ÅLANDSBANKEN

E-identification

Technical service description

E-identification - Technical service description

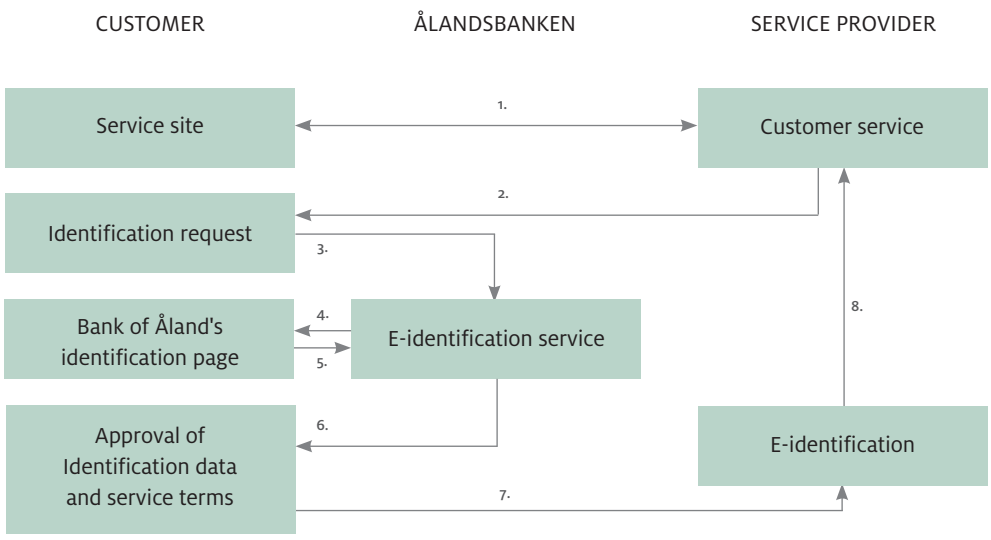
Introduction

The e-identification service, delivered by the Bank of Åland Plc through Crosskey Banking Solutions Ab Ltd, is a service where a service provider can use the bank's electronic identification solutions to reliably identify its customers on the Internet. Via the e-identification service the Bank of Åland identifies the customer on behalf of the service provider.

The e-identification service complies with the standards and guidelines given by The Federation of Finnish Financial Service[1] in the document: Tupas Service Description and Service Provider's Guidelines v.2.1.

This document describes the functionality and the needed data that is specific for the e-identification service for Bank of Åland. Thereto it describes a way for testing the service within the production environment.

Process description



1. The customer using the identification service contacts the service provider's page. The data connection must be SSL-encrypted when the customer enters data into the identification service. During stages 2-7 the connection is always SSL-encrypted.
2. The service provider sends the customer an identification request. The customer verifies the data in the request. The identification request page contains a cancel button and buttons that take the customer to service provider's page.
3. The customer clicks on the button which leads the customer to the Bank of Åland's identification service. An identification request which contains the required data on the service provider and the transaction is transmitted to the Bank of Åland. The bank confirms the integrity of the request and the authenticity of the data.
4. If the service provider's identification request is valid, the bank sends the customer an identification request. If the bank notices errors in the request the customer receives an error message.

1 www.fkl.fi

5. The customer is identified using Bank of Åland's identification service. The bank returns an error message to the customer if the identification fails.
6. After a successful identification Bank of Åland forms a return message and sends the message to the customer's browser. The bank's identification service activates the customer's *accept* and *cancel* buttons.
7. The customer verifies the identification data and accepts its transmission to the service provider. The customer can use the *cancel* button to reject the identification and return to the service provider's service.
8. The service provider verifies the integrity and uniqueness of the return message. The service provider attaches the identification to the customer's service transaction, and stores it for as long as the other service information. The customer's identification data may not be used for other purposes.

Functionality and data

Although the e-identification service follows given standards, some functionality and data is system specific. Below we describe that functionality and data.

