STANDARD TERMS AND CONDITIONS OF THE SECURITY ELEMENTS AGREEMENT

Applicable at Danske Bank A/S Estonia branch, Danske Bank A/S Latvia branch and Danske Bank A/S Lithuania branch from 19 December 2018

1. GENERAL PROVISIONS

1.1. The Standard terms and conditions of the Security Elements Agreement regulate the issue and use of the Security Elements to identify the User performing the Operations via Electronic Channels.
1.2. The following definitions are used:
Agreement means the Security Elements agreement which contains the Special terms and conditions and the Standard terms and conditions. All amendments and annexes, if any, to the Agreement constitute an inseparable part of the Agreement. The General Conditions, the Standard terms and conditions of the Electronic Services agreement, the Standard terms and conditions for provision of payment services and the Price List apply to the Agreement to the extent they do not conflict with the Agreement.
Customer means natural or legal person holding an account and having concluded the Electronic Services agreement with the Bank.
Danske eBank means the internet banking service of the Bank which provides access to the Customer's account information, payments and other services of the Bank.
Danske mBank means the internet banking service of the Bank through which customers using a mobile device and the Bank's mobile application can obtain information and use the services provided by the Bank. Danske mBank is an integral part of Danske eBank.
Danske Telephone Bank means the Bank's service through which the Customer using a telephone can obtain information and use the services provided by the Bank.
Electronic Channels means Danske eBank, Danske mBank and Danske Telephone Bank, which enable the Customer to perform Operations and use the services offered by the Bank in the remote mode.
Electronic Services means the Bank's services provided to the Customer via the Electronic Channels.
Electronic Signature means an electronic signature/seal that is created by a qualified electronic signature creation device issued by a certification services provider meeting the requirements set by a competent institution, acceptable to the Bank.
General Conditions means the General terms and conditions of the Bank, which set out the general principles and the procedure for communicating with and serving customers as well as the general terms and conditions for conducting transactions between the Bank and the customers.
Operation means any transaction/order which the Bank allows the Customer to perform via the Electronic Channels or via a single Electronic Channel, including payment transactions, securities account transactions, provision of information about the operations carried out in the account and about the balance of funds, submission of the Customer's requests and notifications to the Bank, agreements related to the Bank's services, authentication via Danske eBank towards third parties, etc.
PIN Generator means the identification/authorisation device issued by the Bank, which generates unique password combinations by using a special algorithm.
Security Elements means the identification/authorisation measures acceptable to the Bank (e.g. User ID, PIN Generator, Electronic Signature, etc.) allowing identification of the User and confirmation of the Operations.
Other terms used in these Standard terms and conditions have the same meaning as set out in the General Conditions.

2. CONCLUSION OF THE AGREEMENT

2.1. The Agreement must be concluded at the Bank´s place of Service or via electronic channels acceptable to the Bank. If the Agreement is to be concluded at the Bank´s place of Service, each Party will be provided with a separate copy of the Agreement and all copies will have the same legal effect.
2.2. The Agreement will come into force after the Parties have agreed to its terms and conditions by signing the Agreement on the front page(s) (including details of the Parties, the Special terms and conditions of the Agreement and confirmations of the User).

3. RIGHTS AND OBLIGATIONS OF THE PARTIES

3.1. SECURITY ELEMENTS

3.1.1. The User performs Operations pursuant to the authorisation granted by the Customer under the Electronic Services agreement concluded between the Customer and the Bank. The Customer and the User may coincide or differ.
3.1.2. The User must use the Security Elements personally.
3.1.3. The Bank must identify the User by means of the Security Elements.
3.1.4. The User must confirm the Operations by means of the Security Elements or other methods accepted by the Bank (e.g. by clicking the button in Danske eBank etc.).
3.1.5. The Bank is entitled to determine which of the Security Elements must be used to confirm the Operations. The Security Elements acceptable to the Bank are published on the Bank's website and/or in the agreement regulating the relevant Operation and/or in the information provided at the time when the Operation is performed.
3.1.6. At the signing of the Agreement, the Bank will provide the User with the User ID, which must be used to log in to Danske eBank and Danske mBank.
3.1.7. At the User's request, the Bank may provide the User with the PIN Generator. Instructions on how to use the PIN Generator are available on the Bank's website.
3.1.8. The PIN Generator is protected by a PIN code. Having turned on the PIN Generator for the first time, the User must create a four-digit code that must be entered every time the PIN Generator is used. If the User enters a wrong code multiple times, the PIN Generator will be blocked. In order to unblock the PIN Generator, the User must visit the Bank's place of Service and present the PIN Generator.
3.1.9. The User may obtain the Electronic Signature from the certification services provider or mobile network operator, which provides a mobile Electronic Signature service.

