SPECIAL CONDITIONS FOR USAGE OF ELECTRONIC AND MOBILE BANKING FOR PRIVATE INDIVIDUALS, ENTREPRENEURS AND AGRICULTURISTS

I. GENERAL PROVISIONS

1. The rights and obligations of the e-banking/m-banking Users shall be governed by way of these Special Conditions for usage of electronic and mobile banking for private individuals, entrepreneurs and agriculturists (**hereinafter referred to as: the Special Conditions**), Cut-off time plan for payment accounts for private individuals, entrepreneurs and agriculturists, Tariff for general banking services for private individuals and agriculturists, Tariff for general banking services for entrepreneurs (hereinafter referred to as: the Tariffs for general banking services), which are integral parts of the User Framework Contract.
2. E-banking/M-banking system use is a service provided by the Bank to its Clients only, i.e. to the private individuals, entrepreneurs and agriculturists holding an account with the Bank, which includes e-banking/m-banking services.
3. The information in respect of the offer of Electronic Channel products and the services that the User may provide by using certain e-banking/m-banking products is available at the Bank's sub-branches and on its webpage www.unicreditbank.rs
4. For each contracted e-banking/m-banking product, the Bank will enable the User to have access to all necessary information in respect of using the selected product as well as use all services stated in the Request and these Special Conditions.
5. By filing the Request, the Client acknowledges to be conversant and agrees with the provisions of these Special Conditions, accepting them in full.
6. The User is responsible for the accuracy of all information necessary for proper and secure operation of the agreed e-banking/m-banking product furnished to the Bank, and is obliged to notify the Bank of any change thereof (e.g. phone number, mobile phone number and model, e-mail address, etc.).
7. To be able to use certain e-banking products, the User must ensure appropriate computer infrastructure. Technical requirements for using certain products are available on the Bank's webpage www.unicreditbank.rs and/or at the Bank's branch network. The User is obliged, subject to the technical requirements of individual e-banking products, to notify the Bank of the type of equipment the User uses in order to ensure proper operation of the product.
8. These Special Conditions shall govern the conditions for and manners of using the Bank's electronic payment instruments, and the rights, obligations and responsibilities for their contracting and using of private individuals, entrepreneurs and agriculturists **(hereinafter referred to as: the Users),** as private individuals authorised to use electronic payment instruments on behalf of entrepreneurs **(hereinafter referred to as: the End-Users)** and the Bank.
9. The information that the Bank forwards to the User or End-User of an e-banking/m-banking product shall have the same value as the documents sent by mail by the Bank and may replace them.

II. GLOSSARY

Certain terms used herein shall have the following meanings:

1. **User** is private individual, entrepreneur and agriculturist that contracts with the Bank usage of some of the electronic banking/mobile banking products;
2. **End-User (Authorisee)** is a private individual authorised by the User for using a particular e-banking product for and on behalf of the User;
3. **Username** is a unique set of alphanumeric characters constituting one of the elements by which the End-User is identified in the registration process for an e-banking service;
4. **Signatory** is the User/End-User who owns the device storing the electronic authorisation, and which is authorized by the Request that on behalf of the User sign (authorize) payment orders, other instructions and messages from the Bank;
5. **User Manual** is a written document, describing the registration process and the use of e-banking/m-banking products for the User and/or End-User**.**
6. **Unlock Code/Password** is a code/password used to unlock smartcards or USB Flash Drives in the event when a smartcard or USB Flash Drive is locked due to successive entries of a wrong PIN; In case of a locked token it is necessary for the Client to comply with the procedures for submission the locked token LOCK PIN to the Bank, the Bank to comply with the procedures for sending the unlock PIN to the Client in order to unlock the token.
7. **Encryption** is a process transforming information into a format readable only by the intended recipient.
8. **Decryption** is a process by which the recipient makes the encrypted information readable.

9. **Electronic Channels** are means and forms of electronic communication enabling use and/or contracting certain banking and non-banking services without any simultaneous physical presence of the User/End-User and the Bank's employee in the same place, and they include a network of services made available by the Bank to the User: Electronic Banking (online banking, mobile banking, BusinessNet Professional, MultiCash, Halcom), as well as connection through other Electronic Channels made available by the Bank to the User.
10. **Smartcard and USB Flash Drive** are certified cryptographic devices for secure electronic certificate storage**.**
11. **Certificate** is a set of data in electronic form which is attached to or logically associated with an electronic document serving for the e-banking service user identification.
12. **Electronic Signature** is a set of data in electronic form which is attached to or logically associated with an electronic document serving for the signer identification.
13. **Qualified Electronic Signature** is an electronic signature reliably guaranteeing the signer's identity and electronic document integrity and disabling any subsequent denial of responsibility for the contents thereof, and which meets the conditions stipulated in the Electronic Signature Act.
14. **Activation code** – array of letters and numbers that bank delivers to customers in order to activate mobile application or mobile token. Activation code is unique code, for ome time use, and its use is limited by time.
15. **QR code** (Quick Response) Standardized two-dimensional mark, which represent two-dimensional barcode, based on ISO 18004.

