

VUB, a. s. Business Terms and Conditions for Bancaidentity Service

1 GENERAL PROVISIONS

1.1 VUB, a. s. Business Terms and Conditions for Bancaidentity Service (hereinafter „Terms and Conditions“ or „TC“) govern the relationships between the Všeobecná úverová banka a.s. with its registered seat at Mlynské nivy 1, 829 90 Bratislava 25, Company Reg. NO. 31 320 155 entered in the Business Register of the District Court Bratislava I, Section: Sa, Insert No. 341/B and the client in connection with conclusion an Agreement on Bancaidentity Service (hereinafter „Agreement“), in which a part of its content refers to Terms and Conditions or exercising of rights and performing of obligations arising from the Agreement. Terms and Conditions form integral part of the Agreement, unless the Agreement provides otherwise. Should there be any conflict between the provisions of the Agreement and Terms and Conditions, the provisions of the Agreement shall prevail.

2 DEFINITIONS AND INTERPRETATIONS

2.1 The terms started with a capital letter listed in this article carry, in Terms and Conditions or other documents that Terms and Conditions refer to, a meaning specified in this article, unless Terms and Conditions or other documents provide otherwise:

Act on Banks

Act No. 483/2001 Coll. on Banks as amended.

Act on Electronic Signature

Act No. 215/2002 Coll. on Electronic Signature as amended.

Act on Payment Services

Act No. 492/2009 Coll. on Payment Services as amended.

Act on Personal Data Protection

Act No. 122/2013 Coll. on Personal Data Protection as amended.

Asymmetric Keys

Pair of Public and Private keys (sets of random data generated by the Certificate Holder using the algorithms contained in the relevant security software program).

Authentication

Process of User's identity verifying during login into the Bancaidentity Portal or Portal via Security Credentials.

Authorization

Consent to execute operation via InBiz Service based on prior User's entitlement verification.

Bancaidentity Agreement or Agreement

Agreement on Bancaidentity Service entered into by and between the Bank and the Client subject of which is provision of Bancaidentity Services.

Bancaidentity Portal

Internet portal accessible on <https://ca.intesasanpaolo.com>, dedicated to management of Certificates in relation to the InBiz Service usage.

Bancaidentity Service

Certification Services provided to the Client by the Bank under Bancaidentity Agreement.

Bank or VÚB

Všeobecná úverová banka a.s., with its registered seat at Mlynské Nivy 1, 829 90 Bratislava, Identification No. 31 320 155, entered in the Business Register of the District Court Bratislava I, Section: Sa, Insert No. 341/B.

Bank's Branch

Premises of the Bank's branches or other administrative areas, where the Bank is generally performing its banking transactions and services provisions.

Bank Representative

Authorized employee acting on behalf of the Bank – for example Front Office Clerk or Relationship Manager.

Bank Working Day

Working day when the Bank and/or other payment services providers provide their business via Portal or Bancaidentity portal and this day is not public holiday or non-banking day. Bank Working Day is not the day stated by the Bank as non-banking day because of serious operating reasons.

Billing Account

Client's Account held by the Bank and used for charging of Bancaidentity Service fees.

Certificate or Digital Certificate

Electronic certification, set of data digitally signed by Certifier, which expressly identifies the Certificate Holder and holder of Private Key corresponding to relevant Public Key. Certificate enables to sign Data Flow with Electronic signature.

Certificate Holder or User

Natural person in whose name the Certificate is registered upon Client's request and who is authorised to use the InBiz Service and Bancaidentity Service.

Certification Service or Service

Certification service provided to the Client by the Bank under Agreement on Bancaidentity Service.

Certifier

Intesa Sanpaolo S.p.A., which issues the Certificate as an authorised Certifier.

Civil Procedure Code

Act No. 99/1963 Coll. Civil Procedure Code as amended.

Claim

Exercised right related to the Bank's liability for defects of products and services within stipulated time frames.

Claim Procedure

Rules issued by the Bank governing Bank's and Client's rights and obligations related to settlement of Client's claims regarding the quality and correctness of Bank's services provided to the Client as well as payment services under the Act on Payment Services.

Client

Company or legal entity or other person who enters into Agreement and InBiz Agreement.

