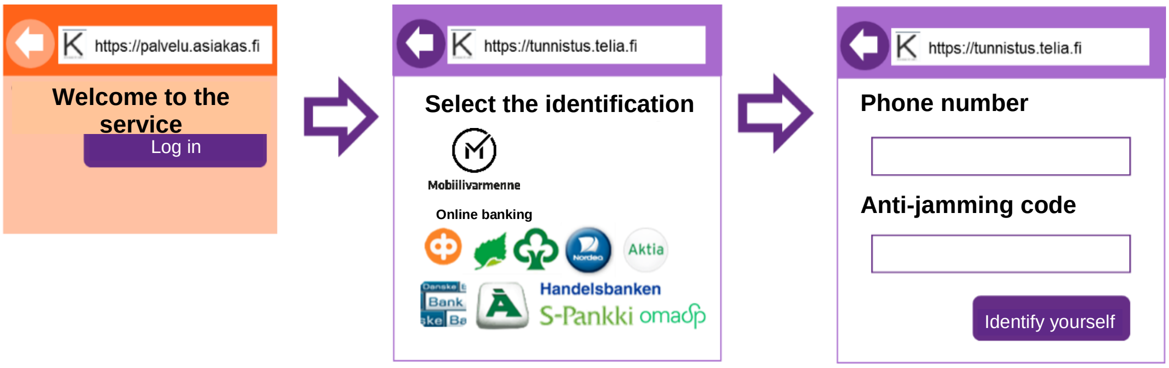

Figure 3. Use of the web link (identification by means of mobile certificate)

In the case of the IFrame technology, an *IFrame* element is embedded in the customer’s web service, and the contents of the element are retrieved from the address of the Telia Tunnistus service. For example, by means of the fancybox library, it is possible to open IFrame on top of the web service in the same way as a so-called modal window.

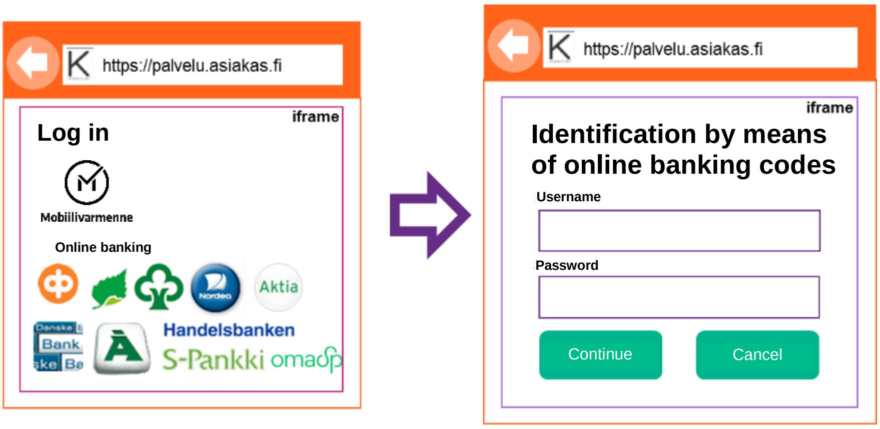

Figure 4. Insertion of the dialog page for selecting the identification method in an IFrame element (identification by means of online banking codes)

It is possible to embed the identification methods (icons) directly in the customer's web page. In this case, the customer's web service sends an identification request according to the interface to request identification by means of the selected method.

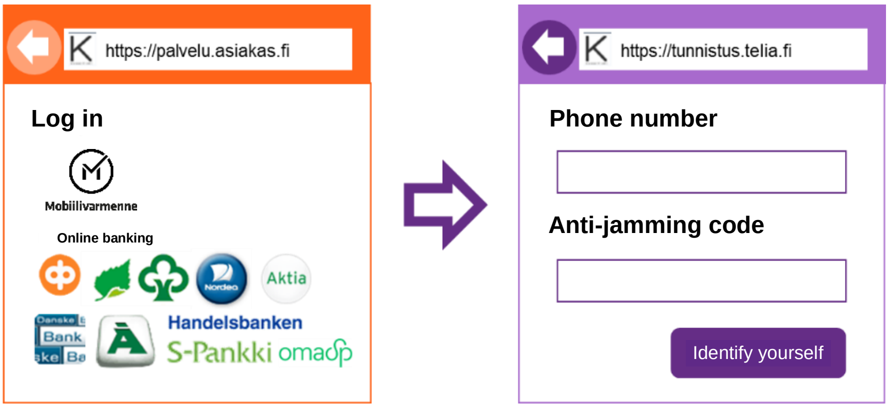

Figure 5. Selection of the identification method directly in the transaction service (identification by means of mobile certificate)

3.4 Single sign-on

Telia Tunnistus enables single sign-on to several different services of the customer by means of one and the same strong electronic identification. In this case, the user does not need to identify him/herself again. Single sign-on is to be agreed on separately with the customer.

