

TERMS AND CONDITIONS FOR IDENTIFICATION SERVICE

Valid 31.12.2017

1. Parties

This Agreement is made between Danske Bank A/S, Finland Branch (hereinafter “the Bank”) and the service provider (hereinafter “Service Provider”) that uses Danske Bank’s Identification Service (hereinafter “Identification Service”) for its Internet service (hereinafter “Portal”). Based on this Agreement the Service Provider can implement the Identification Service in which Danske Bank in a reliable way identifies the person (hereinafter “Customer”) who makes business transactions in the Portal. Customer refers to a natural person or a user that a company or a corporation has appointed user (hereinafter “Legal Entity”) and who, based on an Agreement between the Legal Entity and the Bank, is authorized to represent the company in the Bank’s Identification Service. For Identification the Customer, based on his/her Agreement with the Bank, has access to the Bank’s Service Keys (hereinafter “Service Key”).

2. Identification Service and Usage Requirements

Within the Bank’s Identification Service, the Bank,

- Acting for the Service Provider, certifies the Customer’s identity. In the Identification Service between companies, the Bank certifies the Service Key in the possession of the Legal Entity. Acting for the Customer, certifies the Service Provider using the Identification Service and to whom the Bank has delivered the Service Key and a secret key (hereinafter “Service Provider Password”).
- In the Identification Service the Service Key is a means for electronic identification and signing provided that the Customer and the Service Provider have made an Agreement regarding this legal implication in the Portal or otherwise. Before the Identification Service is taken into use, the Bank and the Service Provider agree on the characteristics of the service Danske Bank is providing, which in addition to the Customer’s full name in plain text comprises transmission of the Customer’s social security number in encrypted format.
- transmission of the last four digits of the Customer’s social security number in plain text; or transmission of the Customer’s entire social security number in plain text.

Identification Service, which transmits the social security number in plain text, is intended for Service Providers legally required to process social security numbers in their own operations, e.g. those required to give the reports stated in the Act on Detecting and Preventing Money Laundering and Terrorist Financing (503/2008). In intra-company Identification Service, the Bank supplies a service key in encrypted or plain text format identifying the Legal Entity. Information identifying the user and the Legal Entity is only proof of his/her empowered right of position. Based on it, no presumption can be made that the user is authorized in the Trade Register or a corresponding Official Register to represent the company or corporation. The Service provider’s responsibility is to check the user’s right to represent the Legal Entity. Furthermore, an administrative service on user rights can be connected to the Identification Service. This shall be agreed separately.

3. Functional Description of the Identification Service

The Customer logs via a link from the Service Provider’s Portal onto the Bank’s Identification Service which is located inside the outermost firewalls of the Bank’s information systems (hereinafter “Control Sphere”). Using the Service Provider Password, the Bank identifies the Service Provider from whose Portal the Customer has logged onto the Bank’s Identification Service.

The Bank identifies the Customer using the Service Key that the Bank has accepted, and sends the Customer’s (and, for a corporation, its Legal Entity’s) Service Key to the Customer for checking and approval. The Customer checks the data and approves or rejects it. When the Customer approves the data and at the same time accepts the transmission of his or her data from the Bank to the Service Provider, the Bank sends the Service Provider the data confirmed by the Customer. The Service Provider is liable to comply with the instructions provided by the Bank for the Identification Service. The Identification Service is based on the standard for TUPAS Identification Service Description, confirmed by the Finnish Bankers’ Association, which is available for viewing at Danske Bank’s web-site.

4. The Bank's Responsibility

The Bank is responsible for identifying the Customer (and, for a corporation, its Legal Entity) through the Service Key approved by the Bank, the Service Provider through the Service Provider's password, and for sending the Service Provider the data approved by the Customer. The Bank is not a party of legal actions between the Customer/Legal Entity and the Service Provider.

The Bank is not liable for

- the solvency of the Customer/Legal Entity the Customer's authority of legal proceedings (age, bankruptcy, interest coverage), nor for the authority or title of the user appointed by the Legal Entity.

The Bank stores the Service Keys in its possession in such a way that it will not come to the cognizance of a third party. The Bank is responsible for taking the following measures within a reasonable time period:

- preventing the use of the Service Key in the Identification Service after the Customer has informed the Bank of the loss of the Customer's Service Key or that the Service Keys have come to the cognizance of a third party;
- preventing the use of the Service Key in the Identification Service between companies after the Legal Entity has informed the Bank of having terminated the Customer's right to use the Identification Service between companies.

