

Article 1. Introductory Provisions

- 1.1 The below Terms and Conditions of the Issue and Use of a Personal and Company Certificate (hereinafter the "**Conditions**") represent the Product Terms and Conditions as foreseen by the General Business Terms and Conditions of the Bank (hereinafter the "**General Conditions**"). The Conditions form part of the Contract and the Client is obliged to familiarise himself/herself with them and comply with them.
- 1.2 Terms in these Conditions that begin with a capital letter have the meanings defined in Article 7 hereof.
- 1.3 By signing the Contract, the Client confirms that he/she is familiar with the contents of the Certification Policy and shall abide by its provisions.
- 1.4 The Bank issues a Personal Certificate and Company Certificate. The Personal Certificate and Company Certificate can only be used by the Client to whom they have been issued. Besides, the Company Certificate may be used by a natural person authorised by the Client who shall supply him/her with the Company Certificate.
- 1.5 The fee for the issue of a Certificate and other services relating to the Certificate's use is governed by the Tariff of Fees.

Article 2. Terms and Conditions of Issuing the Certificate

- 2.1 The Bank issues the Personal Certificate either in the form of a Personal Certificate stored in a data file or on a chip card, or in both forms. A Company Certificate may only be issued in the form of a Company Certificate stored in a data file.

Personal and Company Certificates stored in a data file

- 2.2 Information on the method of obtaining and creation of a Certificate stored in a data file is available on the Bank's website.
- 2.3 The Client shall apply for the issue of a Certificate at the Bank's point of sale that provides him/her with any of Banking Services or, if no Banking Service has yet been provided, at any point of sale of the Bank. After entering into the Contract, the Bank shall send to the Client without any unnecessary delay upon entering into the Contract a single-use password for the generation of a Private and Public Key and for the issue of the Certificate. The password shall be sent by SMS message to an agreed GSM mobile telephone number or, in case of a Company Certificate, by e-mail at an agreed electronic address of the Client. Using the single-use password, the Client shall take necessary steps in the Certification Guide in order to obtain the Certificate. While the Certificate is being generated, the Client is asked, among other things, to confirm the entry data and input a required password. As soon as the Certificate is generated, the Client shall save the Certificate, which contains the Public and Private keys. The single-use password shall remain effective for a period of 30 days after being sent to the Client. After the lapse of the aforesaid period, the Certificate may only be issued to the Client upon entering into a new Contract executed in the Client's Point of Sale.
- 2.4 One GSM mobile telephone number indicated in the Contract as that to which the Bank should send the single-use password and/or Authorisation SMS Messages can only be assigned to this purpose in one Contract and for one Client of the Bank.
- 2.5 Before generating the Private and Public Key and prior to the issue of the Certificate, the Client shall be obliged to check the accuracy of his/her identification data displayed and to verify that they are consistent with the data stated in the Contract.
- 2.6 The Bank shall not be held liable for any damage caused by the fact that the Client might have stated a wrong GSM mobile telephone number or electronic address to which the Bank should deliver the single-use password and/or Authorisation SMS Messages.
- 2.7 If the GSM mobile telephone to which the Bank should send the single-use password is lost or stolen or the electronic address is misused or blocked before the Client generated the Private and Public Key, the Client shall be obliged to notify the Bank without any unnecessary delay at the telephone number 800152152 and

agree upon an alternative method of delivery of a new single-use password. The Bank shall subsequently invalidate the old password.

Personal Certificate stored on a chip card

- 2.8 The Client shall apply for the issue of a Certificate at the Bank's point of sale that provides him/her with any of Banking Services or, if no Banking Service has yet been provided, at any point of sale of the Bank. Immediately after entering into the Contract, the Bank in cooperation with the Client shall generate a Private and Public Key and issue to the Client a Certificate stored on a chip card directly at the Client's Point of Sale, or the Bank shall send to the Client without any unnecessary delay upon entering into the Contract a single-use password for the generation of a Private and Public Key and for the issue of the Certificate, which the Client shall perform by himself/herself using the Certificate Guide. The single-use password shall remain in force for the period of 30 days after sending. The Bank shall also supply the Client with the chip card and an envelope containing the PIN and PUK.

