VÚB, a.s., Mlynské nivy 1, 829 90 Bratislava 25, kontakt@vub.sk
Business Reg.: District Court Bratislava I
Section: Sa, Insert No. 341/B, ID: 31320155, www.vub.sk

Object of Business: Pursuant to the Banking Act
Supervisory Body: National Bank of Slovakia
I. Karvaša 1, 813 25 Bratislava
Bank License granted upon NBS Decree
UBD-1744/1996 of September 26, 1996

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

1 GENERAL PROVISIONS

VUB, a. s. Business Terms and Conditions for InBiz Service (hereinafter „Terms and Conditions" or „TC") govern the relationships between 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 Disctrict Court Bratislava I, Section: Sa, Insert No. 341/B and the client in connection with conclusion of an Agreement on InBiz 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 an integral part of the Agreement, unless the Agreeement 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 Personal Data Protection
Act No. 122/2013 Coll. on Personal Data Protection as amended.

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

Additional Services
Services offered by the Bank beyond the Basic Offer, which the Client may use upon his/her request through the InBiz Service.
Additional Services include:

- FileGate;
- CashPool reports;
- Multibank;
- Financing limit overview;
- PDF statements for current account, term deposits and loan accounts.

This list of Additional Services could be changed or amended by the Bank. Additional Services could be charged according to the actual Pricelist VUB, a.s...

Agreement or InBiz Agreement
A common name for the Principal Agreement or Connected Agreement.

Approval
A document with the name " Approval and Power of Attorney", by which the Principal Client grants an approval to connect the Connected Person to the Principal Agreement based on the Secondary Agreement and with closing of the Secondary Agreement.

Asymmetric Keys
A 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
The process of User´s identity verification during the login to the Portal via Security Credentials.

Authorization
The consent to execute an operation via the InBiz Service based on prior User's entitlement verification.

Authorization Rights
The right of a User to Access the defined Connected Accounts and Connected Services.
Authorization Rights are defined by the Client in the Request, or by the Master User or Configurator directly through the Portal, and separately for each of the Users.

Authorization to Connect ISP Group Account to InBiz Service
The document named Authorization to Connect ISP Group Account to InBiz Service, by which the Client authorizes the Servicing bank for the Data flow exchange and Data provision in line and scope described in the relevant document.

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

Bancaidentity Portal
The internet portal accessible on https://ca.intesasanpaolo.com, dedicated to management of Certificates in relation to the InBiz Service usage.

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

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

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 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 Disctrict Court Bratislava I, Section: Sa, Insert No. 341/B.

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

Basic Offer
Services, offered by VÚB to all Clients based on the closed Agreement and charged through the price for InBiz service.
Basic Offer includes the following services:

- Payment operations
  - SEPA, Non SEPA credit transfers
  - Automatic transfers
  - Standing orders
  - SEPA direct debits
- Waiting and rejected transactions:
  - List of waiting SEPA and Non SEPA credit transfers
  - List of incoming and outging SEPA direct debits
  - Historical overview of the rejected SEPA, Non SEPA credit transfers and SEPA direct debits
- Owner´s transactions:
  - Management of SEPA direct debit authorizations
  - Management of the account protection against SEPA direct debit
  - Management of account movements and event Notifications
- Account balances and transactions:
  - Account balances and transactions on current accounts, term deposits and loan accounts
- Payment cards
  - Payment cards transaction overview and payment cards information
  - Payment cards management
- InBiz Mobile

The Bank is authorized to change or amend the list of the Basic offer services without Client´s agreement.

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

Certificate Holder
A natural person in whose name the Certificate is registered upon Client's request.

Certificate or Digital Certificate
An electronic certification, set of data digitally signed by the Certifier, which expressly identifies the Certicate Holder and the holder of the Private Key corresponding to the relevant Public Key.

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

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
An excercised 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 the 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
A common name for the Principal Client and the Connected Person.

Connectable Account
Any account of the Client, company, legal entity or other person (based on the granted Power of Attorney), held by the Bank, Group Bank or another bank or branch of a foreign bank, not beeing a Group Bank. Account held by the Group Bank or another bank or branch of a foreign bank, not beeing a Group Bank, could become a Connected Account, if the technical prerequisities and conditions for the electronic data exchange between the bank and another bank or branch of a foreign bank have been fulfilled for its connection to the Service.

Connectable Service
A common name for the services included in the Basic offer and Additional Services and/or Service provided to the Client by a Group Bank.

Connected Account
An account from the list of the Connectable Accounts defined by the client and held with a Group Bank. The Client can access Connected Accounts only through the Inbiz Service.

Connected Person
A company, legal entity or other person belonging to the group of the Principal Client or connected to the Principal Client by another economic or legal relationship, which closed with the Bank the Secondary Agreement based on the Approval of the Principal Client..

Connected Service
A common name for the services included in the Basic offer and Additional Services and/or Service provided to the Client by a Group Bank, included in the list of Connectable Services, which the Client has connected to the Inbiz Service in the Attachment A of the InBiz Agreement.

Contact Centre, or KONTAKT service, or Help Line
The Bank's help line provided to 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
A Security Credential assigned to the Certificate Holder that is used for User´s identification and Authentification during the User´s login to the Bancaidentity portal.

Data Flows

Any flows containing information or instructions, which are possible to be transferred between the Client and the Bank via the Portal and/or FileGate.

Electronic Signature
A digital signature on the principle of asymmetric encryption.

FileGate
A service, which enables an exchange of Data Flows between the Bank and the Client via a separate application installed on the Client´s workstation. FileGate also allows automatic or manual download of Data Flows received from the Bank and an upload of Data Flows to the Bank. FileGate is established for the Client based on a separate request.

FileGate login credential
A common name for the FileGate Login ID and the FileGate password.

FileGate Login ID
A login credential delivered to the Administrator, which serves for logging in to FileGate.

FileGate Password
A login credential delivered to the Administrator, which serves for logging in to FileGate.

Group Bank
Any bank belonging to the Intesa Sanpaolo Group; unless otherwise stated or required by the context herein, such term includes the Bank.

Group or ISP
Intesa Sanpaolo Bank Group.