Contact Centre or KONTAKT or Help Line

Bank's help line provided to the Clients and Users reachable at phone number 0850 11 17 17 (for domestic calls within Slovakia) or +421 2 48 555 973 (for calls abroad).

CRP Code

Security Credential assigned to the Certificate Holder that is used for User's identification and Authentication during User's log in into the Bancaidentity portal.

Data Flows

Data flows, created from electronic documents via Portal containing information or instructions, sent or received by the User through the InBiz Service.

Electronic Signature

Digital signature on the principle of asymmetric encryption.

Handover Protocol

Confirmation of Security Credentials and Security Device Handover for InBiz Service – Certificate Holder. By signing of this document the Certificate Holder confirms delivery of Security Credentials and Security Device and undertakes to act in accordance with this document.

InBiz Agreement

Agreement on InBiz Service entered into by and between the Bank and the Client subject of which is provision of InBiz Service.

InBiz Login ID or Login ID

Security Credential assigned to the User that is used for

User's identification during User's log in into the InBiz Portal.

InBiz Portal or Portal

Internet portal needed for InBiz Service access and usage accessible on <https://inbiz.vub.sk>. It has public and private section. Public section is available to the public, private part is available to the Users after their log in.

InBiz Profile

Information related to the Users published on the Portal.

InBiz Service or service InBiz

Service of electronic banking provided to the Client by the Bank under InBiz Agreement.

Operating Manual

Document defining the rules and instructions for the use of the Certificates and Bancaidentity Portal. The actual version of the Operating Manual is available on the website <https://ca.intesasanpaolo.com> and <http://www.vub.sk>.

Operational Manager

Certificate Holder nominated by the Client to manage Certificates of all Certificate Holders issued under the same Bancaidentity Agreement. The Client is obliged to nominate a minimum of one up to a maximum of two Operational Managers. The Operational Manager is authorized to:

- Suspend/unsuspend any Certificate issued under the Agreement;
- Revoke any Certificate registered under the Agreement.

Personal Number

Security Credential assigned to the Certificate Holder that is used for Certificate Holder's identification and Authentication in the Bancaidentity Portal.

PIN to USB Flash Drive for Electronic Signature

Security Credential in the form of numeric code required to access USB Flash Drive for Electronic Signature.

Pricelist VUB, a.s. or Pricelist

Document containing list of fees and charges for services provided by the Bank, including examples. Pricelist is published on Bank's Web Site and in Bank's Branches. The Bank is entitled to alter the Pricelist unilaterally within the period stated in relevant legal acts.

Private Key

Reserved part of the pair of Asymmetric Keys.

Public Key

Public part of the pair of Asymmetric Keys through which the authenticity of the Electronic Signature is verified.

Publication

Publication of documents or information in publicly accessible places of Bank's Branches and/or through selected InBiz Services and/or through the Web Site and/or any other suitable form, by which the document or information takes effect, unless otherwise stipulated in the document or information.

Request

Any Client's request regarding Bancaidentity Service, properly signed by the Client (in case the Client is entered in the Business Register, in compliance with the act's procedure therein stipulated).

Security Credential

Is a component used for User's Authentication and/or Authorization in the Portal or Bancaidentity Portal. Security Credentials are assigned to a specific Certificate Holder.

Security Credentials for:

- InBiz Portal usage: InBiz Login ID, Certificate saved on USB Flash Drive for Electronic Signature secured by a PIN to USB Flash Drive for Electronic Signature;
- Bancaidentity Portal usage without the Certificate (e.g. first login): CRP Code, Personal Number and the number of Bancaidentity Agreement;
- Bancaidentity Portal usage with the Certificate: Certificate saved on USB Flash Drive for Electronic Signature secured by a PIN to USB Flash Drive for Electronic Signature.

Security Device

USB Flash Drive for Electronic Signature.

USB Flash Drive for Electronic Signature

Security Device for secured creation and storage of Certificates.

VUB General Terms and Conditions

VUB a.s. General Business Terms and Conditions for Deposit Products.

Web Site

A full set of web pages managed by the Bank, especially www.vub.sk.