The Bank is liable for ensuring that the Identification Service is available at all times, with the exception of interruptions due to service, maintenance or development of the service. The Bank is not liable for any circumstances outside the Bank's Control Sphere, such as the Portal of the Service Provider, the link to the Identification Service, a data connection provided by the Service Provider or a third party, business transactions between the Service Provider and the Customer, or Agreements or other legal transactions made by the Customer in the Portal.

5. The Service Provider's Responsibility

5.1. The Service Provider's Portal

The Service Provider is liable to ensure that the Identification Service can be used on the Service Provider's Portal and that the use of it complies with the stipulations in the Acts of the branches in question and the regulations of the Authorities regarding e.g. identification and outsourcing, which the Bank is not liable to investigate. The Service Provider decides in which context of the Portal the Identification Service is used. The keyboard key for the Identification Service shall, however,

be within the Control Sphere of the Service Provider in the Service Provider's own Portal and it/a link to it must not be linked to e-mail.

The Service Provider is responsible for

- the definition, planning, implementation and maintenance of the Portal, the usability, data protection and data security of the Portal, the qualities, propriety and legality of the Portal, such as possible limitations in age, citizenship, branch or authorization of the Portal as well as the development of checks and controls in connection with the use of the Identification Service in the Portal.
- The Service Provider is responsible for the view ability and usability for the Customer of the link from the Portal to the Identification Service in the Portal so that the Customer can move to the Identification Service via the link; the protection and encryption of the data connection outside the Bank's Control Sphere in the manner required by the Bank; and the Service Provider's Web server software supporting SSL encryption.

5.2. Usage and Handling of Identification Data

The Service Provider is liable to reliably handle and store the information received from the use of the Identification Service. The Service Provider shall not handle the information received, such as knowledge of the fact that the Customer is a Bank customer, for any other purpose than in connection with the one specific Portal transaction, legal relationship and legal transaction for which the Identification Service was used originally.

The Service Key transmitted through the Identification Service can be used only once. The Service Provider is not permitted to create, using the Identification Service, own Service Keys based on those of the Bank's Identification Service, unless expressly agreed otherwise.

If the Service Provider uses an Identification Service which transmits a social security number or its last digits in plain text, the Service Provider must have a valid legal right to manage the Customer's social security number.

The Service Provider is liable to store the password of the Service Provider carefully.

The Service Provider can use the Identification Service for electronic signatures, provided that the Service Provider agrees with the Customer in the Portal on the legal consequences of the use of its Service Key.

When necessary, the Service Provider is responsible for acquiring, in connection with the use of the Identification Service or otherwise, the Customer's Agreement, based on which the Bank is allowed to transmit Customer data to the Service Provider as legal proof of a single Portal Transaction which the Bank has stored in connection with the transmission of Service Keys.

If the Service Provider learns that another person has used a Service Key than the Customer for whom it was created and to whom it was transmitted by the Bank, the Service Provider is liable to notify the Bank hereof without delay.

5.3. Charges and Fees

The Service Provider is liable for the payment to the Bank of any charges and fees resulting from the implementation and use of the Identification Service in accordance with the Bank's Service Tariff or a separate agreement. If the Service Provider asks the Bank for additional information about the Customer for reports to the Authorities or as legal proof, the Bank charges the hourly fee stated in the Service Tariff for this investigation.

5.4. Duty of Disclosure

The Service Provider is responsible for the accuracy of the information that it has provided or transmitted to the Bank. The Service Provider is liable to notify the Bank immediately of any changes in the Service Provider's identification, contact, contact person or in other information.

6. Immaterial Rights

By way of this Agreement the parties do not to any degree transfer rights to the other party for brands, trademarks, brand names or other immaterial rights, which must not be used, surrendered or otherwise utilized, for instance in marketing, unless agreed otherwise. However, the Service Provider is entitled to use the Bank logo in connection with the Identification Service during the period of validity of this Agreement, and in accordance with instructions given by the Bank.

7. Mutual Responsibilities of the Parties

The parties are responsible for the hardware, software, software and data security updates, systems and data connections within their Control Sphere, their security, functionality and development and any costs related to their maintenance, service and updates, usage and development. The parties are responsible for their own data communication costs. Neither party shall have the right to claim damages from the other party for indirect

loss. An indirect loss is, for example, loss of profits and income, interest loss, unrealized revenue, and damage that is due to reduction or interruption of business, an agreement between the Customer/Legal Entity and a third party, or a cancellation thereof, or of any other claim by a third party to the Customer/Legal Entity.