Holding
A common name for the Principal client and all his Connected Persons, who signed Secondary Agreements to the Principal Agreement.

InBiz Connected Services
A common name for the Basic Offer and Additional Services.

InBiz Login ID or Login ID
A Security Credential assigned to the User that is used for User's identification during User´s log in to the InBiz Portal.

InBiz Mobile
A web application designed for smartphones. It offers a smaller set of functionalities of the InBiz Services than the desktop application. InBiz Mobile is available only for the InBiz OTP Token users.

InBiz OTP Token
A Security Device – HW component granted to the User for his/her Authentification and Authorization of the transactions executed by the User in the InBiz Portal.

InBiz portal or Portal
The internet portal needed for InBiz Service access and usage, accessible on https://inbiz.vub.sk. It has a public and private section. The Public section is available to the public, while the private part is available to the Users after their login.

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

InBiz Profile
Information related to the User, published on the Portal.

InBiz User Role
A role, defined by the Client for the User to Access the Portal and for the usage of the InBiz service – Master User, Configuratior or Operator.

Limit
The limitation, which defines the amount, up to which the authorized Users could execute payment operations.

Master User Authorization Rules
User Access rights granted to the InBiz user with a role of Master User or Configurator. This user is allowed via the Portal:

- To manage the list of existing Connected Persons – Connected Persons can be deactivated/activated. However, He/she is not allowed to add a new Connected Person to this list;
- To manage the list of existing Connected Accounts – Connected Accounts can be deactivated/activated. However, He/she is not allowed add a new Connected Account to this list;
- To define and change the Scope of user Access rights of other Users;
- Temporarily block and/or unblock Access to the Portal for a user.

Multibank
Additional service, which allows the User to connect to and to execute transactions over accounts, not held by VUB.

Notification
A Service, which the Bank offers to the Client through SMS message or e-mail. The Client is responsible for the correctness of the contact data, where the messages are to be sent.

Operating Manual
A document defining the rules and instructions for the use of the Certificates and Bancaidentity Portal.

OTP code
A Security Credential, displaying a combination of numeric characters on the InBiz OTP Token display after the request for OTP generation

Password (PIN)
A Security Credential granted to the User for Identification and Authorization of the User during the login to the portal and to the transaction Authorization in the Portal.

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

Power of Attorney
Power of Attorney granted based on §31 Art. 1 Act No. 40/1964 Coll. Civil Code as amended, for disposal with the defined accounts of the Principal through the InBiz Service.

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

Principal Agreement
An agreement for the use of the Inbiz Service – Principal Agreement entered into by the Principal Client and the Bank for the use of the Inbiz Service.

Principal Client
A company, legal entity or other person who entered into the Principal Agreement with the Bank.

Private Key
The reserved part of the pair of Asymmetric Keys.

Publication
A 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.

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

Request
Any Client´s request regarding the 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). In such case, where the changes executed by the Bank based on the Client´s request could be executed also by the User through the Portal, the change published on the Portal is valid.**Routing bank**
For InBiz Service purposes it is a bank or a branch of a foreign bank (including the Bank), which is sending the Data Flows.

Secondary Agreement
The agreement for the use of the Inbiz Service – Secondary Agreement entered into by a Connected Person with a Group Bank and connected to the Principal Agreement.

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

- For InBiz OTP Token users: InBiz Login ID, Password (PIN), OTP code generated by the InBiz OTP Token;
- For USB Flash Drive for Electronic Signature users:
  - InBiz Portal usage: InBiz Login ID, Certificate saved on a USB Flash Drive for Electronic Signature secured by a PIN to the 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 the USB Flash Drive for Electronic Signature secured by a PIN to the USB Flash Drive for Electronic Signature.

Security Credential Handover Protocol
A common name for the Confirmation of Security Credentials and Security Device Handover for InBiz Service - OTP User and the Confirmation of Security Credentials and Security Device Handover for InBiz Service - Certificate Holder, by signing of which the User confirms the handover of the Security Credentials and Security Device by the Bank and undertakes to operate in accordance with the signed document.

Security Device
InBiz OTP Token and USB Flash Drive for Electronic Signature.

Services offered by a Group bank
Services offered to the Client by a Group bank, based on conditions set by the Group Bank which fulfill technical prerequisities compatible with the Service.

Servicing Bank
For the purpose of the InBiz Service it is the bank or the branch of a foreign bank (including the Bank), which is receiving the Data Flows.

Signature Group
The name of the group with at least one User, which is necessary for the Authorization of the Data Flow in the Portal.
Inclusion of any User into the Signature Group is defined by the Client in the Attachment B of the InBiz Agreement. It is not possible to modify the Signature Rights through the Portal, even not by using the Master User rights.

Signature Right
The rule defining the scope and way of disposal with the financial means on the Connected Account through the Portal. The Signature Right will be applied on each Data Flow and has the following parameters:

- Connected Account, for which the Signature Right will be applied;
- Limit in EUR valid for each payment operation contained in the Data flow. Each payment contained in the Data flow must be of lower or equal amount than the limit;
- Connected Service – it is possible to apply the Signature Right only in frame of this Connected Service;
- Way of disposal.

Signature Rights are defined by the Client in the Attachment A of the InBiz Agreement for each Connected Account separately. It is not possible to modify the Signature Rights through the Portal, not even by using the Master User rights.

Signature Weight
The number of points from 1 to 100 assigned to the User based on the required Authorization as defined by the Client in the Attachment A of the InBiz Agreement.

USB Flash Drive for Electronic Signature
A Security Device for secured creation and storage of Certificates.

User
The person authorised to use the Inbiz Service in the name and on behalf of the Client in accordance with the specific role assigned to him/her as a User, Signature Group and Authorization Rules.

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

Way of Disposal
Defines a combination of the Signature rights and the number of necessary User´s Authorizations.

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 SERVICE OFFERING CONDITIONS

3.1 Offering of the service is based on the electronic data Exchange between the Client and the Bank, Group Bank or another bank or a branch of a foreign bank, not beeing a Group Bank through the Portal.