2.2 Unless Terms and Conditions or a document that Terms and Conditions refer to imply no other intention it is assumed that:

- a) each reference to a person means individuals and legal entities, unless otherwise stated or implied, as well as their legal successors, assignees or acquirers of rights and/or obligations that became the assignees or acquirers of rights or obligations under the Agreement, to the rights and/or obligations of which they entered into;
- b) each reference to a document or legal regulation means the relevant document or legal regulation as amended, including its novations;
- c) each reference to an article means a reference to the relevant article in Terms and Conditions;

2.3 If a term is used as a definition directly in an article of Terms and Conditions, this term carries a meaning attached to it in this article of Terms and Conditions.

3 BANCAIDENTITY SERVICE PROVISION CONDITIONS

3.1 Prerequisite of the Bancaidentity Service's provision is:

- Conclusion of the InBiz Agreement;
- Conclusion of the Bancaidentity Agreement;
- Nominated Operational Manager by the Client.

3.2 The Bancaidentity Agreement may be signed by the Client at any Bank's Branch Office or other place mutually agreed with the Bank Representative. The Client shall sign the Bancaidentity Agreement(s) in front of Bank Representative otherwise the Client's signature on the Bancaidentity Agreement shall be officially verified.

3.3 The Client may use Bancaidentity Service through its Certificate Holders listed in the Attachment 1 to the Bancaidentity Agreement. The Client shall provide the Bank with Certificate Holder's personal data necessary for Certificate Holder's registration and for proper Service usage (e.g. e-mail address). The Client is liable for provision of correct Certificate Holder's data and is obliged to inform the Bank about any change of these data without undue delay.

3.4 The Client is entitled to alter the list of Certificate Holders unilaterally via Attachment B to the InBiz Agreement. The Attachment B to the InBiz Agreement shall be correctly filled in and delivered by the Client to Bank Representative. The Bank will execute the requested modification within the period of five (5) Business Working Days following the day when the Attachment B to InBiz Agreement (correctly filled in and signed by the Client) shall be delivered to the Bank. When justified reason occurs (i.e. the Attachment B to the InBiz Agreement is not correctly filled in or signed by the Client etc.) the Bank is entitled to postpone execution of abovementioned modification for necessary period and inform the Client without undue delay. The Bank shall inform the Client about the execution of Certificate Holder's modification without undue delay and deliver to the Client actual version of the Attachment 1 to Bancaidentity Agreement.

3.5 The Certificate Holder shall obtain following Security Credentials and Security Device:

- InBiz Login ID delivered to the Certificate Holder in a separate document where the InBiz Login ID is listed;
- Personal Number delivered to the Certificate Holder as part of Handover Protocol;
- CRP Code, whose delivery is splitted into two parts: 1st part of CRP Code is delivered to the Certificate Holder via e-mail as specified by the Client in InBiz Request, 2nd part of CRP Code is delivered to the User in a separate document where the CRP code is listed;
- USB Flash Drive for Electronic Signature for secured creation and storage of Certificates and PIN to USB Flash Drive for Electronic Signature, both stored in USB package. USB package is delivered to the Certificate Holder into own hands. The Certificate is generated on USB Flash Drive for Electronic Signature after Certificate Holder's login into the Bancaidentity Portal.

3.6 Security Credentials and Security Device are issued to a specific Certificate Holder and delivered into his/her own hands. The Certificate Holder confirms handover of Security Credentials and Security Device by signing of Handover Protocol. Security Credentials and Security Device are deemed to be delivered to Certificate Holder at the moment of their handover by Certifi-

cate Holder and in case of their email delivery on the day following the day of their sending unless other/earlier term of their delivery is proved.

4 ISSUANCE AND VALIDITY OF THE CERTIFICATE

- 4.1 The Certificate is issued by Certifier via USB Flash Drive for Electronic Signature which is delivered to the Certificate Holder in person.
- 4.2 The Certificate is generated on the USB Flash Drive for Electronic Signature after Certificate Holder's login to the Bancaidentity Portal. The Certificate Holder can access InBiz Portal and use InBiz Service only after the Certificates are generated on the USB Flash Drive for Electronic Signature.
- 4.3 The Certificate is registered in the name of the Certificate Holder nominated by the Client.
- 4.4 The Certificate is valid for a period of 3 (three) years starting from the date on which the Certificate has been issued, following the instructions set out in the Operating Manual.
- 4.5 Two weeks before expiration of period stipulated in the Article 4.4. hereof, the Certificate Holder can apply for the issuance of a new Certificate, following the instructions set out in the Operating Manual.
- 4.6 Data Flows signed using Electronic Signature satisfy the legal requirement of the written form. The Electronic Signature is legally valid provided that, at the time when the Data Flow is signed, the Certificate is registered in the name of the Certificate Holder and is not expired, revoked or suspended.