Article 3. Validity and Effectiveness of the Certificate

- 3.1 A Personal Certificate stored in a data file, a Personal Certificate stored on a chip card, as well as a Company Certificate, shall be valid for 2 years. The term of validity of a specific Certificate is specified in the Certificate. The Client may use a valid and effective Certificate while utilising the Services, including renewing its validity in the Certification Guide, until the lapse of the validity of the Certificate.
- 3.2 The Bank shall issue a new Certificate to the Client based on his/her application submitted to the Bank during the term of validity of the existing Certificate under the existing Contract. The Client shall apply for the issue of a new Certificate using the Certification Guide. When an application for the issue of a new Certificate is dispatched, the Client and the Bank shall accordingly proceed in compliance with Article 2 hereof. The new Certificate issued to the Client shall have the same form and the same identification data as the previous Certificate. The Client shall be obliged to apply for the issue of a new Certificate as per this Article 3.2 if his/her e-mail address stated in the Certificate has changed. As of the moment of issue of the new Certificate the Client shall not be allowed to use the previous Certificate.
- 3.3 If the Client's identification data stated in the Contract (including the GSM mobile telephone number to which Authorisation SMS Messages are to be sent) should change, the Client shall inform the Bank of this fact without any unnecessary delay in writing and shall apply for the issue of a new Certificate. The Bank shall issue a new Certificate to the Client based on a new Contract.
- 3.4 Upon the lapse of the validity of the Certificate, the Client shall only be entitled to apply for the issue of a new Certificate based on a new Contract.

Article 4. Revocation, Suspension and Blocking of the Certificate

- 4.1 If the Certificate is revoked (cancelled), its validity and effectiveness shall also be terminated and the Certificate may no longer be used.
- 4.2 If the Certificate's effectiveness is suspended, the Certificate shall remain temporarily ineffective even during the term of its validity and the client may not use it when accessing Services until its effectiveness is renewed.
- 4.3 The Certificate may be revoked or suspended upon the request of the Client or, under the conditions specified below, by the Bank.
- 4.4 The Bank shall be entitled to revoke or suspend the Certificate, or demand that the Client apply for the issue of a new Certificate, in case of at least one of the following events:
 - the Certificate was issued on the basis of false, incomplete or misleading information;
 - the identification data which form part of the Certificate are no longer valid;
 - the Client is in breach of any obligation under the Contract;

- the GSM mobile telephone to which the Bank should send the single-use password and Authorisation SMS Messages was used in several Contracts and/or for several Clients;
 - the Bank has ceased to issue Certificates;
 - the Bank is required to do so by law;
 - security risks have risen or might rise, or measures related to the use of the Certificate have become more strict.
- 4.5 The Bank shall inform the Client of the revocation or suspension of the Certificate by the Bank via electronic mail, unless this contravenes the law.
- 4.6 The Client shall only be entitled to request revocation of the Certificate by submitting an application filled-in in person at the Client's Point of Sale. The Bank shall inform the Client of the revocation of the Certificate via electronic mail no later than on the following Business Day after receiving the Client's request for the revocation.
- 4.7 The Client may request the suspension of the Certificate at the telephone number 800152152, at any point of sale of the Bank, or in the Certification Guide application on the Bank's web site.
- 4.8 The Client shall be obliged to request that the Bank revoke the Certificate if he/she finds any discrepancy between the content of the Certificate and the data information/data in the Contract.
- 4.9 The Client may check at the Bank's web site whether the Certificate has been suspended.
- 4.10 The Client may get information regarding the current status (effectiveness and validity) of the Certificate in the Certification Guide and, if need be, make a double check by consulting the certificate revocation list CRL available at the Bank's web site.
- 4.11 If the Certificate has been suspended at the request of the Client, the Client may ask for its re-activation by submitting an application filled-in in person at the Client's Point of Sale. The Bank shall re-activate the Certificate no later than on the following Business Day after receiving the application.
- 4.12 For Certificates stored on a chip card, the chip card shall be blocked upon the third incorrect PIN entry. The Client may ask for the chip card to be unblocked at the Client's Point of Sale or can do it himself/herself using the software supplied by the Bank to the Client upon the issue of the chip card. To unblock the card either, the Client shall state the PUK code in both cases.