Telia Tunnistus supports logout, which means that the person can no longer use the single sign-on within the scope of the previous identification event. If the customer's service uses the SAML interface of the Telia Tunnistus service, it is possible to transmit the logout request to the customer's service.

3.5 Initial identification

The customer has the right to use the Telia Tunnistus service for creating their own identification device (so-called chained initial identification) when granting an electronic identifier to their own customer (person) in order to verify the customer’s identity.

4 Attributes offered to customer service

After a successful identification request, Telia Tunnistus returns at least the following information on the identified user (person):

- the person's unique identifier (personal identity number)
- the person’s first name
- the person's last name
- the person’s date of birth

and information on the assurance level of the identification device (substantial or high).

5 An example of the use of the Telia Tunnistus service

5.1 Transmitting identification based on mobile certificate

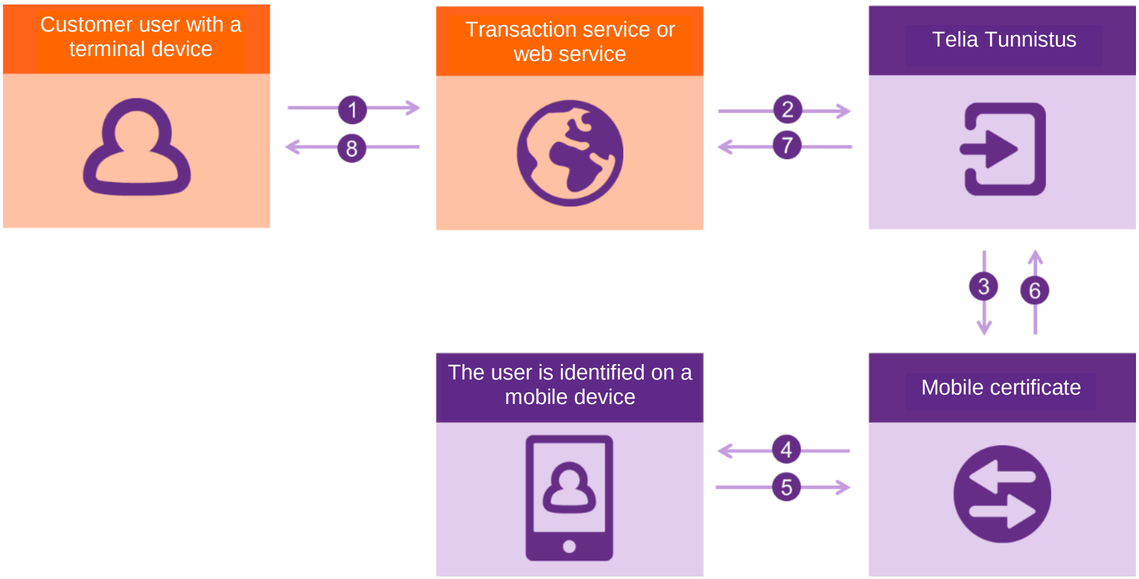
Customer user with a terminal device
Transaction service or web service
Telia Tunnistus
1
8
2
7
3
6
The user is identified on a mobile device
Mobile certificate
4
5

Figure 6. Transmission of identification (identification based on mobile certificate)

1. The customer’s service requires strong electronic identification of the person to be identified. The customer may define whether strong electronic identification is required for the use of the service in general or for only some of its functions.
2. The service directs the person to be identified to the Telia Tunnistus service over a predefined identification transmission interface (SAML, OpenID Connect or Tupas).
3. Telia Tunnistus sends an identification request to the mobile certificate service.
4. The mobile certificate service sends an identification request to the mobile phone of the person to be identified.
5. The person to be identified accepts the identification request by entering an anti-jamming code on request on the website, provided that the code has been activated, and by entering his/her PIN on the mobile phone.
6. Telia Mobile Certificate transmits the information on the identification event to the Telia Tunnistus service.