5 SUSPENSION OR REVOCATION OF THE CERTIFICATE

- 5.1 The Client and the Certificate Holder may request, at any time, the suspension, unsuspension or revocation of the Certificate, in accordance with the procedures set out in the Operating Manual.
- 5.2 The Bank provides support to obtain requests for Certificate suspension or unsuspension via Bank's Branches (during working hours) or Contact Centre (24x7).
- 5.3 The Bank and the Certifier may suspend or revoke the Certificate for justified reasons for example reasons related to the security of Certificate or reasons related to suspicion of unauthorized or fraudulent usage of the Certificate. In such cases, the Bank notifies in advance the Certificate Holder thereof, informing them of the effective date of the suspension or revocation or without undue delay after the suspension or revocation.

6 OBLIGATIONS OF THE CLIENT AND OF THE CERTIFICATE HOLDER

- 6.1 The Client and the Certificate Holder undertake to communicate to the Bank without undue delay:
 - a) any error or inaccuracy in the data contained in the Certificate or any malfunctioning or suspect-

- ed malfunctioning of the Certificate or of the USB Flash Drive for Electronic Signature, which is not in accordance with the Operating Manual;
- b) the theft or loss of the Security Device or Security Credential (s).

In these cases, the Client or the Certificate Holder shall request the Bank for suspension or revocation of the Certificate.

- 6.2 The Client and the Certificate Holder undertake to inform the Bank about any change of personal data of the Certificate Holder without undue delay.
- 6.3 The Client and the Certificate Holder undertake to not modify the software supplied by the Bank and not to make any change to its operation or configuration.
- 6.4 The Certificate Holder also undertakes to:
 - a) keep with the maximum care and not to allow any third parties to use the Security Device and Security Credentials;
 - b) keep the Security Device in a place different from the one where the Security Credentials are kept.
- 6.5 In case of breach of obligations stipulated in this Article 6, the Client is with the Certificate Holder jointly and severally, liable to the Bank and the Certifier for caused damage.

7 OBLIGATIONS OF THE CERTIFIER

- 7.1 The Certifier issues the Certificates in accordance with the legislation applicable to the registered certifiers.
- 7.2 The Certifier and the Bank do not have any control or checking duties with respect to the content and purposes of the Data Flows signed with the Electronic Signature.
- 7.3 The Certifier and the Bank are obliged to carry out the controls required by specific provisions of law (e.g. anti-money laundering law).

8 PROTECTION OF THE IDENTRUST TRADEMARK

- 8.1 The IdenTrust trademark and its technical specifications are in ownership of IdenTrust Inc. and are part of licence granted to the Certifier.
- 8.2 All software sub-licensed by the Certifier and provided by the Bank to the Client and Users for the purpose of using the Bancaidentity Service and InBiz Service, including the IdenTrust specifications, can not be further sub-licensed, assigned or transferred to third parties by the Client or Users.

9 TERMINATION OF THE AGREEMENT

- 9.1 The Agreement terminates automatically on the day of termination of related InBiz Agreement.
- 9.2 The Agreement may be terminated by mutual agreement of the Bank and the Client, by notice or by withdrawal in cases stated in article 9.4 herein.
- 9.3 Any of the contracting party may terminate the Agreement by notice. Client's Request for Ban-

caidentity Service cancellation shall be deemed as Agreement's termination by notice. The notice period is one month and it shall start on the first day of the month following the month when a written notice shall be delivered to the other party. This shall not apply if the Client has acted provably fraudulently in this case the Bank is entitled to withdraw from the Agreement in accordance with article 9.4 herein.

