PRECISION OF DANSKE BANK IDENTIFICATION SERVICE

Valid as from 31.12.2017

1. SERVICE DESCRIPTION

Danske Bank Identification Service allows service providers to reliably identify private customers and corporations that have Danske Bank service key agreements.

Danske Bank's technical solution is based on the TUPAS Identification Service to Service Providers standard created by the FFI (Federation of Finnish Financial Services). With Danske Bank Identification Service, the service provider can be sure that the customer is reliably identified.

Danske Bank Identification service allows service providers and customers to make binding agreements on the Web. The agreements can be based on invoicing because the customer's identity has been verified and the order has been signed and dated.

2. AGREEMENT

The service provider must make an agreement with Danske Bank on the features and use of the service. When the agreement has been made, Danske Bank will give the service provider a customer code and an encrypted key to be used in the service.

3. INFORMATION AND SUPPORT

- Your own branch office during opening hours
- Customer support, tel.+358 100 2580 Mon – Fri 08-18

Corporate customers can send a message to Customer support through the Web bank in protected environment

4. DATA CONTAINED IN IDENTIFICATION SERVICE

4.1 Request for identification

Identification service URL: https://verkkopankki.danskebank.fi/SP/tupaha/TupahaApp

FORM DATA GROUP

Field	Name of data	Length	Data	Comment
1. Message type	A01Y_ACTION_ID	3-4	701	Standard, "701"
2. Version	A01Y_VERS	4	0003	
3. Service provider	A01Y_RCVID	12		Customer ID
4. Service language	A01Y_LANGCODE	2	FI SV EN	Finnish Swedish English
5. Request identifier	A01Y_STAMP	20	yyyymmddhhmmssxxxxxx	Data length must be 20 digits

6. Identifier type	A01Y_IDTYPE	2	01 02 03 11 12 13 21 22 31 32 33 41 42 51 52	Encrypted basic identifier Plain text basic identifier Plain truncated identifier Encrypted social security number Plain text social security number Truncated social security number Encrypted business ID Plain business ID Encrypted social security number or business ID code Plain social security number or business ID code Truncated security number or business ID code Encrypted social security number of corporate user and business ID code Plain social security number of corporate user and business ID code Encrypted social security number and business ID code or encrypted social security number Plain social security number and business ID code or plain social security number
7. Return address	A01Y_RETLINK	199		https address OK return address for the certificate
8. Cancel adress	A01Y_CANLINK	199		https address Return address in the event of cancellation
9. Rejected address	A01Y_REJLINK	199		https address Return address in error situations
10. Key version	A01Y_KEYVERS	4	0001	Key's version data
11. Algorithm	A01Y_ALG	2	03	SHA-256
12. Control field	A01Y_MAC	64		64 digit MAC; message authentication code of the request

4.2 Explanation of fields in identification service:

Field 1: Message type: standard in identification service is 701.

Field 2: Version number of identification request message in Danske Bank is 0003.

Field 3: Service provider number or customer ID number, 12 digit long.

Field 4: Service language code. Danske Bank's identification service is opened in this language.

Field 5: The service provicer's individual code for the request. It can be any series of 20 numbers. The number series can be e.g. a reference/customer number or combination of date, time, consecutive identifiers and reference. Please note: the field must be exactly 20 digits long.

Field 6: An agreement should be made with Danske Bank regarding the requested identification to be sent to service provider. The types of identification in use in Danske Bank are:

01=Encrypted identifier
02= Plain text identifier
03= Plain truncated identifier

11= Encrypted social security number
12= Plain text social security number
13= Truncated social security number

21= Encrypted business ID
22= Plain business ID

31= Encrypted social security number or business ID
32= Plain social security number or business ID
33= Truncated security number or business ID

41= Encrypted social security number of corporate user and business ID
42= Plain social security number of corporate user and business ID

51= Encrypted social security number and business ID or encrypted social security number
52= Plain social security number and business ID or plain social security number

Field 7: The address of the service provider's return page where the service continues to after successful identification. The address must start with https; it is a SSL protection page

Field 8: The continuation address in the event that the customer cancels the transmission of the certificate. The service address must start with https; it is a SSL protection page

Field 9: The continuation address if a technical error occurs during the identification transation. The return address must start with https; it is a SSL protection page

Field 10: The version of an encrypted key used by Danske Bank is e.g. 0001. The key will be changed at regular intervals for safety reasons and then the key version will change too