3.2 Condition for the offering of the Service is:

a) existence of at least one current account held by the Bank, in case of a Connected Person in the Bank or a Group Bank;
b) closing of the Agreement ;
c) closing of Bancaidentity Agreement (in case the Client requires at least one User with the USB Flash Drive for Electronic Signature);
d) defining at least one User with a Master User role in case of Principal client.

3.3 The 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 Agreement in front of Bank Representative, otherwise the Client´s signature on the Bancaidentity Agreement shall be officialy verified.

3.4 The Client is using the Service through Client defined Users. Principal client is obliged to define at least one User for the Service. The Client is obliged to provide the Bank with personal data of the Users for the purpose of their identification, registration and service usage. The Client is responsible for the correctness of the given personal data of Users and is required to inform the Bank about any change of the personal data of Users without any delay.

4 INBIZ SERVICE

4.1 CONNECTED SERVICES

4.1.1 The Client may use all services belonging to the Basic Offer Services and the specified Additional Services. Additional Services, specified by the Principal Client as Connected Services, are defined in the Attachment A to the Principal Agreement.

4.1.2 Principal Client may change the extent of Additional Services by changing the Attachment A of Principal Agreement. Attachment A has to be properly filled in by the Principal Client and delivered to the Bank representative. The Bank will execute the change required by the Principal Client in 5 (five) bank working days from receipt of a complete and by the Principal Client duly signed Attachment A. In reasonable cases (e,g,. Attachment A has not been duly signed or fulfilled etc.) is the Bank authorized to suspend temporarily execution of the relevant change, and this for the necessary period, which the Bank will inform the Principal Client about without undue delay. The changed Attachment A will replace the previous version of the Attachment A and will become an unseparable part of the Principal Agreement. The Bank will inform Principal Client about the execution of the relevant change.

4.2 CONNECTED ACCOUNTS

4.2.1 Through InBiz service The Client may access all Connected Accounts specified in the Attachment A. Through InBiz service the Client may access also all Connected Accounts of the Holding, according to the extent specified in the Authorization Rules assigned to the Users of the Holding.

4.2.2 Connecting of an Account, held by the Group Bank, to the List of Connected Accounts is allowed only by signing of Authorization to Connect ISP Group Account to InBiz Service of this Group Bank and activation of the Additional Service „Multibank".

4.2.3 Connecting of an Account, held by the bank or branch of a foreign bank, not beeing a Group Bank, is allowed only by request for connecting of account, addressed to this bank by the Client as well as by fulfillment of relevnat conditions, specified by this bank or branch of a foreign bank, and by activation of the Additional Service „Multibank".

4.2.4 The Client is authorized to change by himself specified Connected Account by changing Attachment A to the Agreement. Attachment A has to be properly filled in by the Client and delivered to the Bank representative. The Bank will execute the change required by the Client in 5 (five) bank working days from receipt of a complete and by the Client duly signed Attachment A and in case of connecting account held by a Group Bank also Authorization to Connect ISP Group Account to InBiz Service. In reasonable cases (e,g,. Attachment A has not been duly signed or fulfilled or the Bank will not receive the Authorization to Connect ISP

Group Account to InBiz Service or other necessary information or documents from the Group Bank and/or bank or branch of a foreign bank, not beeing a Group Bank etc.) is the Bank authorized to suspend temporarily the execution of the the relevant change, and this for the necessary period, about which the Bank will inform the Client without undue delay. The changed Attachment A will replace the previous version of the Attachment A and will become an unseparable part of the Agreement. The Bank will inform Client about execution of the relevant change.

4.3 **CONNECTED PERSONS**

4.3.1 The condition for connecting a Connected Person to a Principal Agreement based on the Secondary Agreement is the signing of the Approval before closing the Secondary Agreement. The Principal Client is authorized to cancel the Approval anytime, about which the Principal Client must inform the Connected Person (specified in the relevant Approval) without undue delay.

4.3.2 Connected Persons may through the Portal use only those services of the Basic Offer and Additional Services, which were selected for them by the Principal Client of the list of his Connected Services. The Principal Client is obliged to inform the Connected Person about the services of the Basic Offer and Additional Services, which the Connected Person is authorized to use, as well as about all relevant later changes.

4.4 **USE OF THE SERVICE**

4.4.1 The Client is using the Service through the Users, specified in the Agreement.

4.4.2 The Client is obliged to define Authorization rules for each Connected Account separately.

4.4.3 The Client is authorized to change the list of Users by changing Attachment B of the Agreement and the Authorization rules changing Attachment A of the Agreement. Attachment A and/or B has to be properly filled in by the Client and delivered to the Bank representative. The Bank will execute the change required by the Client in 5 (five) bank working days from receipt of a complete and by the Client duly signed Attachment A and/or B. In reasonable cases (e,g,. Attachment A and/or B has not been duly signed or fulfilled etc.) is the Bank authorized to temporarily suspend the execution of the relevant change, and this for the necessary period, which the Bank will inform the Client about without undue delay. The changed Attachment A and/or B will replace the previous version of the Attachment A and/or B and will become an unseparable part of the Agreement. The Bank will inform Client about execution of the relevant change.

4.4.4 Based on the way of disposal specified by the Client in the Attachment A of the Agreement, the Bank will define the type of the disposal and will assign Signature Weights to each User for each Connected Account, Connected Service and Limit in a following way:

- The Client has chosen Authorization from the same Signature Group. The allowed combinations of the Authorization are "A", "AA", "AAA", "B", "BB", "BBB"). The Bank will setup for the Authorization rules the type of the disposal „simple disposal". According to the number of relevant characters the setup of the Signature weights for the User will be in following way:
  - for "A" or "B" Signature weight 100 points.
  - for "AA" or "BB" Signature weight 50 points.
  - for "AAA" or "BBB" Signature weight 34 points.

  Each in this way defined User will be defined on the Portal for the relevant Authorization rule into the Signature Group „A". Application of the Authorization rule is beeing considered as successfull, when the sum of the signature weights of the Users based on the same Authorization rule will be at least 100 points.
- The Client has chosen Authorization from different Signature Group. The allowed combinations "AB", "AAB", "ABB". The Bank will setup for the Authorization rules the type of the disposal „combined disposal". According to the number of the relevant „A" or „B" characters the setup of the Signature weights for the User will be in following way:
  - for "AB" – each User in the Signature Group „A" will have Signature Weight 50 points and in the Signature Group „B" will have Signature Weight 50 points.
  - for "AAB" and "ABB" – each User in the Signature Group „A" will have Signature Weight 34 points and in the Signature Group „B" will have Signature Weight 34 points.

