Terms and Conditions of the Issue and Use of a Personal Certificate

Article 1. Article 1. Introductory Provisions

1.1 The below Terms and Conditions of the Issue and Use of a Personal Certificate (hereinafter the "**Conditions**") represent the Product Terms and Conditions as foreseen by the General Terms and Conditions of the Bank (hereinafter the "**General Conditions**"). These Conditions form part of the Contract and the Client is obliged to familiarise himself/herself/itself with them and abide by them.

1.2 Terms in these Conditions that begin with capital letters shall have the meaning 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 the Personal Certificate. The Personal Certificate may only be used by the Client to whom it has been issued.

1.5 The fee for the issue of the Certificate and other services relating to use of the Certificate shall be governed by the Tariff of Fees.

1.6 The Client shall be entitled to use the Personal Certificate in relation to the Bank or, as the case may be, also to the third parties listed on the Bank's website. The rights and obligations of the Client and third party arising from the use of the Personal Certificate shall be subject to a separate legal relationship between the third party and the Client. The Bank shall not be held liable for any damage incurred by the Client while using the Personal Certificate in relation to third parties.

Article 2. Terms and Conditions of Issuing the Certificate

2.1 The Bank issues the Personal Certificate in the form of a Personal Certificate stored on a smart card (chip card).

2.2 The Client shall apply for the issue of the Certificate at the Client's Point of Sale. a one-time 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. Using the one-time password, the Client shall take necessary steps in the Certification Wizard 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 enter the PIN. As soon as the Certificate is generated, the Client shall save the Certificate, which contains the Public and Private Keys. The one-time 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. The Bank shall send to the Client a smart card, envelope with a PIN and PUK.

2.3 The GSM mobile telephone number agreed upon in the Contract for sending the one-time password may only be used for a single Contract and a single Client of the Bank.

2.4 Before generating the Private and Public key and prior to the issue of the Certificate, the Client is obliged to check the accuracy of his/her/its identification data displayed and to verify that they are consistent with the data stated in the Contract.

2.5 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 to which the Bank should deliver the one-off password.

2.6 If the mobile telephone to which the Bank should send the one-time password is lost or stolen before the Client generates the Private and Public Key, the Client shall be obliged to notify the Bank without any unnecessary delay at the telephone number 800 118 100 and agree upon an alternative method of delivery of a new one-time password. The Bank shall invalidate block the old password.

Article 3. Validity and Effectiveness of the Certificate

3.1 The Personal Certificate stored on a smart card 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 Wizard, until the lapse of the validity of the Certificate.

3.2 The Bank shall issue a new Certificate to the Client under the existing Contract based on Client's application submitted to the Bank during the term of validity of the existing Certificate. The Client shall apply for the issue of a new Certificate using the Certification Wizard. 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. The new Certificate issued to the Client shall have the same form and the same identification data as the previous one. The Client shall be obliged to apply for the issue of a new Certificate as per this Article 3.2 if his/her/its 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 should, the Client shall be obliged to inform the Bank of this fact in writing without any unnecessary delay and, at the same time, execute an amendment to the Contract, or apply for the issue of a new Certificate. The Bank shall issue the Client with a new Certificate on the basis of a new Contract.

3.4 Once the validity period of a Certificate has expired, the Client shall only be entitled to apply for the issue of a new Certificate based on a new Contract.

Article 4. Blocking of the Certificate

4.1 If the Certificate is blocked, its validity and effectiveness shall also be terminated and the Certificate may no longer be used.

4.2 The Certificate may be blocked upon Client's request or, under the conditions specified below, by the Bank.

4.3 The Bank shall be entitled to block the Certificate, or demand that the Client apply for the issue of a new Certificate, if at least one of the following events occurs:

- the Certificate was issued on the basis of false, incomplete or misleading information,
- the identification data that form part of the Certificate are no longer valid,
- the Client is in breach of any obligation under the Contract,
- the Bank has ceased to issue Certificates,
- the Bank is required to do so by law,
- security risks have arisen or might arise, or measures relating to the use of the Certificate have become stricter.

4.4 The Client shall only be entitled to request the blocking of the Certificate at the telephone number 0800 118 100, at the Client's Point of Sale or on the Bank's website using the Certification Wizard application.

4.5 The Client shall be obliged to request that the Bank block the Certificate if he/she/it finds any discrepancy between the content of the Certificate and the details contained in the Contract.

4.6 The Client may check on the Bank's website whether the Certificate has been blocked.

4.7 The Client may get information regarding the current status of effectiveness and validity of the Certificate in the Certification Wizard or, as the case may be, check it by consulting the certificate blocking list (CBL) available at the Bank's website.

4.8 For Certificates stored on a smart card, the smart card shall be blocked upon the third incorrect PIN entry. The Client may ask for the smart card to be unblocked at the Client's Point of Sale or can do this himself/herself using the *Cryptoplus KB* application In both cases, the PUK code must be stated to unblock the smart card.

Article 5. Security

5.1 The Client is responsible for the process of generating the Public Key and Private Key, including filling-in the request for the issue of the relevant Certificate on the PC which 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 on a smart card is protected by a PIN.