Field 11: Type code of the algorithm used in MAC calculation is 03 = SHA-256

Field 12: MAC-control. 64 digit calculated control

4.3 Return message

Field	Data name	Length	Data	Comment
1. Version	B02K_VERS	4	0003	0003
2.Certificate identification	B02K_TIMESTMP	23	800yyyymmddhhmmssxxxxx	
3. Certificate number	B02K_IDNBR	10		Identifier number given by the bank
4. Request identifier	B02K_STAMP	20		Request data field 5 (A01Y_STAMP)
5. Customer	B02K_CUSTNAME	-40	Name of the identified person or company from the Bank's database	
6. Key version	B02K_KEYVERS	4	0001	Version of the key. Version of the key will be change when secret key is renewed.
7. Algorithm	B02K_ALG	2	03	SHA-256
8. Identifier	B02K_CUSTID	12		Encrypted/plain text social security number or company code.
9. Identifier type	B02K_CUSTTYPE	2	01 02 03 05 06 08 09 10 11 12	Plain text social security number Plain text control of social security number Plain text business ID Encrypted social security number Encrypted business ID Plain text business ID and plain text social security number of corporate user Encrypted business ID and encrypted social security number of corporate user Response message 10, 11 and 12 sent to "rejected" URL (REJLINK). Request data of customer not found Social security number of customer not found Business ID code not found
10. User ID	B02K_USERID	40		Encrypted identifier or social security number of corporate user
11. User name	B02K_USERNAME	-40		Corporate customer's name
12.Control field	B02K_MAC	64		64 digit security check of response

Field 1: Version number of identifier in Danske Bank is 0003.

Field 2: Time stamp created by Danske Bank in which 800 is the Danske Bank number

Field 3: Individual identifier number given by Danske Bank

Field 4: Individual data field 5 of identification of request message

Field 5: Name of identified customer from Danske Bank's database

Field 6: The version of an encrypted key used by Danske Bank is e.g 0001. The key will be changed at regular intervals for safety reasons and then the key version will change too

Field 7: 03=SHA-256 calculation

Field 8: The contents of the field in Danske Bank can be encrypted/plain text/truncated last digits of social security number or encrypted/plain text business ID code.

Field 9: Danske Bank uses the following individual identifier data::

01 = Plain text social security number

02 = Plain text control of social security number

03 = Plain text business ID code

05 = Encrypted social security number.

06 = Encrypted business ID code.

08 = Plain text business ID code and plain text social security number of corporate user or any other identifier agreed on by the bank/service provider.

09 = Encrypted business ID code and encrypted social security or any other identifier agreed on by the bank/service provider.

If data in response message is 10, 11 or 12 the response message will be sent to "rejected" address (A01Y_REJLINK)

10= Request data of customer not found

11= Social security number of customer not found

12= Business ID code not found.

Field 10: Social security number of corporate user or encrypted code

Field 11: Name of corporate user

Field 12: 64 digit security check of response

5. DANSKEBANK IDENTIFICATION SERVICE BUTTON

The Danske Bank's logo is available at:
https://danskebank.fi/-/media/files/fi/logo-.-la=fi-fi.gif

Do not adjust the size of the logo.

6. TESTING THE SERVICE

The service provider can test the Identification Service in its business environment already prior to making an agreement by using the service provider's testing ID, MAC key and Mac Key version. The test takes place in a business-like environment, in which all the same safety requirements are valid as in the actual business environment.

The testing can be done by creating the identification request on one's own or by filling in the information on the form available at http://business.danskebank.fi/businesssbfi/IdentificationServiceProdToCustomers.html in which case the application software creates the identification request.

When making the test you must use your own bank identifiers. When you use the test service provider, no fees will be charged.

Test ID and MAC for Service Providers

Service Provider ID: 000000000000

Service Provider MAC: pAwfvWTD7g9etWGNTVR5zCj5EhHt5yuHdLrxQH2BD5gZxk7xBUrfqubtYv8vZvs4

Mac key version (A01Y_KEYVERS): 0001

Identifier type: 52

Fill all fields in the testform. Please note: Request identifier (AY01_STAMP) must be 20 digits long, e.g. 12345678901234567890. The web addresses used for testing must start with https //.

The return message includes the following information:

Personal customer:

- Name: TESTI Å-ÄÖ
- Social security number: 141072-933S

Corporate customer:

- YRITYS OY
- Business ID: 0000000-0