7. Telia Tunnistus transmits the information on the identification event to the customer's web service.
8. The customer's web service allows the person to be identified to access the function requiring strong electronic identification.

5.2 Transmitting identification based on banking codes

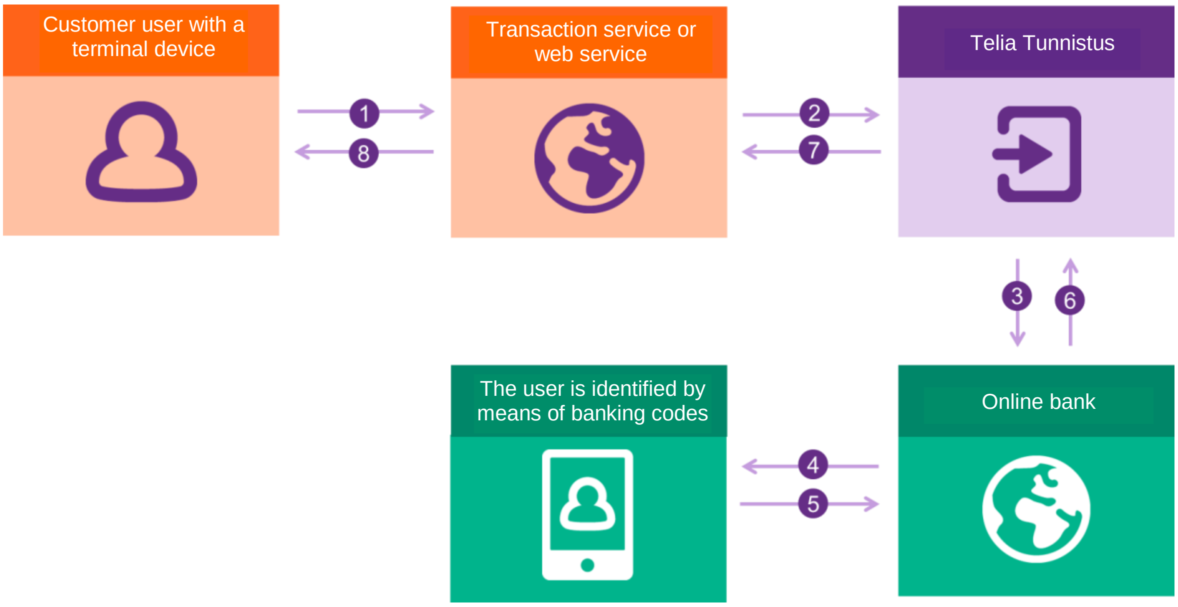
Customer user with a terminal device
Transaction service or web service
Telia Tunnistus
1
8
2
7
3
6
The user is identified by means of banking codes
Online bank
4
5

Figure 7. Transmitting identification (identification based on banking codes)

1. The customer's service requires strong electronic identification of the person. The customer may define whether strong electronic identification is required for the use of the service in general or for only some of its functions.
2. The service directs the person to the Telia Tunnistus service over a predefined identification transmission interface.
3. Telia Tunnistus sends a Tupas identification request to the selected banking service. The selection of the bank depends on how the selection of the identification method has been implemented in the customer's service.
4. The banking service sends an identification request to the person.
5. The person to be identified accepts the identification request by means of an identification device provided by the bank.
6. The banking service transmits the information on the identification event to the Telia Tunnistus service.
7. Telia Tunnistus transmits the information on the identification event to the customer's web service.
8. The customer's web service allows the person to access the function requiring strong electronic identification.

6 Contents of the identification service

The Telia Tunnistus service is available as a service tied to the number of events per month. The identification service includes the following service elements.

SERVICE ELEMENT	
Customer interface (SAML) for the transmission of identification events.	Included
Customer interface (OpenID Connect) for the transmission of identification events.	Included
Customer interface (Tupas) for the transmission of identification events.	Included
Transmission of the minimum personal data according to FICORA's regulation 72 as well as the assurance level of the identification device.	Included
Transmission of strong electronic identification performed by means of a mobile certificate	Included
Transmission of strong electronic identification performed by means of banking codes	Optional
Technical customer service for fault situations (24/7)	Included

6.1 Availability and capacity of the Telia Tunnistus service

Unless otherwise agreed, Telia commits itself to the following service level in the service provided:

- the service is available 24 hours a day seven days a week
- with the exception of servicing, service updates, maintenance, any disturbance and fault situations that cause a break in the identification service

7 Customer support

Telia Corporate Customer Service (020 693 693) assists in questions related to the service management, delivery and additional orders by phone and email from Mon to Fri, 8:00 am to 4:30 pm.