  Each User with the signature right to authorize Data Flows is assigned in frame of the Authorization rule to the same Signature Group as being defined by the Client in the Attachment A. Application of the Authorization rule is being considered as successful, when the sum of the signature weights of Users based on the same Authorization rule will be at least 100 points and at the same time from each Signature Group at least one User has authorized the Data Flow.

4.4.5 The Client is obliged during using the Service to proceed in line with the Agreement, Terms and Conditions and recent version of the Operating Manual.

4.4.6 The User is obliged during using the Service to proceed in line with the Terms and Conditions and recent version of the Operating Manual.

4.4.7 The Bank is authorized to change the Operating Manual for technical reasons (e.g. by purpose of increasing the security of the Service etc.) or for reasons of changing the offered Connectable Services, about which the Client will be informed through the Portal or Web site without indue delay after the execution of this change.

4.4.8 In case of any difference between the provisions in the Operational Manual and Terms and Conditions the Terms and Conditions are valid.

4.4.9 The Client is obliged to implement on his own costs and responsibility the necessary technical infrastructure (HW and SW) required for the Access to the Service . The Client is also obliged to implement necessary security measures against programs and cyber attacks, which could damage technical infrastructure or electronic platform or the system of the Bank.

4.4.10 The Client is responsible for all acts executed by his/her Users through the Service. The Client is obliged to implement all measures needed for prevention of any damages, which could arise to the Bank relevant to the acts of the Users (e.g.. in the Bank system).

4.5 **USERS**

4.5.1 The Users are authorized to use the Service in line with the InBiz User role, Signature Group and Authorization Rules to the Connected Accounts and Connected Services, defined by the Client (in case of the Authorization rules also by the User with Master Users rights) for each User separately.

- Any User could have one of the following InBiz User roles:
  - Master User – can be only one for the whole Holding, assigned to the Principal Client, who defines the Master User. Master User has Master User's rights in relation to the whole Holding and its Users. At the same time he has also the InBiz User Role Operator, unless not specified differently by the Client.
  - Configurator – has Master User's rights, in relation to the Principal Client and/or Connected Persons and their Users, with exception of the Master. At the same time he/she has also the InBiz User Role Operator, unless not specified differently by the Client.
  - Operator – can view, create, authorize, send and receive Data Flows in the extent specified in his/her Authorization rights.

4.5.2 The Client is authorized to change the InBiz User role and/or the Signature Group of the User by changing Attachment B of the Agreement. Attachment B has to be properly filled in by the Client and delivered to the Bank representative. The Bank will execute the change required by the Client in 5 (five) bank working days from receipt of a complete and by the Client duly signed Attachment B. In reasonable cases (e.g. Attachment B has not been duly signed or fulfilled etc.) is the Bank authorized to temporarily suspend the execution of the relevant change, and this for the necessary period, which the Bank will inform the Client about without undue delay. The changed Attachment B will replace the previous version of the Attachment B and will become an unseparable part of the Agreement. The Bank will inform the Client about the execution of the relevant change.

4.5.3 The Client is authorized to change the Authorization rights of the User based on a written request delivered to the Bank or by change applied directly on the Portal through Master User and/or Configurator. In case of a written request the request has to be properly filled in by the Client and delivered to the Bank representative. The Bank will execute the change required by the Client in 5 (five) bank working days from receipt of a complete and by the Client duly signed request. In reasonable cases (e,g,. request has not been duly signed or fulfilled etc.) the bank is authorized to temporarily suspend the execution of the relevant change, and this for the necessary period, which the Bank will inform the Client about without undue delay. The Bank will inform Client about the execution of the relevant change.

4.5.4 In case of InBiz User role changes, the Bank will assign to the User a new Security Device and Security Credentials.

4.5.5 The most recent and valid version of the Authorization rights of Users is always present on the Portal.

4.5.6 The Bank accepts requests for suspension of the User either in its Bank's Branches during working hours of the relevant Bank's Branch or through the Contact center 24x7. The Bank accepts requests for unsuspension of the User in its Bank's Branches during working hours of the relevant Bank's Branch.

4.5.7 The unsuspension of the User can be requested only by the Client.

4.5.8 Suspension and unsuspension of the User may be executed also by Master User on the Portal in frame of Master Users rights.

4.5.9 Users with authorization for Card management and Card report.are set by the Client in a Request. Through InBiz, the User with the assigned authorization for Card management and Card report has access to the following:

a) Debit cards issued to the Account (Accounts) owner of which is the Principal client, as well as to debit cards issued to the Account (Accounts) owner of which is a different person than the Principal client who, based on a Power of Attorney, authorized the Principal client to execute any action related to these debit cards and/or acquire any information related to these debit cards.

b) Credit cards and approved loan limit (loan limits) owner of which is the Principal client, as well as to credit cards with the approved loan limit (loan limits), owner of which is a different person than the Principal client, who based on a Power of Attorney, authorized the Principal client to execute any action related to these credit cards and/or acquire any information related to these credit cards.

4.5.10 In case of a Holding use of the InBiz Service, the User with the authorization for Card report and Card management has the access to all:

a) Debit cards issued to an Account (Accounts) owner of which is a Connected Person, in relation to which the User has the set Authorization rights.

b) Credit cards and approved loan limit (loan limits) owner of which is a Connected Person, in relation to which the User has the set Authorization rights.

4.5.11.The Card report service enables the User to access information on debit and/or credit cards, e.g. processed transactions, set limits, card expiration date and similar..