III. TYPE AND SCOPE OF SERVICES AND SECURITY SYSTEM

1. Bank provides the Users with the following type of electronic banking:

- Global Web Solution (hereinafter referred to as GWS)- online electronic banking system (**Online banking** for private individuals, **BusinessNet Professional** for entrepreneurs)
- HAL e-bank system for electronic banking (hereinafter: HAL e-bank) for entrepreneurs
- MultiCash system for electronic banking (hereinafter: MultiCash) for entrepreneurs
- Mobile banking - system for electronic banking via mobile telephone (hereinafter: M banking) for private individuals
- SWIFTNET MT101 for entrepreneurs
- E-statement service for entrepreneurs

2. **Online banking** is an electronic way of communication between the User and the Bank, respectively via Internet browser for accessing the Bank's website, which enables him/her fast and efficient implementation of banking services without obligation to go to the Bank's branch. This application uses the one-time password token mechanism to access the system and sign orders. In order to provide the Clients with a high information security level, three levels of protection are used: personal identification, one-time password token identification and SSL encryption.

2.1 **Token** is an electronic device received on initiating the use of the Online banking e-banking tool. The user enters the token PIN code, after which token generates time password that is valid for 30 seconds and is used for log-in to Online Banking application. The user himself defines the PIN code which he/she will use and he/she can change it at any time. Algorithms on which token is functioning are private information.

2.2 **Mobile token** – within M banking application that can be installed on mobile device, there is possibility of using software token – application that after entering PIN code generates one time password which identifies User of direct channel. During activation of Mobile token application, the user will be asked for personal identification as well as activated code after which the User will be enabled to create its own PIN code. In this way, the application allows users to use mobile device/tablet as token.

2.3 **SSL/TLS PROTOCOL** is a 256-bit key Encryption as the industrial standard in secure online communications. It is used by 99% of major web presentations such as banks, companies dealing with online investments, stock-exchange transactions or commerce.

2.4 **Username** is a unique set of alphanumeric characters constituting one of the elements by which the User is identified in the registration process; The Client is presented by personal identification (username) and prove its identity (token), with the help of temporary password generated by token, after which the system access is granted.

The following services are available through Online Banking application:

- access to a bank account via the Bank's site by using the username and password which are generated by token
- realization of payment transactions in domestic payment system and in international payment system by providing the necessary documentation provided by regulations

- internal transfer of funds within personal accounts
- creation of a payment order with execution date in the future ,
- issuing standing orders for payment in domestic payment system
- access to account balance and transactions on all accounts (including loans),
- inquiry into the balance of the account, in real time,
- account balance for debit and credit cards (data, transactions),
- conversion of foreign currencies into dinars at the Bank's buying exchange rate, within personal accounts
- conversion of dinars into foreign currencies at the Bank's selling exchange rate, within personal accounts
- electronically messaging between the User and the Bank,
- Issuing requests remotely (e.g. change the daily limit for issuing the order, add accounts, etc.),
- availability overview of the list of exchange rates,
- delivery notice from the bank if the User determines for this channel of communication
- Receiving useful information (contacts, if necessary, notifications on current offers that are adjusted to the user, various notifications)

3. **BusinessNet Professional** is an online e-banking application and a product of Unicredit Bank. This application uses the one-time password token mechanism to access the system and sign orders. In order to provide the Clients with a high information security level, BUSINESSNET PROFESSIONAL uses three levels of protection: personal identification, one-time password token identification and SSL/TSL encryption.

3.1 **Token** is an electronic device received on initiating the use of the BusinessNet Professional e-banking tool. The user enters the PIN code, after which token generates time password that is valid for 30 seconds and is used to log into BusinessNet Professional application. The user defines the PIN code to use and can change it at any time. Algorithms on which token is functioning are private information.

3.2 **SSL/TLS PROTOCOL** is a 256-bit key Encryption as the industrial standard in secure online communications. It is used by 99% of major web presentations such as banks, companies dealing withonline investments, stock-exchange transactions or commerce.

3.3 **Username** is a unique set of alphanumeric characters constituting one of the elements by which the User is identified in the registration process for the BusinessNet Professional service. The Client is presented by personal identification (username) and prove its identity with the help of temporary password generated by token, after which the system access is granted.

In the domain of payment transactions, the Client may provide two types of authorisations within the BusinessNet Professional application to its End-Users on accounts as follows:

i. In this system "all rights" include the following authorisations:
   a) administration
   b) entry of order
   c) signing the order – signature and the signed daily and transactional limits are directly determined through Request of the Client, and in accordance with technical capabilities of the system
   d) conversion of foreign currency into local currency
   e) review of reports received from the Bank
   f) sending of signed orders to the Bank.

ii. Category "Without right to sign" includes all aforesaid rights of the User/End-Users except the right to sign.

Contracted scope of services can be changed additionally by using already existing security instruments.

4. **HAL e-Bank** is a software product of Halcom Informatika d.d. Ljubljana, named HAL e-bank.,At HAL e-bank, in order to ensure secure e-banking with the Bank , two types of security instruments have been introduced:

4.1 **HALCOM certificate embedded on the smartcard or USB key** is an electronic, identification instrument enabling the User/End-User to work with the User's current accounts opened at the Bank. The End-User rights on the User's current accounts are precisely defined on the E-Banking Application. By using the digital certificate false personation is disabled i.e. reliable authentication of the User/End-User is ensured.