8. Amendments to this Agreement

The Bank has the right to amend the Terms and Conditions of this Agreement without notifying the Service Provider in advance, by publishing the amendment on the Bank's Web site www.danskebank.fi/varmennepalvelu, unless caused otherwise by the next paragraph. The amendment will become valid when it has been published on the Bank's Web site.

If an amendment to these Terms and Conditions, which is not due to a change in law or an official ruling, and which is made on the initiative of the Bank, substantially increases the liabilities of the Service Provider or decreases its rights, the Bank will notify the Service Provider in advance of the amendment. The amendment will become valid at the time notified by the Bank, however, not earlier than one (1) month after the Bank has notified the Service Provider.

9. Amendments to User Instructions, Hardware, Software and Systems

The Bank is entitled to

- make amendments to the layout and User Instructions of the Identification Service;
- and make modifications to the Identification Service and to the Web addresses, hardware, software and systems related to it, required for the maintenance and development of the service;
- without prior notice to the Service Provider.

10. Limitation or Discontinuation of Service

The parties have the right to limit the functionality of the Identification Service during necessary maintenance, repair or other equivalent measures, or due to data security reasons. The parties shall make an effort to notify the other party and the Customers in advance of any such measures known to them.

A party is entitled to discontinue the use of the Identification Service, if the activities, hardware, software, systems or data connections of the other party, the Customer/Legal Entity representing the user, or of a third party damage, hamper or otherwise endanger the functionality or security of the Identification Service, or change the activities of the other party.

11. Charges and Fees

The Bank is entitled to charge the Service Provider with the charges and fees related to the Identification Service as stated in the valid Service Tariff, unless explicitly agreed otherwise. The Service Tariff is available for viewing at Bank offices and on the Bank's Web site www.danskebank.fi. The Charges and Fees are inclusive of VAT according to the valid tax rate. The Service charges will be debited the Service Provider's account for each calendar month in arrears by the 20th day of the month. The Service Provider is responsible for keeping sufficient funds for this on its account.

The Bank is entitled to

- change existing Charges and Fees without notifying the Service Provider hereof in advance by publishing the change on the Bank's Web site www.danskebank.fi. The change shall become valid when it has been published;
- adopt a new charge or fee category by notifying the Service Provider hereof in advance. The change shall become valid at the time notified by the Bank, however, not earlier than one (1) month after the Bank has notified the Service Provider.

12. Period of Validity, Termination and Cancellation of the Agreement

The Agreement is valid until further notice.

The parties are entitled to terminate this Agreement with one (1) month's notice by notifying the other party thereof in writing, unless agreed otherwise.

The Bank is entitled to prevent the use of the Identification Service and cancel this Agreement with immediate effect if

- the Service Provider breaches the Terms and Conditions of this Agreement or the User Instructions of the Identification Service;
- the activity of the Service Provider has changed due to legislation, actions or decisions by authorities, or otherwise in a way that can weaken the Bank's reputation or credibility on the market.

13. Force Majeure

The parties are not responsible for any damage due to Force Majeure such as failure in data processing, data transfer, other electronic communications or supply of electricity such as disruptions in electricity, cable or data communication, or other similar reason which causes unreasonable difficulties to the other party's op-

erations. The reason mentioned above entitles the parties to discontinue the use of the Identification Service during the Force Majeure without consequences.

14. Confidentiality

The data transmitted by the Bank through the Identification Service is to be kept absolutely confidential under bank secrecy regulations. The Service Provider commits to adhering to the bank secrecy regulations and to keep confidential the data concerning the Customer/ Legal Entity received in connection with the usage of the Identification Service.

The parties undertake not to disclose any of each other's business and trade secrets, such as information on financial standing and service specifications, which may come to their knowledge in connection with the operations under this Agreement. Further-more, the financial terms of co-operation under this Agreement constitute business secrets.

Confidentiality shall remain in effect also after termination of the Agreement.

15. Obligation to Negotiate, Applicable Law and Place of Jurisdiction

If circumstances following the conclusion of this Agreement change fundamentally due to changes in legislation, actions by the Authorities or other reasons beyond the control of the contracting parties, the parties agree to negotiate in order to amend the Agreement to reflect the changed circumstances.

The parties shall endeavour to settle any ambiguities and disputes arising from the Agreement primarily through negotiations between the parties. If no settlement by negotiation can be reached, any disputes arising from this Agreement shall be resolved in the Helsinki District Court.

Any disputes arising from this Agreement are governed by Finnish law.

This Agreement has been drawn up in two identical copies, one for each party.