4.5.12 The Card management service enables the User to:

a) Send to the Bank a notification about the intent to request an issuance of a new credit and/or debit card, based on which the Bank issues a request for a new debit and/or credit card issuance;

b) send the Bank a request for a re-issuance of a lost, stolen or damaged credit and/or debit card;

c) send a request for a permanent blockage of a credit and/or debit card;

d) change the internet limit on a debit card. The internet limit on a debit card is changed immediately;

e) change the maximum daily limit on a debit card, limit on ATM withdrawals and limit on payments at merchants. The change of the maximum daily limit, and/or the limit on ATM withdrawals and/or the limit for payments at merchants is processed by the bank within five (5) Bank Working Days since the receipt of the Request. In reasonable cases the bank is authorized to temporarily suspend the execution of the relevant change, and this for the necessary period, which the Bank will inform the Client about without undue delay.

f) change the internet limit on a credit card. The internet limit on credit card is changed immediately;

g) change the cash limit on a credit card. The change of the cash limit on a credit card is processed by the Bank within five working (5) Bank Working Days since the receipt of the Request. In reasonable cases the bank is authorized to temporarily suspend the execution of the relevant change, and this for the necessary period, which the Bank will inform the Client about without undue delay.

h) set a Notification about trasactions carried out with the debit and/or credit cards authorized by the card holder.

4.5.13 The User of the FileGate service is the Administrator. All actions performed through FileGate are considered as actions performed by the Client.

4.5.14 The FileGate service enables the User to receive Data Flows sent by the bank and send Data Flows to the bank.

4.5.15 Data Flows can be sent to the Bank by the following methods:

a) directly to the Bank – The Data Flow is sent to the bank for processing directly and without authorization;

b) Through the InBiz Service with the option to edit – The Data Flow is sent from FileGate to the InBiz Service with an option to edit. The Data Flow is a subject to Authorization according to the rules set in the Attachment A of the Agreement;

c) Through the InBiz Service without the option to edit – The Data Flow is sent from FileGate to the InBiz Service without an option to edit. The Data Flow is a subject to Authorization according to the rules set in the Attachment A of the Agreement.

4.6 **SECURITY CREDENTIALS**

4.6.1 Security credentials are used for identification and/or authentication of the User during the login to the Portal and/or for the Authorization of by User executed operations through the Portal (e.g. sending of Data Flows etc.).

4.6.2 Security credentials will be issued for each specific User and will be delivered into own hands of the User after his/her proper identification. Security credentials and Security devices are considered to be delivered just after their handover to the User and in case, they have been sent via e-mail, they are considered to be delivered the day after the day they were sent, if no earlier delivery date can be provided by evidence.

4.6.3 The Client can choose as a Security device for the User either the InBiz OTP Token or USB Flash Drive for Electronic Signature. Issuance of the USB Flash Drive for Electronic Signature and management of Certificates are governed by the provisions of VUB, a. s. Business Terms and Conditions for Bancaidentity Service.

4.6.4 In case the InBiz OTP Token has been chosen for the User, the User will receive from the Bank the following Security credentials and Security devices:

- InBiz Login ID, delivered to the User as attachment to the Security Credential Handover Protocol;
- Password (PIN), delivered to the User to his/her e-mail address, specified by the Client in the Request, or which is listed in his/her InBiz profile in case of later changes;
- InBiz OTP Token, which generates an OTP code. The InBiz OTP Token is delivered to the User into own hands.

4.6.5 In case the USB Flash Drive for Electronic Signature has been chosen for the User, the User will receive from the Bank the following Security credentials and Security devices:

- InBiz Login ID, delivered to the User as attachment to the Security Credential Handover Protocol;
- Personal Number, delivered to the User as in the Security Credential Handover Protocol;
- CRP code, delivered to the User in 2 parts: 1st part of CRP Code has been delivered to his/her e-mail address, specified by the Client in the Request or which is listed in his/her InBiz profile in case of later changes and 2nd part of CRP Code is delivered to the User as attachment to the Security Credential Handover Protocol;
- USB Package containing a USB Flash Drive for Electronic Signature and PIN to the USB Flash Drive for Electronic Signature. USB Package is delivered to the User into his/her own hands. The Certificate is generated on the USB Flash Drive for Electronic Signature after Certificate Holder's login to the Bancaidentity Portal. Only after generating Certificates on the USB Flash Drive for Electronic Signature the User can log in to the Portal and execute Authorization of the transactions in the Portal by inputting PIN to the USB Flash Drive for Electronic Signature.

4.6.6 In case the User is a User of more Holdings, Security credentials and Security devices are assigned to the User by each Holding separately.

4.6.7 The User is authorized to use the Security credentials in relation to all Connected Accounts and Connected Services of the Holding according to his/her Authorization rights to the Connected Accounts and Connected Services.

4.6.8 The Client and/or the User may anytime request a suspension or cancelling of the InBiz OTP Token or USB Flash Drive for Electronic Signature.

4.6.9 The Bank may without any prior notice suspend Security credentials and Security devices in case of suspition for a misuse or unauthorized use of a Security credential and Security device or due to the reasons of its security. The Bank will inform the Client about the suspension of the Security credential and/or Security device through its Bank's Branches, through the Contact center or through the Portal.

4.6.10 The User is obliged to inform the Bank about any loss/theft/misuse or unauthorized use of a Security credential and/or Security device without undue delay and request their suspension through the Contact Center or Bank's Branches. A Security credential and/or Security device can be blocked also by the User (for himself/herself or in case of Master User/Configurator also for other Users) through the Portal and in case of Certificates through the Bancaidentity Portal in accordance with the procedure included in the Operation Manual.

4.6.11 The Bank accepts requests for suspension of Security credentials and/or Security devices either in its Bank's Branches during working hours of the relevant Bank's Branch or through the Contact center 24x7. The Bank accepts requests for unsuspension of Security credentials and/or Security devices in its Bank's Branches during working hours of the relevant Bank's Branch.

4.6.12 Suspension of a Security credential and/or a Security device doesn´t allow the User to use the Service in relation to the Holding, to which those Security credentials and/or Security devices were assigned.

4.6.13 Until the moment of informing the Bank about the loss/theft/misuse or unauthorized use of a Security credential and/or Security device according to Article 4.6.11

the Client bears every relevant loss and/or damage.