A Qualified Electronic Certificate is an electronic certificate issued by a certification authority in charge of issuing qualified electronic certificates (HALCOM in this case) containing statutory required information. Qualified Electronic Certificates confirm the link between the User's public cryptographic key and the End-User's identity who has signed the electronic document. The Qualified Electronic Certificates and related private cryptographic keys are used for a qualified electronic signature of files or messages and the user authentication. A Qualified Electronic Signature is an electronic signature which meets statutory requirements and which reliably guarantees the signer's identity, electronic document integrity and disables any subsequent denial of responsibility for their contents..
The User accepts the digital certificate as the exclusive verification of its identity when using the HAL e-bank services, without the right to subsequent denial. Smartcards shall be issued with the defined validity of a digital certificate, and following the expiry of deadline, the validity thereof must be renewed. When issuing a new card, the User shall authorize the End-User to work on his/her accounts by sending a new Request.
In the case of revoking-cancelling the rights of usage of a smartcard for certain End-Users, it is necessary to deliver the written Request to the Bank for cancelling the certificate and usage of the HAL e-bank service for the specific End-User**.**

4.2 **WEB Username** enables the User to access the WEB HAL e-bank system (**hereinafter referred to as: WEB e-banking**). This system represents an upgrade of HAL e-bank and serves for the User access via web browsers.
WEB e-b@nking End-Users with authorities to sign orders may remotely sign orders by using web browsers, WEB username and related password, smartcard and smartcard reader.
The End-Users with the right to access WEB e-b@nking, which are authorized to view the statement, may follow the turnover and statement of the User's accounts by using only a web browser, username and password.
WEB Username enables the End-User to access accounts in accordance with the authorities stated in the User's initial Request via the WEB HAL e-bank application.
In the case of revoking-cancelling the right of usage of the WEB Username for the End-User, the User needs to furnish the Bank with the signed Request for revoking-cancelling the right of usage of the WEB Username.
In the case of revoking-cancelling the right of usage of a smartcard for an End-User, the right of usage of the WEB Username shall be automatically terminated if is issued to the person in question. The Request for revoking-cancelling the right of usage should be submitted to the Bank in written form**.**

In the domain of payment transactions the User may provide two types of authorisations within the Hal e-Bank to its End-Users on accounts as follows:

i. In this system "all rights" include the following authorisations:
   a) administration
   b) entry of order
   c) signing the order – signature and the signed daily and transactional limits are directly determined through Request of the Client, and in accordance with technical capabilities of the system
   d) preparation of orders without examination
   e) review of reports received from the Bank
   f) sending of signed orders to the Bank.
ii. Category "Without right to sign" includes all aforesaid rights of the User/End-Users except the right to sign.

Contracted scope of services can be changed additionally by using the already existing security instruments.

5. MultiCash system for e-banking is e-banking software produced by Omikron Systemhouse fromCologne, Germany**.** In order to ensure secure e-banking, MultiCash system is using the following security instruments:

5.1 **BPD file** is a security mechanism in the form of a file stored on a specific data carrier which in combination with the Electronic Signature enables the End-User to work with the

User current accounts of User opened at the Bank. The End-User rights on the User's current accounts are specified in the Request. By using the BPD file and Electronic Signature false personation is disabled, i.e the reliable End-User authentication is ensured.

5.2 **Electronic Signature (ES key pair)** is a security mechanism in the form of a file stored on a specific data carrier. Electronic Signature i.e. ES key pair is created by the User in itsMultiCash application. By using BPD file and the communication code and following creation of the ES key pair for electronic signature (ES key pair), the User is obliged to set up the initial connection with the Bank's server and to send the information in respect of their public key of the ES key pair generated.
The private key of the ES key pair of electronic signature is secured with a secret password entered by the End-User while generating the ES key pair. The password for the ES key pair is known only to the End-User who is the owner of the ES key pairs for signing. During the initial connection, the MultiCash application prints out a document containing a printout of the User's public key (User Initialisation Script) which needs to be signed by the End-User and deliveredto the Bank in order for the End-User's Electronic Signature to be approved for usege on the MultiCash system.
The User shall accept the BPD file and ES key pair (electronic signature) as an exclusive confirmation of its identity when using the MultiCash e-banking system services, without the right of subsequent denial.
Following approval of the Request, the Bank shall issue the BPD file to the End-User, i.e. the person authorised therefor by the User.
If the User wishes to revoke (cancel) the right of usage of the MultiCash system for a specific End-User, it is necessary to submit to the Bank the written Request for cancelling the usage of the MultiCash e-banking system services for that person, thereafter the Bank will cancel the rights to the MultiCash system.

In the domain of payment transactions the User may provide two types of authorisations within the MultiCash to its End-Users on accounts as follows:

i. In this system "all rights" include the following authorisations:
   a) right to communicate with the Bank that implies sending of already signed orders and taking the reports from the Bank
   b) right to sign the order – category of signatures and signed daily and transactional limit are directly determined through Request of the Client, and in accordance with technical capabilities of the system

ii. Category "Without right to sign" includes all aforesaid rights of the User/End-Users except the right to sign.