5.3 The Client is obliged to protect his/her/its Private Key, PIN and PUK intended to be used with the Private Key throughout the entire period of validity of the Certificate, in particular against loss, disclosure to a third party, modification or unauthorised use. The PIN and PUK intended to be used with the Private Key must not be stored in the same place or on the same media as the Private Key and must never be stored in such a manner that would make them accessible to third parties. In particular, the Client must not leave an unsecured Private Key in the computer with the PIN entered and the Key activated, or leave a smart card inserted in the smart card reader unattended. The holder must continuously make sure that the Private Key, PIN and PUK have not been lost, stolen, misused or used without authorisation.

5.4 The Client shall be obliged to inform the Bank without any unnecessary delay of a loss, theft or any risk whatsoever of misuse of the Private Key, PIN or PUK intended to be used with the Private Key. The Client shall further be obliged, without any unnecessary delay, to request that the Certificate be blocked in the event of a loss of the Private Key or suspicion that it has been copied or misused in another manner.

5.5 The Bank shall be entitled to suspend the Service temporarily for serious reasons, particularly those of a security nature. In cases envisaged in the Act on Bankruptcy and Restructuring,[1] the Bank shall be entitled to block access to the Service or to suspend the provision of the Service.

5.6 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, envisaged particularly in Act No. 610/2003 Coll. on Electronic Communications, as amended.

5.7 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 telephone number communicated by the Bank. Should the Client fail to fulfil the duty to inform the Bank within three Business Days of the day on which such duty has arisen without being prevented from doing so by particularly serious reasons, he/she shall be deemed to have failed to notify the Bank without any unnecessary delay.

5.8 The Client shall be held liable for any damage suffered by the Bank as a result of the Client breaching his/her/its obligations set forth under this Article 5.

5.9 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/its obligations set forth under this Article 5, or for any damage resulting from an incorrect authorisation or non-execution of an Order due to reasons caused by the Client or a payee.

5.10 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 the Internet public network, strikes and similar). The Bank shall prove to the Client, in accordance with applicable law, that the procedure has been adhered to allowing for it to be verified that a payment order was submitted, a payment transaction authorised, correctly recorded and cleared, and that it was not influenced by any technical incident or other fault.

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 2 month notice period shall start at the moment of the delivery of notice to the Client,

c) on the Conclusive Day;

d) on the expiry of the period of validity of the Certificate.

6.2 The Bank's right to cancel (withdraw from) the Contract in accordance with the General Conditions shall not be prejudiced.

6.3 The Client shall not be allowed to use the Certificate following the expiry/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:

"Bank" shall be Komerční banka, a.s., registered office at Praha 1, Na Příkopě 33/969, Postal Code: 114 07, Czech Republic, IČ (Company ID): 45317054, entered into the Commercial Register kept by the Municipal Court in Prague, Section B, Insert 1360, acting through its organisational unit Komerční banka, a.s., pobočka zahraničnej banky (a foreign bank's branch), registered office at Hodžovo námestie 1A, Postal Code: 811 06, Bratislava, IČO (Company ID): 47 231 564, Slovak Republic, entered into the Commercial Register kept by the District Court in Bratislava I., Section: Po, Insert No. 1914/B.

"Banking services" shall mean any banking deals, services and products the Bank is entitled to deliver pursuant to applicable law.

"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 legal regulations, 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 a Personal Certificate.

"Certification Policy" is a document in which the Bank lays down the rules and procedures for the use of the Certificate and specifies the Cerificate, which the Bank is entitled to modify. The Bank publishes the Certification Policy at its website. The Certification Policy is also available at the Client's Point of Sale. This document is not a Notification as envisaged by the General Conditions.

"Certification Wizard" is an application that supports and administers the Certificate. The Client may access the Certification Wizard on the Bank's Website.

"**Client**" shall mean a natural person who executes and performs the Contract for purposes not associated with his/her business or job activities.

"Client's Point of Sale" shall mean the Bank's point of sale located at the Bank's registered address or another branch/point of sale, if it exists.

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

"Conclusive Day" shall be a day on which the Bank learns, in a trustworthy manner, about the death of a Client, i.e., a day on which conclusive documents attesting the fact that the Client died or was declared dead are delivered to the Client's Point of Sale (these documents can be, e.g., a death certificate, a court or a notary memorandum of performing the inheritance proceedings, decision of the court with a legal power clause concerning the declaration of the Client's death).

"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 documents, without limitation to them, are not Notices: Certification policy.

"Payment Services" shall be Banking Services falling within the scope of payment services as envisaged by the Payments Act (e.g., payments/transfers made from Payment Accounts or issuing of Payment Instruments).

[1] Act No. 7/2005 Coll. on Bankruptcy and Restructuring, as amended.

"Personal Certificate" is a data report issued to the Client by the Bank on the basis of a Contract, providing a link between the data for verification of the Client's electronic signature and the signing party and allowing for the identification of the Client's identity while using the Services. The Personal Certificate contains a Private Key, Public Key and Client's identification data. Act No. 215/2002 Coll., on Electronic Signature, as amended shall not be applied to the Personal Certificate.

"PIN" is the four-digit personal identification number used to verify the Client's authorisation to use the smart 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 smart card.

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

"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.

7.2 Any reference to the Bank's website shall mean a reference to www.koba.sk or other web addresses, which the Bank uses or shall use in association with providing the Banking services.

Article 8. Final Provisions

8.1 The Bank is 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., a foreign bank's branch, governing the issue and use of personal of 25 July 2011.

8.3 These Conditions shall come into effect on 16 June 2012