4.6.14 From the moment of informing the Bank about the loss/theft/misuse or unauthorized use of a Security credential and/or Security device according to Article 4.6.11 the Client doesn´t bear any relevant financial impacts, excluding cases, where the Client or the User acted in a fraudulent way, or the loss/theft/misuse or unauthorized use of a Security credential and/or Security device has been caused by an intentional unfulfillment of one or more obligations according the article 7.1 Terms and conditions or unfulfillment of one or more obligations accoring the article 7.1 Terms and conditions as a result of a gross negligence.

4.7 **DATA TRANSFER**

4.7.1 The Portal allows to transfer Data Flows from the Routing Bank to the Servicing Bank.

4.7.2 The Client receives confirmation of Data Flows transmission through the Portal.

4.7.3 Data Flows are delivered to the Servicing bank:

- within 2 hours from their transmission, if the Servicing bank is a Group Bank;
- according to the time limit applicable to the electronic transmission defined by the Servicing bank, if the Servicing bank is not a Group Bank.

4.7.4 Data Flow sent to the Servicing Bank, which is a Group Bank, is being considered as delivered (in case the Client and the Group Bank did not agree otherwise):

- On the day, when it has been sent from the Portal, under condition, it has been sent latest till 12:00 on the same Bank working day;
- On the next Bank working day after it has been sent from the Portal, under condition it has been sent after 12:00 on the Bank working day or on the day not being a Bank working day, if the Servicing Bank doesn´t decide, that also such sent Data Flow is being considered as delivered on the day of its receipt by the Servicing Bank.

4.7.5 Data Flow sent to the Servicing Bank, not being a Group Bank, is being considered as delivered in time limits agreed between the Client and this Servicing Bank.

4.7.6 For the consideration of fulfillment of the time limit defined in the Article 4.7.3 and 4.7.4, the local time of that Bank is decisive, where the Connected Account included in the DataFlow is being held.

4.7.7 Data Flows must comply with the technical requirements set out in the Operating Manual; if such requirements are not complied with, Data Flows cannot be transmitted through the Inbiz Service.

4.7.8 The Bank is not responsible for the content of Data Flows sent by the Client or by the Routing Bank. The Bank limits itself to transer Data Flows received from the Client or Routing Bank without checking their content and origination.

4.7.9 The Servicing Bank is not obliged to execute any other additional control of the origination of the Data Flow nor documents contained in the Data Flow.

4.8 **EXECUTION AND CANCELLATION OF DATA FLOW INSTRUCTIONS**

4.8.1 Instructions contained in Data Flows transferred via Portal are executed by the Servicing bank in accordance with the provisions of the Agreements governing the accounts or services which such instructions refer to.

4.8.2 Instructions contained in Data Flows must be accurate, complete and unambiguous and if required, authorized via relevant Authorization rules; if such requirements are not met, the execution of the instructions can be suspended or delayed by the Servicing or Routing bank until receipt of the necessary corrections or supplements from the Client.

4.8.3 Any errors or delays in the execution of an instruction given by the Client through the Inbiz Service are governed by the provisions of the Agreement relating to the account or the service which the instructions refer to. The Bank is not liable for the execution or failure to execute an instruction contained in the Data Flow, unless the Bank is the Servicing Bank.

4.8.4 Client takes into account, that Group Banks are subject to laws and regulations (such as those concerning anti-money laundering, anti-terrorism or embargoes) and measures issued by supervisory authorities and judicial authorities in accordance with such laws and regulations; Group Banks are therefore not liable for any consequences arising from their compliance with such laws, regulations or measures and, in particular, are not liable if for that reason is not possible to execute certain instructions of the Client, contained in the Data Flows.

4.9 **STORAGE OF DATA FILES**

4.9.1 The Bank is obligated to store copies of Data Flows sent or received by the Client through the InBiz Service.

4.9.2 Data Flows exchanged with the Client via the InBiz Service are stored and archived in an electronic form for 10 years.

4.10 **COMMUNICATION**

4.10.1 Information regarding the functioning of the Inbiz Service (such as the notice of temporary outage of the Inbiz Service) is provided to the Client in the public area of the Portal.

4.10.2 Other communication to the Client concerning the Inbiz Service and those regarding Connected Accounts and Connected Services is provided to the Client in the reserved area of the Portal.

4.10.3 Communication according articles 4.10.1 and 4.10.2 is being considered as an equivalent of paper communication and is being considered as delivered to the Client on the next day after its publishment in the relevant part of the Portal.

4.10.4 The Bank can also ensure communication in accordance with the article 4.10.1 in paper form in case it is required by a special jurisdicition, and to the correspondence address specified by the Client in the recent Request.

4.10.5 Any communication sent by the Client to the Bank in a paper form, must be sent to the Bank´s registered seat or to the Bank´s Branch, which usually ensures the communication with the Client.

4.11 **SERVICE UNAVAILABILITY**

4.11.1 Service operations could anytime be temporarily unavailable, if the Bank considers it unavoidable, for ensuring of the security or proper operations of the Service. Information about the planned unavailability of the Service will be published in the public part of the Portal.

4.11.2 If the Bank considers it unavoidable to execute an immediate interruption of Service operations (e.g. for security reasons etc.), the Bank may execute such interruption without prior notification.

4.11.3 The Service may be unavailable also for "vis-maior" reasons. „Vis-maior" reasons mean any event, which the Bank cannot influence or avoid, e.g. outages, delays or unavailability of phone, electricity or electronic connections, state authorities regulation, measure or decision, limitation based on jurisdiction, strike of the Bank´s personnel etc.

4.11.4 The Bank may anytime temporarily interrupt the Data Flow transfer from security reasons (e.g. fraudulent acting suspection); The Bank is not responsible for any damage which incured or could incure to the Client due to such temporary interruption of the Data Flow transfer.

5 TERMINATION OF THE AGREEMENT

5.1 The Agreement may be terminated by mutual agreement of the Bank and the Client, by notice or by withdrawal in cases stated in article 5.2.2 and 5.3.2 or in other way mentioned in this Article of Terms and Conditions.