MultiCash system, technically allows User to administrate rights to other End Users which are not determenated by Request for E-banking activation. Local users administration is fully explained in Users manual. Responsibility for the proper administration of these End Users is entirely at the side of User. The Bank bears no responsibility in the case erroneous setting of these local End users orders as well as for the possible misuse of rights that are granted locally. Contracted scope of services can be changed additionally by using the already existing security instruments.

6. mBanking represents electronic communication between the User and the Bank via an application that is installed on a mobile phone or tablet, which enables him/her quick and efficient implementation of banking services without having obligation to go to Bank's branch UniCredit M Banking applications are predict measures to ensure secure electronic business with the Bank, such as the creation of a PIN code by the User (which is thus known only to him), the necessity of entering personal identification and activation code, while activating applications and creatingits PIN code. The application is copy-protected and protected from instaling it on other phones, as the link and activation code for installing applications can be used only once (once). It is not possible to install the same application which is linked to the same account on two different mobile devices. By downloading application for M banking, software token is installed as well that guarantees complete work safety. The activation code represents a special identification number which serves for activation the service and after that is not usable for further usage.

The following services are available through mBanking application:
- executing of payment orders in domestic payment system
- internal transfer within personal accounts
- inquiry into the balance of the account, in real time
- request for payment at the point of sale
- availability overview of the list of exchange rates
- account balance and transactions on all accounts (including loans)
- account balance for debit and credit cards (data, transactions),
- conversion of foreign currencies into dinars at the Bank's buying exchange rate,

- receiving useful information (information on current offers, various notifications)
- setup the application (change of PIN code, language, font, etc.)
- as well as any additional services that the Bank will develop within the mobile banking application, about which customers will be informed via agreed channels of communication

7. mBusiness represents electronic communication between the User and the Bank via an application that is installed on a mobile phone or tablet, which enables him/her quick and efficient implementation of banking services without having obligation to go to Bank's branch UniCredit mobile banking applications are predict measures to ensure secure electronic business with the Bank, such as the creation of a PIN code by the User (which is thus known only to him), the necessity of entering personal identification and activation code, while activating applications and creatingits PIN code. The application is copy-protected and protected from instaling it on other phones, as the link and activation code for installing applications can be used only once (once). It is not possible to install the same application which is linked to the same account on two different mobile devices. By downloading mBusiness application for mobile banking, software token is installed as well that guarantees complete work safety. The activation code represents a special identification number which serves for activation the service and after that is not usable for further usage.

The following services are available through M Banking (mBusiness) application:

- executing of payment orders in domestic payment system
- internal transfer within personal accounts
- inquiry into the balance of the account, in real time
- request for payment at the point of sale
- availability overview of the list of exchange rates
- account balance and transactions on all accounts (including loans)
- account balance for debit and credit cards (data, transactions),
- conversion of foreign currencies into dinars at the Bank's buying exchange rate,
- receiving useful information (information on current offers, various notifications)
- setup the application (change of PIN code, language, font, etc.)
- as well as any additional services that the Bank will develop within the mobile banking application, about which customers will be informed via agreed channels of communication

8. SWIFTNET MT101 is a service which enables clients to centralize their payment system. These messages are received via SWIFT messages. Client orders that are sent through these messages, and on the basis of the contract between the Bank and the Client, the Bank receives and executes from Client's account in local or foreign currency in accordance with the received instructions.

9. E-statement is a service of UniCredit Bank that enables the delivery of account statements, as well as other forms of information in regard with business relationship between the User and the Bank, electronically to the e-mail address

IV. CONTRACTING OF USE, OBLIGATIONS AND RESPONSIBILITIES OF CONTRACTING PARTIES

The condition for activation of electronic banking services is that the User opens a current account at the Bank in order to be able to use some of the e-banking payment instrument products. The User may at the same time use one or several e-banking products. To agree on individual e-banking products, the User is obliged to submit to the Bank correctly filled in and signed Request relevant for contracting that direct channel. By certifying the Request for contracting an e-banking product the User acknowledges that is familiar with the Special Conditions, Tariffs for general banking services, as well as with General Business Conditions for private individuals, entrepreneurs and agriculturists –to completely accept them, and that regulates contractual obligation.
The User authorizes the Bank to directly debit his current account for maintenance and safety equipment costs, and whose fees are listed in the Tariffs for general banking services.
The Bank has the right to check data and to collect additional information about the User. Data relating to the User, specified in the Request for contracting products of electronic banking, which the Bank last received, will be considered accurate and are applicable to all other products of electronic banking that the User already uses.
The User must designate one or several End-Users, who will use the agreed e-banking product on behalf of the User. Various types of authorities may be selected for a specific End-User. Any selection, change and revocation of End-User authorities shall be based on furnishing the correctly filled in Request for a single or several e-banking products, submitted to the

Bank by the User as stipulated for each e-banking product. The Bank has the right to check data and to collect additional information about the User. The Bank has right to refuse business cooperation with the User without any explanation. In case of rejection of Request, Bank is not obliged to explain its decision. If the User fails to perform the obligations contained herein, which he/she accepted by signing the Request, the Bank shall reserve the right to unilaterally terminate provision of the e-banking system services by way of the Notice. The User may cancel further usage of the e-banking system in written form only. All debits accrued prior to the day of cancelling the usage of the e-banking system, periodical costs related to the period when the cancellation occurred, as well as costs and interests, if any, arising from debit shall be incurred by the User.