Production link:

https://online.alandsbanken.fi/ebank/auth/initLogin.do

The Bank of Åland Identification button can be copied from:

https://online.alandsbanken.fi//images/betalknapp/betalknapp.gif

System specific data

Certificate request	Response message
A01Y_VERS = 0002	B02K_VERS = 0002
A01Y_LANGCODE = FI or SV	B02K_KEYVERS = 0001
A01Y_IDTYPE = 01, 02 & 03	B02K_ALG = 03
A01Y_KEYVERS = 0001	B02K_CUSTTYPE = "see Identifiers below"
A01Y_ALG = 03	

The Bank of Åland's e-identification uses a 03 = SHA256 algorithm. The algorithm is described in the guidelines given by The Federation of Finnish Financial Service[2] in the document: Tupas Identification Service for service providers v.2.3.

Note! When SHA256 is used the security code needs to be converted from hexadecimal to string before it is used in the calculation.

2 www.fkl.fi

How to calculate MAC-code using SHA-256 keys

To be able to calculate the mac code a unique key is needed. The key is delivered to the service provider in two parts:

PART 1: 466B6D35783857734B7541436C795330

PART 2: 307A4F4A7134326368373837383566435933

The first thing the service provider needs to do is to unite the keys (key1 + key2).

466B6D35783857734B7541436C795330307A4F4A7134326368373837383566435933

The service provider needs to convert the key from hexadecimal format to string format before using it in the calculation. This is the value to use in the mac code calculation.

The value presented below is the product of a hex to string conversion on the example key presented above:

Fkm5x8WsKuAClyS00zOJq42ch785fCY3

Example calculation including the key value in string format:

A01Y_ACTION_ID&A01Y_VERS&A01Y_RCVID&A01Y_LANGCODE&A01Y_STAMP&A01Y_IDTYPE&A01Y_RETLINK&A01Y_CANLINK&A01Y_REJLINK&A01Y_KEYVERS&A01Y_ALG&Fkm5x8WsKuAClyS00zOJq42ch785fCY3&

Identifiers

There are three types of identifiers described in the Tupas V22, 6.2.2007; 01 Encrypted basic identifier, 02 Basic plain-text identifier and 03 Truncated plain-text identifier.

All three types of identifiers are available for use in the service, which chosen depends on agreement with customer. The type of identifier administrated for a customer determines which response the customer will receive from the e-identification service. See detailed description below.

Requested identifier	Response
(A01Y_IDTYPE)	(B02K_CUSTTYPE)
01 Encrypted basic identifier	05 encrypted personal identity number
	06 encrypted Business ID
	09 encrypted test customer
02 Basic plain-text identifier	01 personal identity number in plain text
	03 Business ID in plain text
	08 test customer
03 Truncated plain-text identifier	02 last four characters of personal ID number in plain text
	03 Business ID in plain text
	08 test customer last four characters of personal ID number in plain text

For example: If provider requests 03 Truncated plain-text identifier they will receive B02K_CUSTTYPE = 02 and the last 4 characters in plain text (B02K_CUSTID) when a private customer uses the service.

A customer can use several types of identifiers at the same time. The identifiers are connected to specific customer ids and a customer can use several ids with different identifiers connected in the service.

Testing

To make it possible to test the e-identification service in production environment there is a test provider and a test customer implemented in the system. It is possible to test with test customer against test provider.
It is not possible to test with real customer against test provider or test customer against real provider.

The test provider can use all types of valid identifiers, 01, 02 & 03. Therefore it can be used for testing by all types of service providers regardless of preferred identifier.

The test customer uses personal id, not business id. It has static username, password and pin.

Test Provider	
A01Y_RCVID:	AABTUPASID
AAB_MAC_PWD:	PAPAGAJA

Test Customer	
User id (Användar-ID/ Käyttäjätunnus):	12345678
Password (Lösenord/ Salasana):	12345
PIN (Ange kod/ Anna tunnusluku):	Any number containing 4 figures