5.2 **PRINCIPAL AGREEMENT**

5.2.1 Each of the contractual parties (Bank and Principal Client) is authorized to terminate the Principal Agreement. The Client's Request for Service Termination is also being considered a termination by the Principal Client. The termination period is one month and starts with the first day of the month following the month, in which the written termination has been delivered to the other contractual party. This is not valid, if the Prinicipal Client or User was acting in a fraudulent way, when the Bank may withdraw from the Principal agreement in accordance with the article 5.2.2. of Terms and Conditions.

5.2.2 In case InBiz is included as part of the product and service package to Client's current account and the Client requests a termination of the current account, including products and services included in the current account package, the Agreement on InBiz is also terminated the following Bank Working Day.

5.2.3 The Bank may withdraw from the Principal Agrement in following cases:

a) a justified suspicion occurs, that acting of the Principal Client or User is in contrary with legislation or circumvents legislation or is in contrary with good manners or best practices;

b) the Principal Client or User has repeatedly breached the provisions of Terms and Conditions or the Agreement, or the Principal Client or User has breached the Terms and Conditions or the Agreement materially;

c) there have been such changes in Principal Client´s assets, which jeopardize or may jeopardize the 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 the Principal Client;

e) a petition for bankruptcy or restructuring has been filed against the Principal Client, or bankruptcy or restructuring proceedings have been initiated against the Principal Client;

f) the Principal Client has disagreed with any alterations and/or supplements to Terms and Conditions in a manner specified below;

g) In case mentioned in the Article 5.2.1.

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

5.2.4 By termination of the Agreement the following are automatically revoked:

- Users defined under the Principal Agreement;
- Secondary contracts, if closed, including Users defined relevant to the Secondary contracts;
- Relevant Powers of Attorney, if granted;
- Relevant Approvals, if granted and
- Relevant Bancaidentity Agreement (s), if closed, including all Certificate Holders, relevant to the Principal Agreement.

5.2.5 The Principal Client is obliged to inform about the termination of the Principal Agreement:

- All Users relevant defined under the Principal Agreement;
- All Connected Persons to the Principal Agreement.

5.2.6 The Connected Person is obliged to inform all Users about the termination of the Principal Agreement and Secondary Contract under which the Users have been created without undue delay.

5.3 **SECONDARY AGREEMENT**

5.3.1 Each of the contractual parties (Bank and Connected Person) is authorized to terminate the Secondary Agreement. For a termination of a Connected Person is being considered also his/her Request for Service Termination. The termination period is one month and starts with the first day of the month following the month, in which the written termination has been delivered to the other contractual party. This is not valid, if the Connected Person or User was acting in a fraudulent way, when the Bank may withdraw from the Secondary Agreement in accordance with the article 5.3.2. of Terms and Conditions.

5.3.2 The Secondary Agreement will be terminated also on the day of cancelling of the Approval by the Principal Client.

5.3.3 The Bank may withdraw from the Secondary Agrement in following cases:

a) a justified suspicion occurs, that acting of the Connected Person or User is in contrary with legislation or circumvents legislation or is in contrary with good manners or best practices;

b) if the Connected Person or User has repeatedly breached the provisions of Terms and Conditions or the Agreement, or the Connected Person or User has breached the Terms and Conditions or the Agreement materially;

c) there have been such changes in Connected Person´s assets, which jeopardize or may jeopardize the fulfillment of Connected Person´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 the Connected Person;

e) a petition for bankruptcy or restructuring has been filed against the Connected Person, or bankruptcy or restructuring proceedings have been initiated against the Connected Person;

f) the Connected Person has disagreed with any alterations and/or supplements to Terms and Conditions in a manner specified below;

g) in case mentioned in the Article 5.3.1.

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

5.3.4 By termination of the Agreement the following are automatically revoked:

- Users defined under the Secondary Agreement;
- Relevant Bancaidentity Agreement (s), if closed, including all Certificate Holders, relevant to the Secondary Agreement.

5.3.5 The Connected Person is obliged to inform about the termination of the Secondary Agreement:

- All Users relevant defined under the Secondary Agreement;
- The Principal Client.

5.3.6 In case InBiz is included as part of the product and service package to Client's current account and the Client requests a termination of the current account, including products and services included in the current account package, the Agreement on InBiz is also terminated the following Bank Working Day.

6 CLAIM

6.1 The Client may make a Claim regarding the quality and correctness of the provided Bancaidentity Service in accordance with the Claim Procedure as stated in VUB General Terms and Conditions. The provisions of these Terms and Conditions are in case of discrepancies more powerful than those stated in VUB General Terms and Conditions.

6.2 The Client is obliged to inform the Bank about any mistakes in accounting and other mistakes relevant to the payment services, to claim a request for resolving and delivering all claims in a time limit up to 6 months from their origination in a following way:

- By paper form at any of the Bank´s Branches;
- By phone through the Contact service Kontakt (charged as a local phone call).

6.3 If the Client will not fulfill the obligation to inform the Bank about any mistakes in accounting and other mistakes relevant to the payment services in a time limit up to 6 months from their origination, his claim for the damage liability originated by enforcement of the request for resolving those mistakes after the time limit will expire.

6.4 Any claims relevant to the Connected Accounts, held by other than a Group Bank or Connected Services, offered by other than a Group Bank, must be delivered to the bank or a branch of a foreign bank, where the Client closed the agreement about the Connected Account and/or Connected Service.

6.5 Any claims relevant to the execution or not execution contained in the Data Flows must by delivered to the Servicing Bank, which received the Data Flows.

6.6 Any claims relevant to the Connected Account statements held by a Group Bank or relevant to the Connected Service offered by a Group Bank the Client has to deliver in a paper form in the relevant Group Bank, in a time limit specified in an agreement relevant to the Connected Account or Connected service, starting on the day, when the Group Bank has received the Claim.

7 SECURITY

7.1 In order to prevent unauthorized collection and misuse of the data, which are protected under the Act on Banks and/or 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:

- to log into the Portal only from a trusted/reliable computer, on which the antivirus and antispyware software is regularly updated;
- to check safety of the communication and identity of the web site related to Portal;
- to protect the computer against viruses, harmful codes, and Internet attacks;
- 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;
- not to run/open unknown attachments and links included in spams and e-mails from unknown senders;
- 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.