1. GWS - BusinessNet Professional /Online banking/M banking

Contracting Of Use

1.1 The User shall be enabled to use BusinessNet Professional following submission of the signed E-Banking Request, opting for this type of service, legibly filled in and signed by an authorised signer. By way of this Request, the User shall authorise certain private individuals to work in GWS, define account access, and state the type of authorities for the persons by account. The User shall accept the full responsibility for the accuracy of entered information.
1.2 The User shall be enabled to use Online banking/M banking application by submitting a completed and signed Request.
1.3 Bank introduces the User how to access to Onlinebanking/M banking application via Personal identification and PIN code. User selects personal identification and enters into the Request.

Obligations Of Contracting Parties

The User undertakes obligation that he/she will while working with the GWS/M banking system of electronic banking, fully comply with the applicable laws and instructions for use for this software product.The User is obliged to keep and shall cause the End-User to safeguard the token and keep the PIN code confidential in order to prevent them from coming in possession of other party. if User or End-User suspects or finds out that someone revealed its PIN code, it is recommendable to change PINcode.. It may be changed at any time as described in the Instructions for Use.
The User of M Banking application declares that he is familiar with the fact that it is obliged to keep the PIN code, and that the application will be blocked after the input of three incorrect PIN codes, as well as that the Bank is not responsible for this case.
For protection, the User of M banking application shall, at regular intervals, change the PIN code and it is also mandatory if he/she suspects or finds out that someone revealed his PIN code. The user can change the PIN code at any time, as described in the user manual.
The User is responsible for all damages resulting from loss, unauthorized or improper use of token / M Banking application.
The User shall be responsible for the accuracy of all information furnished to the Bank and is obliged to report any change therein. If the Bank independentlyfinds out that the User/End-User information are inaccurate or changed, it may cancel further usage of the GWS services, with a subsequent notice to the User.
The User is obliged to provide a licensed, properly configured operating system on the computers which will be used for the services of UniCredit e-Banking. If a User after commencement of the usage of UniCredit e-Banking, on the same computer uses unlicensed, unadjusted or untested applications, the Bank is not responsible for non-orders and any other possible adverse consequences of the User.
The User is required to provide the appropriate mobile device that is able to support the M baking and M token application, if he/she wants to arrange this service. If User does not provide a suitable mobile device, he/she will not be able to use the service, and all the responsibility and all the costs bears alone.
The User cannot use Token – hardware device and Mobile token at the same time. In accordance with the specified, he/she must choose one of these two options in Request. If the User uses Token – hardware device, and wants to use Mobile token and fulfil conditions from the previous paragraph. He/she is obliged to return Token – hardware device to the Bank or to pay fee in the case of the lost Token – hardware device.

2. HAL e-bank

Contracting Of Usage

In order to activate the HAL e-bank service, depending of the level of the service, the User shall deliver to the Bank the following filled in and signed documents:

i. Request for E-Banking, opting for this type of service, with whichthe User authorises certain private individuals – End-Users, to define account access, and states the type of authorities for End-Users for accounts.

ii. General Order Form for issuing qualified personal digital certificates for a entrepreneur
iii. Request for End-User Digital Certificate (each private individual for which the smartcard issuance is applied for).
iv. Digital Certificate Validation Confirmation, personally signed by the User (authorised person), who is at the same time the certificate owner (in the Request, it is necessary to add the number of the certificate embedded in the smartcard registered under the name of the End-User who is the owner of the digital certificate next to the name of the authorised person).
v. Copy of the User's identity card i.e. the statement that the End-User's personal information furnished by the User are accurate

If the Client is already User of HAL e-bank electronic banking products through another commercial bank, he/she shall submit to the Bank the documents listed under numbers i., iv. and v. in the previous paragraph. Digital certificate on the smart card is not transferable and is on the name of the End-user.
Based on the aproved Request for E-banking and General order form, Smart cards will be delivered to User by Halcom AD in their premises or via post service.The User can get its Smart card in the premises of the Bank, only in the case when qualified certificate is not at stake.

On the basis of aproved Request for E-Banking for WEB user name for certain End-User, Bank will deliver WEB user name and WEB password to End-User or to other person authorized by User.

Obligations and Responsibilities Of Contracting Parties

The User undertakes the obligation that he/she will while working with the HAL e-bank system, fully comply with the applicable laws and instructions for usage of this software product.
The User is obliged to safeguard and shall cause the End-User to safeguard smartcards as well as to keep the PIN confidential in order to prevent them from coming in possession of other party. If End-User suspects or finds out that someone revealed its PIN code, it is recommendable to change PINcode. It may be changed at any time as described in the Instructions for Use.