9.4 The Bank may withdraw from the Agreement in following cases:

- a) a justified suspicion occurs that Client's or CertificateHolder's act is in contrary with legislation or circumvent legislation or is in contrary with good manners or best practices;
- b) Client or Certificate Holder has repeatedly breached provisions of Terms and Conditions or Agreement, or Client or Certificate Holder has breached Terms and Conditions or Agreement materially;
- c) there have been such changes in Client's assets, which jeopardize or may jeopardize fulfillment of Client's obligations to the Bank;
- d) a distraint petition or a motion for decision enforcement pursuant to the Civil Procedure Code has been filed against Client;
- e) a petition for bankruptcy or restructuring has been filed against Client, or bankruptcy or restructuring proceedings have been initiated against Client;
- m) Client has disagreed with any alterations and/or supplements to Terms and Conditions in a manner specified below;
- f) In case mentioned in the Article 9.3.

9.5 The withdrawal is effective elapsing seven (7) calendar days after the day when the withdrawal has been sent to the Client.

9.6 By termination of the Agreement Certificates of all Certificate Holders issued under the Agreement are automatically revoked.

9.7 The Client is obliged to inform all Certificate Holders about the termination of the Agreement under which Certificates of Certificate Holders has been issued without undue delay.

10 CLAIM PROCEDURE

10.1 The Client may make a Claim regarding the quality and correctness of provided Bancaidentity Service in accordance with the Claim Procedure as stated in VUB General Terms and Conditions.

11 BANK'S LIABILITY FOR BANCAIDENTITY SERVICE

11.1 The Bank shall not be liable for damages the Client may incur due to a misuse of Certificate (s), if the Client or CertificateHolder provide Security Credentials to any third party or allow to use Security Device to any third party for any reason.

11.2 Furthermore, the Bank is not liable for any damage incurred the Client as a result of the Client's or

User's acts in contrary with the Agreement, Terms and Conditions or Operating Manual.

11.3 The Bank is liable only for damage caused by it.

12 FEES

12.1 Fees for Bancaidentity Service shall be charged by the Bank from the Billing Account as specified in Agreement by the Client according to the actual Pricelist VUB, a.s..

12.2 In case of unjustified Claim according to the Claim Procedure is the Bank authorized to charge the Client fees according to the actual Pricelist VUB, a.s..

12.3 Management of Security Credentials by the Bank based on Certificate Holder's and/or Client's request or provision of new Security Credential or Security Device may be charged with a fee as stipulated in the Pricelist VUB, a.s..

13 SECURITY OF BANCAIDENTITY SERVICE

13.1 In order to prevent unauthorized collection and misuse of the data, which are protected under the Act on Banks and/or and Act on Personal Data Protection, via fraudulent e-mails (PHISHING), telephone calls made by unauthorized parties in attempt to gain trust with the called person (VISHING) or fraudulent websites (PHARMING), the Client/Certificate Holder is obliged to comply with the following rules:

- a) to log into the Bancaidentity Service only from a trusted/reliable computer, on which the anti-virus and antispyware software is regularly updated;
- b) to check safety of the communication and identity of the web site related to Bancaidentity Service;
- c) to protect the computer on which Bancaidentity Service is accessed against viruses, harmful codes, and Internet attacks;
- d) not to reply to e-mails and telephone calls, in which a person, including any person pretending to be employee of the Bank has required the Client/User to disclose data protected under the Act on Banks and/or Act on Personal Data Protection or Security Credentials. The Client / User is obliged to inform the Bank immediately about any abovementioned attempt to obtain data protected under Act on Banks and/or Act on Personal Data Protection;
- e) not to run/open unknown attachments and links included in spams and e-mails from unknown senders;
- f) not to send and not to insert data protected under the Act on Banks and Act on Personal Data Protection onto non-encrypted and non secured web pages.

13.2 When using the Bancaidentity Service, the Certificate Holder agrees that the Bank is entitled to verify Certificate Holder's identity via Security Credentials in Bank's requested combination and to ask Certificate Holder to change his/her Security Credentials.