Article 5. Safety

- 5.1 The Client is fully responsible for the process of generating the Public and Private Keys, including filling-in the application for the issue of the relevant Certificate on the computer that he/she has used for this purpose. The Client is the sole user of the Certificate including the Private Key and is liable for its use.
- 5.2 A Private Key stored in a data file is protected by a password. A Private Key stored on a chip card is protected by a PIN.
- 5.3 The Client is obliged to protect his/her Private Key and password and, as the case may be, a PIN and PUK, to be used with the Private Key throughout the entire term of the validity of the Certificate, in particular from possible loss, disclosure to a third party, modification, or unauthorised use. The password or PIN and PUK to be used with the Private Key should not be stored in the same place or on the same media as the Private Key and may never be stored in a manner that would make it accessible to third parties. In particular, the Client must not leave an unsecured Private Key in the computer with a password entered and the Key activated, nor leave a chip card inserted in the chip card scanner unattended. The Holder must continuously make sure that the password, Private Key etc. have not been lost, stolen, misused or used without authorisation.
- 5.4 The Client to whom a Company Certificate has been issued shall ensure that all persons authorised to use it are familiar with the Contract and the Certification Policy, as well as any other documents regulating the use of the Certificate, and shall see to it that they abide by the provisions thereof.
- 5.5 The Client shall be obliged to inform the Bank without any unnecessary delay about a loss, theft or any threatened misuse of

the Private Key and related password and/or, as the case may be, PIN and PUK. The Client shall further be obliged to request suspension or revocation of the Certificate in case of its loss, attempted copying or any other misuse of the Private Key. The Bank shall consequently revoke or suspend the Certificate.

- 5.6 The Bank shall be entitled to suspend the Service temporarily for serious reasons, particularly those of a security nature. The Bank shall be further entitled to block access to the Service or suspend the Service in cases envisaged in the Insolvency Act¹.
- 5.7 Electronic communications networks (public telephone lines, mobile network lines, e-mail and fax) used for the communication between the Bank and the Client pursuant to these Conditions are beyond the Bank's direct control; the Bank is therefore not liable for any damage caused to the Client by their potential misuse. The relevant providers of electronic communications services are obliged to secure the protection of these networks and the confidentiality of messages sent via the networks, as envisaged particularly in Act No. 127/2005 Coll., on Electronic Communications, as amended.
- 5.8 The Client shall discharge his/her duty to inform the Bank as required by these Conditions, particularly under Article 5 hereof, at the Client's Point of Sale, by electronic message delivered at the address indicated in the relevant Product Terms and Conditions, or over the telephone at a number communicated by the Bank. Should the Client fail to fulfil the duty to inform the Bank within three Business Days from the day on which such duty has arisen without being prevented from doing so by particularly serious reasons, he/she shall be deemed to fail to notify the Bank without any unnecessary delay.
- 5.9 The Client shall be held liable for any damage suffered by the Bank as a result of the Client breaching his/her obligations set forth under this Article 5.
- 5.10 The Bank shall not be held liable for any unauthorised or erroneously performed payment transactions, for any damage suffered by the Client as a result of a breach of his/her obligations set forth under this Article 5, or for any loss or damage resulting from an incorrect authorisation or non-execution of an Order due to reasons caused by the Client or a payee.
- 5.11 The Bank shall not be held liable for cases where the Certificate cannot be used due to circumstances that are beyond the control of the Bank or its partners (power failure, interruption to the connection with the Bank via a public telephone/Internet network, strike, etc.). The Bank shall not be obliged to demonstrate to Clients who are not Qualified Clients as envisaged by the General Conditions that it has followed the procedure that makes it possible to verify that a payment order has been submitted, the relevant payment transaction has been authorised, correctly documented and entered in the books, and it has not been affected by technical problems or other flaws.

Article 6. Termination of the Contractual Relationship

- 6.1 The Contract shall expire/be terminated:
- a) by a notice of termination from the Client. The Client may terminate the Contract in writing without giving a reason. The termination shall be effective as of the first Business Day following the day the notice shall have been delivered to the Bank;
 - b) by a notice of termination from the Bank. The Bank may terminate the Contract in writing without giving a reason. The termination shall be effective as of the last day of the month following the month in which the notice shall have been delivered to the Client, except in cases where the Bank terminates a Contract with a Qualified Client, in which cases the Bank shall be entitled to terminate the Contract in accordance with the General Conditions;
 - c) as at the Conclusive Date;
 - d) upon the lapse of the validity of the Certificate.

¹ Act No. 182/2006 Coll., On Bankruptcy and Its Resolution (Insolvency Act), as amended.

- 6.2 The Bank's right to revoke the Contract in accordance with the General Conditions shall not be prejudiced.
- 6.3 Client shall not be allowed to use the Certificate following the termination of the Contract.