Telia's Technical Customer Service for Business Customers (020 693 693) provides support in technical issues related to the service and in fault situations, around the clock.

7.1 Communications on faults and incidents

Telia informs the customer by email on any problems, breaks or disturbances in the service. Insofar as possible, Telia also informs the customers about third-party-related problems, breaks and disturbances affecting the service provided by the customer.

Telia issues the notifications to its customers using Telia Mobile ID, other strong authentication devices provided by Telia Tunnistus, other partners in Finnish Trust Network (FTN), and to Traficom regarding availability, security, or major threats to personal ID usage accordin to Finnish law.

In connection with the order, the customer should give Telia an email address to which the fault and disturbance notifications will be sent.

7.2 Complaint

Telia processes any customer complaints centrally at one point. Complaints are replied to either in writing or orally and as soon as possible. In complaints related to invoicing, the applicable terms of delivery are applied.

8 Technical requirements for introduction

The customer's information systems must have the following technical features.

- Compatibility to send identification requests over the interface agreed between Telia and the customer (SAML, OpenID Connect, Tupas).
- Compatibility to receive transmitted information on identification events over the interface agreed between Telia and the customer (SAML, OpenID Connect, Tupas).
- A certificate granted by a certification service provider for certifying SAML identification requests and metadata, if an SAML interface is used for the transmission of information on identification events.
- Under FICORA's regulation 72, the following methods must be followed in the encryption of the interface, the exchange of keys and the encryption-related signature:
    - The DHE methods or the ECDHE methods using elliptic curves must be applied in the exchange of keys. The size of the finite field used in the calculations must be at least 2,048 bits in the DHE method and at least 224 bits in the ECDHE method.
    - When RSA is used for the electronic signature, the key length must be at least 2,048 bits. When the elliptic curve method ECDSA is used, the minimum size of the field below is 224 bits.
    - The encryption algorithm in symmetric encryption must be AES or Serpent. The key length must be at least 128 bits. The encryption mode must be CBC, GCM, XTS or CTR.
    - The cryptographic hash function must be SHA-2, SHA-3 or Whirlpool. SHA-2 refers to the functions SHA224, SHA256, SHA384 and SHA512.
- The TLS protocol version to be used is TLS 1.2 or later.

9 Deliverytime

Deliverytime is 2 – 4 weeks from ordering.

10 Data protection

The parties comply with the valid laws and decrees applicable to this service.

When providing the Telia Tunnistus service, Telia is entitled to disclose personal data to customers that are entitled under the applicable law to process the personal data in their own services.

Telia processes and saves personal data of customers according to Telia's data privacy policies, based on the authorization given by the individual authenticating with a service utilizing Telia Tunnistus.

As regards the personal data files that may result from the processing of personal data in the customer service, the customer acts as a controller as referred to in the Personal Data Act.

The customer is responsible for seeing to it that they are entitled to receiving and processing the identification event and the related personal data in their own services as accordance to Personal Data Act. If the information on the identification event includes the personal identity number of the person, this can be disclosed to the customer only if the customer has legal grounds for receiving and processing personal identity numbers.

The customer has its own description of file which describes the processing of personal data in the transaction service. The customer is obliged to make sure that the description of file is available to the person and that the customer fulfils their obligation to inform and other obligations towards the person using the service.

The customer informs Telia of any data protection violations and information security threats and disturbances in their own transaction service or the Telia Tunnistus service to enable Telia to anticipate situations and make any necessary contingency plans or corrective actions related to the Telia Tunnistus service. The customer undertakes to participate actively in troubleshooting.

11 Fault situations

A fault situation is considered to be an event where the normal transmission or processing of a message in the system is disturbed in such a manner that a certificate event does not proceed till the end.

Telia is entitled to invoice the customer for such troubleshooting costs that are generated by a problem or disturbance caused by the customer’s equipment, telecommunications connection or software.

12 Changes to the service description

Telia has the right to change this service description. If essential changes are made to the service description, the customer will be notified at least one month before the change enters into force.