The User/End-User is obliged to safeguard the PUK code, with which is possible to unblocki a smartcard and enter a new PIN code in the case it is blocked following three unsuccessful entries of the PIN codeIn the case of loss of the PUK code, itis impossible to unlock the blocked card and issue a new one The Bank shall not be responsible therefor.
The User shall incur the full damage due to any loss, unauthorised or inadequate use of the card.
The Client shall be responsible for the accuracy of all information furnished to the Bank and is obliged to report any change therein.
Any copying of the Digital Certificate is prohibited. Any damage due to copying or attempted of copying shall be incurred by the Client.
The User is obliged, on the computers where he/she uses the HAL e-bank services, to provide a licenced, properly configured operating system (minimum Windows 7 and up in case of the single user version of HAL e-bank). If the Client, following the initial use of the HAL e-bank services, uses on the same computer any non-licenced, non-configured or untested applications, the Bank shall not be responsible for any failure in execution of orders or other consequences, if any.
Users who have ordered the installation and training for HAL e-bank at their business premises following receipt of the Bank's notice that conditions have been created for the installation of the HAL e-bank system, are obliged within 15 days to arrange the software installation by phone or by email to: e-banking@unicreditgroup.rs or by calling the technical support on: (+381 11) 3021 333. The Users who have the HAL e-bank package for independent installation, after receipt of the Bank's notice, are obliged within 30 days of the notice to take over the HAL e-bank package at any of UniCredit Bank's branches.
If the User abandons the usage of the HAL e-bank service prior to the completed implementation of the system itself, following the notice by the Bank that the technical conditions have been created for implementation of some of the electronic services, as described in detail in the wording hereof, the Bank may charge the User fees regarding the installation processin accordance with the Tariff for general banking services. The Bank is entitled, and the User agrees, to retain the assets it collected at the time of filing the Request.

3. MultiCash

Contracting Of Usage

In order to activate this e-banking service, the User is obliged to deliver to the Bank the following filled in and signed documents:

i. Request for E-Banking, by which the User is determined for this type of e-banking service and lists End-User authorised for working therein, as well as the accounts they will have access.
ii. Copy of the User's identity card i.e. the statement that the End-User's personal information delivered by the User are accurate

Obligations and Responsibilities of Contracting Parties

The User undertakes obligation that he/she will while working with the MultiCash e-banking system, fully comply with the applicable laws and instructions for usage of this software product. The User is obliged to safeguard and shall cause the End-User to safeguard the Electronic Signature and the Electronic Signature password as well as the password to access the MultiCash application and the password for communication with the Bank to prevent them from coming in possession of other party. If User suspects or finds out that someone revealed one of the passwords, it is recommendable to change password. It may be changed at any time as described in the Instructions for Usage of the MultiCash software.

The User shall incur all the damage due to any loss, unauthorised or inadequate usage of security instruments: the BPD file and Electronic Signature.
The User is obliged, while using the MultiCash services, to comply with the Rules and abide by the User Instructions, which are an integral part of the MultiCash programme.
The User shall be responsible for the accuracy of all information delivered to the Bank and is obliged to report any change therein.
Any copying of the Electronic Signature and BPD file is prohibited. Any damage due to copying or attempted of copying shall be incurred by the Client.
The User needs to provide on the computers where the MultiCash services will be used a licenced, properly configured operating system (minimum Windows 2000 Service pack III). If the User, following the initial use of the MultiCash services, uses on the same computer any non-licenced, non-configured or untested applications, the Bank shall not be responsible for any failure in execution of orders or other consequences, if any.
The Users who have ordered the installation and training for MultiCash at their business premises following receipt of the Bank's notice that conditions have been created for the installation of the MultiCash system are obliged within 15 days to arrange the software installation by phone or by email to: e-banking@unicreditgroup.rs or by calling the technical support on: (+381 11) 3021 333.
If the User abandons the use of the MultiCash system service prior to the completed implementation of the system itself, following the notice by the Bank that the technical conditions have been created for implementation of some of the electronic services, as described in detail in the wording hereof, the Bank may charge the User fees regarding the installation process in accordance with the Tariff for general banking services. The Bank is entitled, and the User agrees, to retain the assets it collected at the time of filing the Request.

4. MT101

Contracting Of Usage

In order to activate this e-banking service, the User is obliged to deliver to the Bank filled in and signed Authorisation to Execute MT101 Messages. The User, an international client, may also activate this service directly through Bank Austria by signing the document entitled Unique Service Level Agreement for MT101 only.
The Bank is authorised to refuse completion of MT101if with the required SWIFT user from whose SWIFT address MT101 is initiated cannot be approved by the RMA (Relationship Management Application).

5. E- excerpt service

Contracting Of Usage
The User gets the ability to use E-statement service by submitting an appropriate Request, and which defines the email address to which the Bank will carry out account statements and other information regarding the business relationship between the User and the Bank.