Article 7. Definition of Terms

- 7.1 Terms in these Conditions that begin with a capital letter have the following meanings:

"Authorisation SMS Message" shall be a message sent by the Bank to the Client at an agreed-upon GSM mobile telephone number operated by a Czech provider, by which the Client shall receive an SMS authorisation code. The SMS authorisation code shall be used for identifying the Client while using the *MojeBanka* direct banking service, whereby the verification is made by a Personal Certificate stored in a data file.

"Bank" shall mean Komerční banka, a.s., registered office at Prague 1, Na Příkopě 33/969, Postal Code: 114 07, IČ (Company ID): 45317054, entered in the Commercial Register kept by the Municipal Court in Prague, Section B, Insert 1360.

"Banking Services" shall mean any banking deals, services and products provided by the Bank based on its banking licence, including investment services provided by the Bank in its capacity of a brokerage house.

"Business Day" shall mean a day that does not fall on a Saturday, a Sunday, a public holiday or other holidays within the meaning of the applicable law, on which the Bank is open for the provision of Banking Services and on which other institutions that take part in the provision of Banking Services, or on which the provision of the Banking Services depends, are open and provide the relevant services.

"Certificate" shall mean the Personal Certificate or Company Certificate.

"Certification Guide" shall mean an application that supports and administers the Certificate. The Client may access the Certification guide on the Bank's website.

"Certification Policy" shall mean a document in which the Bank sets forth the rules and procedures for using the Certificate and its specification, which the Bank is entitled to modify. The Bank publishes the Certification Policy on its website. The Certification Policy is also available at Bank's points of sale. This document is not a Notice as envisaged by the General Conditions.

"Client" shall mean a natural person or legal person who has entered into the Contract with the Bank.

"Client – Consumer" shall mean a natural person who executes and performs the Contract for purposes not associated with his/her business or job activities, or a person requesting a provision of a Banking Service.

"Client's Point of Sale" shall mean the Bank's point of sale at which the Client has executed the Contract.

"Company Certificate" shall mean a Statutory Certificate issued by the Bank to a natural person (business) or a legal person, which also contains the Private Key.

"Contract" shall mean a contract under which the Bank undertakes to issue a Company Certificate or Personal Certificate to the Client.

"Direct Channel PB Service" is a direct banking service, which the Client may utilise based on the Contract for the Provision of Direct Banking.

"Notices" shall mean communications in which further conditions and technical features of providing the Banking Services are specified in accordance with the General Conditions or relevant Product Terms and Conditions. The following document, without limitation to it, is not a Notice: Certification Policy.

"Payment Services" shall be Banking Services falling within the scope of payment services as envisaged by the Payments Act (e.g., money transfers, issuing of payment instruments and cash depositing/withdrawing).

"Personal Certificate" shall mean a Statutory Certificate issued by the Bank to a Client – Consumer, which also contains the Private Key.

"PIN" shall be a four-digit personal identification number used to verify the Client's authorisation to handle the chip card.

"Private Key" shall mean data used for creating the Client's electronic signature.

"Product Terms and Conditions" shall mean Bank's terms and conditions regulating the provision of separate Banking Services.

"Public Key" shall mean data used for verifying the Client's electronic signature.

"PUK" shall be an eight-digit code used to unblock a chip card.

"Tariff of Fees" shall mean a list of all charges, other fees and payments for the Banking Services and operations associated with the Banking Services.

"Service" shall mean any Banking Service provided to the Client, for which the Client uses the Certificate.

"Statutory Certificate" shall mean a data message issued by the Bank to the Client under the Contract. The message links data for verifying the Client's electronic signature with the signing person and makes it possible to verify Client's identity when using the Services in accordance with Act No. 227/2000 Coll., On the Electronic Signature, as amended. The Statutory Certificate contains the Public Key and Client's identification data.

- 7.2 Any reference to Bank's web sites shall mean a reference to www.mojebanka.cz or other web addresses the Bank currently uses or shall use in association with providing the Banking Services.

Article 8. Final Provisions

- 8.1 The Bank shall be entitled to amend these Conditions on an ongoing basis in the manner set forth in the General Conditions.
- 8.2 These Conditions shall repeal and replace the Terms and Conditions of Komerční banka, a.s. governing the issue and use of personal and company certificates of 23 October 2010.
- 8.3 These Conditions shall come into effect as of 25 July 2011.