- 13.3 To ensure protection of access to Bancaidentity Portal the Client is recommended by the Bank to change his/her PIN to USB Flash Drive for Electronic Signature during the first login. Certificate Holder may change his/her PIN to USB Flash Drive for Electronic Signature at any time via Bancaidentity Portal.
- 13.4 Bancaidentity Portal is a website secured by the SSL protocol with valid (trusted) certificate and the address of website is: <http://ca.intesasanpaolo.com>. This certificate makes possible to verify directly through the internet browser the authenticity of the Bancaidentity Portal. In case the internet browser does not show the right website address or it displays any warning about not trusted certificate, to ensure protection of the Certificate Holder's access, the Bank recommend the Certificate Holder not to use his/her Security Credentials. Non-compliance incident shall be immediately reported to the Contact Centre.
- 13.5 To ensure confidentiality of data, which are subject to protection under the Act on Banks and/or the Act on Personal Data Protection, the Certificate Holder is required not to use Bancaidentity Service on publicly accessible computers (e.g. in Internet cafe, at universities, at hotels, etc.). The Bank shall not be liable for misuse of Bancaidentity Service when using publicly accessible computers.
- 13.6 The Security Credentials and Security Device shall be protected against misuse, theft and any third party access to such Security Credentials and Security Device. The Certificate Holder shall be obliged to make sure that he/she takes all necessary preventive measures against the misuse of the aforementioned Security Credentials and Security Device.
- 13.7 The Bank will never request the Client and/or Certificate Holder to:
- Disclose or enter his/her Security Credentials and/or data protected under the Act on Banks and/or and Act on Personal Data Protection via Bancaidentity Service;
 - Disclose any data of and from Security Credentials over the telephone, with the exception of situations when the Client or Certificate Holder has initiated the contact or ask for contact with the Bank via the KONTAKT.
- 13.8 Any request for entering more data of and from Security Credentials may lead to the phishing attack.
- 13.9 If the Client or Certificate Holder suspects any of the Security Credentials or Security Device was misused, the Client and/or the Certificate Holder shall forthwith request their blocking at any Bank Branch or via KONTAKT.
- 13.10 The Certificate Holder has a limited number of consecutive incorrect attempts for entering of PIN to the USB Flash Drive for Electronic Signature. After the limit is used up, the Certificate will be automatically locked. The Operational Manager or Certificate Holder may unlock the Certificate via Bancaidentity Portal. The Client or Certificate Holder may also request to unlock the Certificate at any Bank Branch.
- 13.11 In the event of a successful login to InBiz Service or Bancaidentity Service the number of unsuccessful attempts is nullified.

14 JOINT PROVISIONS

14.1 GOVERNING LAW AND JURISDICTION

- 14.1.1 The Agreement and related relationships shall be governed by Slovak law.
- 14.1.2 Agreement and related documents and all communication between the Bank and the Client/Certificate Holder are executed in the Slovak language. If the Agreement is executed in other than the Slovak language their Slovak version shall prevail for the purpose of their advisement and interpretation of terms.
- 14.1.3 Relationships between the Bank and the Client which are not explicitly regulated by the Agreement, or Terms and Conditions or VÚB General Terms and Conditions are governed by the provisions stipulated in the relevant legal acts to the extent which does not change the purpose and/or intention specified in the abovementioned documents, with the exception of mandatory provisions set out therein.

14.2 DELIVERY OF DOCUMENTS

- 14.2.1 All documents are delivered by the Bank in person, by courier, by mail or by electronic communication media (e-mail or another electronic means) at the address as latest specified by Client in Client's Request.
- 14.2.2 Written documents delivered in person are deemed to be delivered once handed over to the Client or to a person authorized by the Client which Client or authorized person shall confirm to the Bank in writing.
- 14.2.3 Documents delivered by a courier service are deemed to be delivered on the third day after their handover.
- 14.2.4 Documents delivered by mail are deemed to be delivered in Slovakia on the third day after their dispatch and in foreign countries on the seventh day after their dispatch.
- 14.2.5 Documents are deemed to be delivered also if Bank's consignment is returned as undeliverable as specified in Sub-sections 14.2.2. to 14.2.3 herein provided it was sent to the latest address notified by the Client on the Client's Request.
- 14.2.6 Documents delivered by e-mail or another electronic medium are deemed to be delivered on a day after the day of their sending, unless an earlier/another delivery date is proved.
- 14.2.7 The Client is obliged to inform the Bank on a failed delivery of documents of any type, the delivery of which is expected, mainly of documents delivered by electronic means, otherwise the Bank is not liable for any potential damage caused by such failed delivery.