Bank's responsibility

The Bank is obliged to make computer-based records of all User's actions. Computer-based records shall be retained in accordance with applicable laws.
The Bank shall reserve the right to change the content or part of the content of the GWS / HAL e-bank / MultiCash/ M banking system available to the User, without a prior notice. Any change of the content or part of the content of GWS / HAL e-bank / MultiCash/ M banking will be communicated by the Bank to the User and the instructions will be delivered accordingly.
The Bank shall not be accountable for any interferences in telecommunications and teletransmission services offered by third parties, as well as for any errors or damage arisen therefrom.
The Bank is obliged to deliver to the User the Instructions for Use of GWS / HAL e-bank / MultiCash/ M banking system.
The Bank is committed to transmit to User, who is Requesting contracted service M-banking, text message with the download and install applications and activation code necessary to run

the application. Employees in the branches will show them a way to install the application.
The Bank is committed to notify a user, who has ordered by Request installation and training for usage of MultiCash, and who, within a maximum of 30 days after the Request was initiated, has prepared
the technical requirements for the introduction of MultiCash by the information provided in the documentation submitted, that the technical requirements for the introduction of MultiCash sending messages via e-mail to the email address of the contact person specified in the Request have been met. If the user has not entered a valid e-mail address, the Bank shall notify the User about that on the phone number specified in the Request.

V. EXECUTION OF PAYMENT TRANSACTIONS

1. Any payment transaction initiated via one of electronic banking application is considered to be authorised. The fact that the Bank**,** as the usage of a payment instrument has recorded, , the usage of assets for identification and verification which are accessed by a personalised security instrument, shall be sufficient in order to prove that the User, i.e. End-User, has authorised the payment transaction in question, whereby the User assumes the responsibility for the executed transaction in question. The client is responsible for accuracy of all information in issued payment order.
2. The Bank will, upon receiving a payment order, via the same channel through which the order has been received, deliver to the User a message of successful receipt of the order. The message of successful receipt of a payment order shall not imply that the order will be executed, but only that it has been received by the Bank.
3. The Bank shall execute correct payment orders within timelines set out in the General Conditions for providing payment services to private individuals, entrepreneurs and agriculturists (**hereinafter referred to as: General Conditions for providing payment services)** and the Cut-off time plan, applicable at the time of executing the payment transaction.
4. The payment orders which are sent to the Bank by any of the electronic payment instruments before the execution value date, may be cancelled by the User and/or End-User until the execution date set out in the applicable Cut-off time plan for payment accounts. The payment orders may be cancelled by using the same channel through which are sent to the bank, in accordance with the General Conditions for providing payment services, unless if there is no possibility , where in that case the User may cancel the order by written form at any Bank's-branches.
5. Bank may refuse order execution in accordance with the General Conditions for providing payment services.
6. The Bank retains the right to limit the amount of the payment transaction that the user is realizing through a system of the electronic/mobile banking. Information about the limitation will be available to the user, through the application which he use.
7. The Bank shall not be responsible for any failed execution of a payment transaction or improper execution thereof by electronic instruments, occurring due to incorrectly entered information in the User's i.e. End-User's order.

VI. EXECUTION OF INSTANT PAYMENT TRANSFER AT POINT OF SALE

1. The Bank offers to its customers with whom it has contracted the use of the Mobile Banking service, the possibility of executing domestic payment transactions at the point of sale by using instant transfer. Payers have two ways of initiation of instant transfers :
   a) by presenting payers data through QR code
   b) by downloading data about the merchant from the code

2. The Bank shall, immediately after receiving the authorized instant transfer order, execute it in the shortest possible time if the conditions for execution of the order are fulfilled within the available funds on the account.

3. The Bank shall, immediately after the execution of instant transfer order, provide via a mobile banking message information on the amount and currency of the executed payment request, as well as the reference mark identifying the payment transaction at the point of sale. The Bank shall inform the Payers in the same way in case of refusal of instant transfer.

4. It is not possible to recall instant transfer payment based on the Request for payment at the point of sale. Users have possibility to initiate a refund request based on payment at the point of sale. Upon receipt of the Refund Request from the point of sale at the point of sale, the Bank shall proceed to the execution of all necessary checks whether the payment request at the point of sale has been properly executed. If, on the basis of the preformed checks, it has been established that there is a basis for repayment, the Bank shall initiate a request for a refund to the account of the beneficiary.

VII. DISABLING E-BANKING ACCESS, LOSS AND BLOCKADE OF SECURITY

1. Any loss, theft, suspicion of abuse, or abuse of identification and verification instruments, certificates stored on an identification and verification instrument, or personalised security features, knowledge or suspicion that an unauthorised party revealed personalised security feature, knowledge or suspicion that an unauthorised party has accessed an agreed channel, must be forthwith reported by the User or End-User to the Bank, requesting the e-banking access to be blocked. The report of loss or theft of an identification and verification instrument where the certificate is stored shall be the basis to revoke the certificate. The Bank is obliged to revoke the certificate upon receipt of the report.
2. The Bank will, even without any User's or End-User's report, automatically disable access to an e-banking product if the personalised security feature has been entered unsuccessfully as many times as stated in the User Manual for individual products.
3. The Bank is authorised, without any User's or End-User's report, to disable access to certain or all e-banking products in the following instances:
   a) in case of suspicion of unauthorised use or abuse of identification and verification instruments or personalised security features
   b) if an e-banking product is being used for fraud or abuse.
4. The Bank shall notify the User and End-User beforehand of an intended blocking of access and/or inability to use a particular e-banking service, as well as of the reasons therefor, unless giving such notice is contrary to objectively justifiable security reasons, or against the law. The Bank is not obliged to notify the User and End-User beforehand of blocking the e-banking access in the event of unsuccessful entry of the personalised security feature, or expiry of the certificate stored on the End-User's identification instrument. The notice of inability to use e-banking products or a particular service available through E-banking shall be sent by the Bank to the User and End-User by any other means available.
5. All the payment orders received by the Bank prior to revocation of the certificate or blocking of an e-banking product access, will be executed.
6. The Bank may, upon giving a notice no later than 24 hours beforehand, disable the use of agreed e-banking products in the case of changes and upgrades to the Bank's information system, including its information security system, or in the event of changes and upgrades to e-banking products. The notice of a temporary inability to use e-banking products shall be sent by the Bank to the User and End-User through the same e-banking product, by publishing it on the Bank's webpage or by other means available.