3.2. SECURE USE OF THE SECURITY ELEMENTS AND ELECTRONIC SERVICES

3.2.1. Prior to starting to use Danske eBank or Danske mBank for the first time and every time the Bank requests so, the User must familiarise himself/herself with the advice on secure use of Danske eBank published on the Bank's website and must take all actions recommended therein.
3.2.2. The User must use Danske eBank on a computer with an Internet connection and a browser that enables log-in to Danske eBank (the browser version is checked during log-in, so if the version is outdated, the User may receive warning messages or logging in to Danske eBank may be banned). Danske mBank can be used in Android, iOS or other operating system acceptable to the Bank and installed on the User's mobile device.
3.2.3. The User must ensure that the hardware and software he/she uses will not damage, modify or otherwise disrupt the information and computer systems of the Bank and will not cause damage or harm to the Bank, the Bank's customers or third parties and that no other actions not authorised by the Bank are taken.
3.2.4. The User must carefully safeguard the Security Elements, ensuring the confidentiality of the Security Elements and keeping them safe from third parties.
3.2.5. The User must not store the Security Elements in a form recognisable to third parties or allow third parties to use them. The User has under no circumstances any right to transfer the Security Elements to any third party or provide any other access to the Security Elements to third parties, including the Customer, employees and representatives of the Customer and the Bank (except where the Bank's representative identifies the User of the Danske Telephone Bank service or when the User ID is specified in the relevant documents signed by the Bank and the User).
3.2.6. The User must immediately inform the Bank of the loss, theft and unauthorised or incorrect use of the Security Elements or if they have been disclosed to a third party or such a risk exists. As regards the Electronic Signature, the User must immediately notify the above to the relevant certification services provider who has the right to terminate the validity of the respective Electronic Signature service.
3.2.7. If the Bank receives notification in accordance with clause 3.2.6, the Bank will take all reasonable measures to stop the unauthorised use of the Security Elements. The Bank may decide to

restore the use of the Electronic Services by issuing new Security Elements to the User or resume the use of the existing Security Elements once the reasons for stopping the use of the Electronic Services no longer exist.
3.2.8. If any third party has obtained access to and/or has used the Security Elements as a result of a crime (theft, fraud, etc.), the User must notify the competent law enforcement authorities of the crime and cooperate with them and/or with the Bank for the purpose of exposing such crime.
3.2.9. If the User has not taken any action in Danske eBank and Danske mBank within the time limit set by the Bank, the User is required to log in again in order to perform new actions.
3.2.10. After finishing a session in Danske eBank or Danske mBank, the User must log off securely.
3.2.11. The Bank warns the User that the User may receive e-mails or calls from persons pretending to be representatives of the Bank or government officials and requesting the User to provide the data on the Security Elements. The User must keep the data of the Security Elements secret, not submit to the provocation and inform the Bank of such attempts immediately by calling the Bank or visiting the Bank's nearest place of Service.
3.2.12. When performing User identification in Danske Telephone Bank, the Bank must identify the User in accordance with the User's personal data and a code generated by the PIN Generator or mobile Electronic Signature creation device. The identification of the User in Danske Telephone Bank can be performed during the business hours of the Bank.
3.2.13. If the User refuses to perform the identification procedure in Danske Telephone Bank or performs it incorrectly, the identification of the User must be deemed to have failed and the Bank will be entitled to reject execution of the Operations initiated by the User.
3.2.14. The User must not use the Electronic Services for unintended purposes (including illegal activities or in a manner that may harm the Bank or a third party).
3.2.15. The User bears full liability for the use of the Security Elements as well as for non-performance or inappropriate performance of the Agreement.
3.2.16. The User must notify the Bank of any unauthorised Operations or errors in the execution of an Operation immediately after becoming aware of it.