7.2 When using the Service, the Client agrees that the Bank is entitled to verify User´s identity via Security Credentials in Bank´s requested combination and to ask Client to change his/her Security Credentials.

7.3 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 the Bancaidentity Portal.

7.4 The Portal is a website secured by the SSL protocol with valid (trusted) certificate and the address of the website is: http://ca.intesasanpaolo.com. This certificate makes it possible to verify the authenticity of the Portal directly through the internet browser. In case the internet browser does not show the right website address or it displays any warning about a not trusted certificate, to ensure protection of the Client´s and User´s access, the Bank recommends the User not to use his/her Security Credentials. Non-compliance incident shall be immediately reported to the Contact Centre.

7.5 To ensure the confidentiality of data, which are subject to protection under the Act on Banks and/or the Act on Personal Data Protection, the User is required not to use the Service on publicly accessible computers (e.g. in Internet cafe, at universities, at hotels, etc.). The Bank shall not be liable for misuse of Service when using publicly accessible computers.

7.6 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 User 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.

7.7 The Bank will never request the Client and/or User to:

a) Disclose or enter his/her Security Credentials and/or data protected under the Act on Banks and/or and Act on Personal Data Protection,

b) Disclose any data of and from Security Credentials over the telephone, with the exception of situations when the Client or User has initiated the contact or ask for contact with the Bank via the KONTAKT.

7.8 Any request for entering more data of and from Security Credentials may lead to an attack (phishing, pharming etc.).

7.9 If the Client or Certificate Holder suspects any of the Security Credentials or Security Devices were misused, the Client and/or the Certificate Holder shall forthwith request their suspension at any Bank Branch or via KONTAKT.

7.10 The User has a limited number of consecutive incorrect attempts for entering of the Security Credential. After the limit is used up, the access to the Portal will be automatically locked. The Client can request to unlock the Access to the Portal or to issue a new Security Credential at any Bank Branch, through the Contact Service or through the Portal according to the Operational Manual.

7.11 In the event of a successful login to the Service the number of unsuccessful attempts is nullified.

7.12 Any of the steps executed by the Bank relevant to the issuance or administration of the Security Credentials could be charged according to the actual Pricelist VUB, a.s..

8 BANK´S LIABILITY FOR INBIZ SERVICE

8.1 The Bank is not liable for any damage incurred to the Client as a result of a misuse of Security Credentials and/or Security Devices, if the Client or the User let them use for any reason by a third party, or which were due to the reasons on the Client´s or User´s side allowed to be accessed by a third party. The Bank is not liable for any damage, which could arise by a middle-man step into the running phone connection between the Bank and the Client or the User through the public telephone network. The Bank is not liable for any damage, which could arise by personal presence of any third party during the login to the Service or during the transaction Authorization through the Service. The Bank is not liable for processing and executing of payment operations by a Group Bank or other bank, if the Bank is not a Routing Bank.

8.2 Disclosure of any data of and from Security Credentials and/or Security Devices to any third party or any manipulation with them leading to their disclosure is being considered as a material breach of the Terms and Conditions and the Bank may withdraw from the Agreement according to the Article 5 of these Terms and Conditions.

8.3 The Bank is not liable for any damage incurred to the Client as a result of a failure of the technology equipment provider or due to breach of the contractual agreements between the Client and the information or communication technology provider.

8.4 If any communication channel, through which the Bank is sending any communication to the Client in an agreed way (e-mail, fax), is not protected against breach of its confidentiality, authenticity and integrity by any means nor encryption, the Bank is not liable for any relevant damage which could incurre.

8.5 The Bank is not liable for any damage incurred to the Client during the usage of the Service due to the undelivered, later delivered or corrupted delivery of the Notification due to technical failure, reparation, maintenance, reconstruction or expansion of the public GSM network, or its part, or due to the overflow of the capacity limit.

8.6 Furthermore, the Bank is not liable for any damage incurred to the Client as a result of the Client´s or User´s acts in contrary with the Agreement and/orTerms and Conditions.

8.7 The Bank is liable only for damage caused by itself.

9 FEES

9.1 Fees for the 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..

9.2 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..

9.3 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..

10 JOINT PROVISIONS

10.1 **GOVERNING LAW AND JURISDICTION**

10.1.1 The Agreement and related relationships shall be governed by Slovak law.

10.1.2 Agreement and related documents and all communication between the Bank and the Client/Certficate 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.

10.1.3 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.

10.2 **DELIVERY OF DOCUMENTS**

10.2.1 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.

10.2.2 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.

10.2.3 Documents delivered by a courier service are deemed to be delivered on the third day after their handover.

10.2.4 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.

10.2.5 Documents are deemed to be delivered also if the 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.

10.2.6 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.

10.2.7 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.

10.3 **BANK SECRECY**

10.3.1 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.

10.3.2 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.

10.3.3 The Client and the User both agree with the use of cookies on the websites of InBiz for statistical and safety reasons of the Bank. In case the User does not intend to use the cookies on InBiz websites, it is possible to disable them direcly in the settings of the User's browser. Disabling of cookies can have an impact on the functionality of InBiz.

11 CLIENT'S AND BANK´S REPRESENTATIONS UNDER ACT ON PAYMENT SERVICES

11.1 The Bank and the Client have agreed that following provisions of Act on Payment Services shall not apply on Agreementual 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 pertained.

12 OTHER PROVISIONS

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

12.2 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 receive the document or even if s/he fails to collect 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 Agreementing parties. The termination of the Agreement shall not effect the arbitration clause forming an integral part thereof.

12.3 The data provided by the Bank to the Client based on the Agreement remain valid during the whole existence of Agreementual 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.

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

12.5 These Terms and Conditions are published on Bank Branches and on the Web Site.

12.6 The Bank is entitled to unilaterally alter and/or supplement the 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 the abovementioned alterations/supplements in form of a 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 the 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 on the day the altered and/or supplemented Terms and Conditions take effect.

12.7 On the day these Terms and Conditions take effect the Terms and Conditions from 06/10/2015 expire.

The Terms and Conditions take effect on 01/04/2016.
Všeobecná úverová banka, a.s.