GWS - BusinessNet Professional and Online banking/Mobile banking

The User/End-User is obliged to report any loss or theft of the token or mobile device on which is installed M banking application without delay to inform the Bank on (+381 11) 3021 333 or by e-mail on: e-banking@unicreditgroup.rs .
On the basis of the received notification of the token loss or theft, or mobile device on which M banking application is installed, any further usage of the token or M banking application for disposing of assets on the accounts at the Bank, will be disabled upon receipt of the notice during the working hours of the Technical Support, namely Monday-Friday, 09.00h - 17.00h.
In addition, the User is obliged within 2 working days in written form to notify i.e. to confirm to the Bank, the token loss or theft, or mobile device on which is installed M banking application. The permanently blocked token may not be unblocked, and the costs of re-issuance of the token shall be incurred by the User. The User will incur consequences of abuse, if any, of the lost or stolen token, or mobile device on which is installed M banking application.
In the case if the User three times in a row enters wrong PIN while using M banking application, the software token will be automatically blocked, and it is necessary for the User to reinstall M banking application in the branch of the Bank.

HAL e-bank system

The User/End-User is obliged to report any loss or theft of the smartcard without delay to the Bank on (+381 11) 3021 333 or by e-mail to: e-banking@unicreditgroup.rs. On the basis of the received notice of the card/certificate loss or theft, any further use of the smartcard for disposing of assets in the accounts held with the Bank will be disabled upon receipt of the notice during the working hours of the Technical Support, namely Monday-Friday, 09.00h - 17.00h.
In addition, the User is obliged within 2 working days in written form to notify i.e. to confirm to the Bank, in writing, the card loss or theft. The permanently blocked card may not be unblocked, and the costs of re-issuance of the card shall be incurred by the User.
The User will incur consequences of abuse, if any, of the lost or stolen card. If the User blocks the smartcard, unblocking is possible if the User has information on the PUK and PIN codes, which they were handed together with the smartcard for the HAL e-bank usage and any costs arisen therefrom shall be incurred by the User.
The Bank, on the written request of the User's authorised person, submits the request at Halcom AD Beograd for issuing new smart card with Digital Certificate.

VIII. SAFEGUARDING OF PERSONAL AND CONFIDENTIAL INFORMATION

The Bank shall keep confidential all information, facts and circumstances of individual Users at its disposal. The User agrees that all information furnished to the Bank or learned by the Bank during entering and performing the contract may be processed and used by the Bank to create a client base, prevent money laundering and terrorist financing, search and detect payment operations frauds, resolve complaints and make entries into documentation, which occurs with a view to exercising the rights and performing the obligations under the Contract. The Bank is obliged to treat the foregoing information in accordance with its legal obligation to keep confidential any information it has learned while doing business with the User, ensuring the confidential treatment thereof and the full protection of the banking secret by all parties who will be allowed access to protected information, as well as the usage thereof for legal purposes.

IX. FINAL PROVISIONS

User agrees that the Bank is entitled to change the Special Conditions and Tariff for general banking services, with Bank's obligation to deliver to the User in written form a proposal for amending no later than two months prior to the proposed effective date thereof. The User may agree that the proposed amendments produce legal effect prior to the proposed effective date. It shall be deemed that the User has agreed to the proposed amendments if, before the effective date, User has not notified the Bank that he/she disagrees with the proposal.
If User disagrees with the proposed amendments, prior to the effective date thereof, the client is allowed to terminate the usage of electronic banking service free of charge.

In the case of a dispute, the Court shall have jurisdiction.
For anything not provided in these Special Condititons, it will be applied General Conditions for providing payment services and the General Business Conditions for private individuals, entrepreneurs and agriculturist - general part.
These Special Conditions are made in accordance with the Law on payment services and regulations of the Republic of Serbia and are available on the Bank's web site www.unicreditbank.rs, as well as in all branches of the Bank.
These Special Conditions are made in Serbian and English language. In case of conflict between the Serbian and English versions, the Serbian version shall prevail. The Bank will act in good faith when executing orders and will do everything in its power to protect the interests of users in each case.
The provisions of these Special Conditions shall enter into force upon date of its adoption by the Board of Directors, and shall apply from 1th of April 2019.

Supervisory board of UniCredit Bank Srbija JSC Belgrade