4. PAYABLE FEES

4.1. The User must pay the fees deriving from the Agreement and/or charged by the Bank in accordance with the Price List.
4.2. The Bank is entitled to debit the Service fees from the User's accounts opened with the Bank or require the payment of the Service fees in cash.

5. LIABILITY OF THE PARTIES

5.1. The General Conditions and the Standard terms and conditions for provision of payment services regarding liability also apply to this Agreement.
5.2. The User is responsible to the Bank for the correctness of the instructions, notices and requests as well as the data contained therein, sent to the Bank while using the Electronic Services.
5.3. The User is responsible for the security of the device on which the User uses the Electronic Services and for any consequences arising from a failure to ensure appropriate protection of the User's device.
5.4. The User must not modify or repair the Electronic Services and the Bank's software and must not allow a third party to do so. The User is responsible for the secure use of hardware, software or other equipment and must update anti-virus programs, e-mail anti-spam programs and privacy protection programs. The User is liable for any loss arising from violation of the above provisions and, in such case, the Bank will be released from liability and the fulfilment of its obligations under the Agreement.
5.5. The Bank is not liable in cases where, due to failures or disruptions in electronic communications or telecommunications systems or other reasons beyond the control of the Bank, the User was unable to use the Electronic Services or the information transmitted to the Bank and/or the Customer was lost or distorted.

6. AMENDMENTS TO THE AGREEMENT

6.1. The Bank is entitled unilaterally to amend the Standard terms and conditions of the Agreement by notifying the User of any changes at least 2 (two) months or 60 (sixty) days (depending on which period is longer) prior to the entry into force of such amendments according to the procedure set out in the General Conditions.
6.2. If the User does not agree to the amendments, the User is entitled to terminate the Agreement by notifying the Bank thereof in writing or in another manner agreed in the Agreement before the respective amendments take effect and upon fulfilment of all the User's obligations arising from the Agreement. If the User does not exercise its right to terminate the Agreement, the User will be deemed to have accepted the amendment made and declared that the User has no subsequent claims against the Bank in respect of the amendments to the Agreement.

7. EXPIRY AND TERMINATION OF THE AGREEMENT

7.1. The Agreement is entered into for an indefinite period.
7.2. The Bank may terminate the Agreement ordinarily, irrespective of reason, by notifying the User at least 2 (two) months or 60 (sixty) days (depending on which period is longer) in advance in the manner set out in the General Conditions.
7.3. The Bank may stop the provision of the services immediately and terminate the Agreement if the User is using the Electronic Services in violation of the relevant agreements and/or terms and conditions stipulated by the Bank or intentionally performs unfair actions which damage or may damage the functioning of the Bank's information systems or in other cases set out in the General Conditions.
7.4. The User may terminate the Agreement at any time by notifying the Bank in the manner set out in the General Conditions and by performing in full all obligations under the Agreement. The Bank will terminate the Agreement immediately, but not later than within 5 (five) days after receiving the relevant request from the User.
7.5. The Agreement expires automatically if:
7.5.1. The usage of Security Elements is not required under any valid Service agreement; and
7.5.2. The User has not logged in to Danske eBank within the last 90 (ninety) days or has logged only for authentication purposes.

8. FINAL PROVISIONS

8.1. The Agreement concluded using electronic channels acceptable to the Bank as well as all the amendments thereto and/or any notices provided by any Party using electronic channels acceptable to the Bank will have the same legal effect as the agreements concluded at the Bank and/or notices handed over personally.
8.2. The User may not assign, transfer or otherwise dispose of any of its rights or obligations under the Agreement.
8.3. Any matters not covered by this Agreement are governed by the General Conditions.
8.4. All disputes arising out of the Agreement must be settled according to the General Conditions.
8.5. The Agreement is governed by and construed in accordance with the legislation applicable at the Place of Service.

9. SPECIAL CONDITIONS APPLICABLE TO THE PLACE OF SERVICE ALONE

9.1. As regards the Services in Estonia, the following special conditions apply:
9.1.1. These Standard terms and conditions of the security elements agreement also apply to the Customers that have concluded the Security Elements Agreement on or before March 31, 2018. In such case, any references to the Special terms and conditions in these Standard terms and conditions of the security elements agreement must be deemed to be a reference to the Security elements agreements that have been concluded on or before March 31, 2018.