14.3 BANK SECRECY

- 14.3.1 All phone calls in Contact Centre may be recorded for security reasons, legal acts recording and monitoring of Bank services quality and may be used as a proof in case of Claim or dispute. Information about call recording shall be announced at the beginning of the call, call continuing shall be considered as a Client's or Certificate Holder's consent to recording.
- 14.3.2 The Bank hereby reserves the right to process and store information related to Bancaidentity Service

(including e-mail communication with the Client and/or Certificate Holder) through automated and non-automated tools, e.g. IP address, in order to fraud prevention and protection of rights and legitimate interests of the Client and the Bank.

15 CLIENT'S AND BANK'S REPRESENTATIONS UNDER ACT ON PAYMENT SERVICES

15.1 The Bank and the Client have agreed that following provisions of Act on Payment Services shall not apply on contractual relationship between the Bank and the Client: article 12 par. 1 and 4 and article 33 par. 3. VÚB General Terms and Conditions not in contrary with this provision are not aggrieved.

16 OTHER PROVISIONS

16.1 Terms and Conditions are effective from the day when the Agreement has been signed, during and also after termination of the contractual relationship between the Bank and the Client until all mutual receivables and liabilities are fully satisfied.

16.2 The Bank proposes to Client to resolve any disputes, claims or conflicts arising from or related to the Agreement (including all questions about its existence, validity or termination, hereinafter only the "disputes") via the Permanent Court of Arbitration of the Slovak Banking Association. If the Client fails to provably reject this proposal within 30 days from the date of concluding the Agreement, the Bank shall consider the Arbitration Agreement, in the form of an arbitration clause, to be concluded and the disputes shall be resolved by the Permanent Court of Arbitration of the Slovak Banking Association in accordance with its arbitration rules becoming under this provision an integral part of the Agreement. The place of arbitration proceeding will be Bratislava. The language of arbitration proceeding will be the Slovak language. The arbitration proceeding shall take place in the seat of the arbiter and the arbiter shall decide on the matter without oral hearing, solely on the basis of written documents presented by the parties within the period specified by the arbiter. The arbiter may order oral hearing, provided s/he does not consider the presented documents sufficient. The documents in the arbitration

proceeding shall be sent to parties by the arbiter to the address specified by the party or to its advocate or legal counsel. The delivery shall be effective even if the addressee rejects to take the document over or even if s/he fails to pick it up as a mail in spite of the notification by the post office. The arbitration judgement shall be definitive and legally binding and takes effect of the valid court judgement on the day of its delivery. The Bank and the Client declare that they will voluntarily subordinate to the arbiter's judgement. This arbitration clause forms an integral part of the Agreement and binds legal successors of both contracting parties. The termination of the Agreement shall not effect the arbitration clause forming an integral part thereof.

16.3 The data provided by the Bank to the Client based on the Agreement remain valid during the whole existence of contractual relationship between the Bank and the Client, unless the Bank informs the Client of their alteration /or supplementation on the notice boards at Bank Branches or Web Site.

16.4 The authority supervising financial markets is the National Bank of Slovakia.

16.5 Terms and Conditions are published on Bank Branches and on Web Site.

16.6 The Bank is entitled to unilaterally alter and/or supplement Terms and Conditions in view of the changes related to Bank business policy, legislation, or changes in the financial market. The Bank shall inform the Client of abovementioned alterations/supplements in form of Publication at least two (2) months before the effectiveness of these alterations/supplements. The Client is entitled to express disagreement with the alterations and/or supplements made to Terms and Conditions by a written notice delivered to the Bank in form of registered mail no later than on the day preceding the day of the effectiveness stated by the Bank. If the Client fails to inform the Bank about his/her disagreement with alterations/supplements in accordance with the above, it is understood that the Client accepted alterations/supplements and the altered and/or supplemented Terms and Conditions shall become an integral part of the Agreement concluded between the Client and the Bank as on the day of effectiveness of altered and/or supplemented Terms and Conditions.

The Terms and Conditions take effect on 06/10/2015.
Všeobecná úverová banka, a.s.