Documents of banking products of UniCredit Bank

How to do it?

Clicking on the selected document in the interactive content will take you to the specific document you are interested in.

Tip

If you want to print any document, make sure you have only the pages that are relevant to you selected in the print settings.

UniCredit Bank

Overview of electronic banking services and parameters

Table of contents

* Products and Services can be provided to other than the target segment only based on an individual agreement between the Bank and the Client.

EB Services are provided in accordance with the relevant Price List of banking services for the client target segment.

This overview of electronic banking services and parameters is valid since 1 May 2024.

User's Standard Settings

Electronic banking products	Online Banking Smart Banking
Associated accounts /	All open accounts and products held by the Bank for the Client
Authorisation level	All authorisations active; signature authorisation for active operations
	For minor Users under 8 years of age, only passive access without signature authorisation for active operations
Daily limit	EUR 20,000 for Online Banking and Smart Banking; For foreign currency accounts: CAD 28,000, CHF 24,000, CZK 500,000, GBP 16,000, HUF 6,000,000, USD 25,000 EUR 40 for Online Banking and Smart Banking for a minor User under 18 years of age; For foreign currency accounts: CAD 56, CHF 48, CZK 1,000, GBP 32, HUF 12,000, USD 50

Online Banking – Parameters

Minimum technical requirements	
Operating system	MS Windows Vista, 7, MaC OS X or higher
	Android 1.x.x or higher, iOS, RIM, Symbian*
Internet browser	Microsoft Edge 13 or higher, Microsoft IE 11 or higher, Mozilla Firefox 6.8 or higher, Google Chrome 5.1 or higher, Safari 7.0 or higher, Opera 2.4 or higher
JavaScript, Cookies	Enabled
Other	Adobe Acrobat Reader 6.0 or higher
Security tools	
Security	User ID is assigned by the Bank
	Security key **1. Smart Key (Online Banking Key)** Smart Key is used to log in and sign transactions, contracts and other documentation using push notifications and subsequent confirmation with a security PIN if the client is online. Alternatively, for logging in and signing transactions using a QR code and subsequent confirmation with a one-time code generated in the Smart Key app, if the client is without an internet connection. Access to the app is protected by: a) PIN code, which the User chooses when creating his/her client profile in the electronic environment or in the app; b) Fingerprint (for mobile phones running iOS or Android that support this technology); c) Face ID (only for iPhones running iOS). If one of the biometric methods is used, the User stores fingerprints (Touch ID on iOS or Finger print on Android) / Face ID in the relevant section of the phone. The use of biometric methods is managed by the client, the methods are part of the mobile device, the Bank does not download or store fingerprints / Face ID. In the Smart Key app, the User enables fingerprint/Face ID identification, which can be used the next time they log in. Fingerprint/Face ID can be turned off in the app settings. Even with fingerprint/Face ID login enabled, PIN login can be selected. Fingerprint/Face ID authentication takes place on the User's mobile phone. The Smart Key app must be activated before use. Activation of the Smart Key and Smart Banking takes place simultaneously as part of a unified activation process after opening the app the Activate button. Activation requires two factors: a) Username, which can be chosen by the client (e-mail is also allowed). The Username must be unique in the system. The User may change the Username at any time. b) PIN code (security PIN code), which is identical for both Smart Banking and Smart Key. The PIN code is chosen by the client when creating his/her client profile in the electronic environment or subsequently in the app. Changing the PIN in the app: The User can change the PIN code at any time in the app under Settings –Security – Change PIN code. If the User does not remember the PIN code or does not have it (existing client without digital identity), the PIN reset function is used to obtain a new PIN code. In this case, the User must be authenticated by one of the following methods: a) Authentication by a document, requiring: • scan of identification document (ID card for residents, passport for foreigners); • selfie photos of the face. After data verification and acceptance of the control code sent to the verified phone number, the Bank will allow the client to create a new PIN code, which will be valid for both Smart Banking and Smart Key. b) Authentication through a call centre or branch, which requires identification by the Password to communicate with the Bank. After successful authentication, the User receives a control code, which they enter during the PIN reset process. Upon successful completion of the process, the Bank will allow the User to create a new PIN. This procedure is intended primarily for non-residents and resident Users who have not been correctly authenticated despite repeated attempts to identify them according to point (a). As part of the activation process or at any later time, the User can also activate the biometric method in the settings (fingerprint – for mobile phones with iOS or Android operating system supporting this technology, Face ID – only for mobile phones with iOS operating system). The use of biometric methods is managed by the User The methods are part of the mobile device. The Bank does not download or store fingerprints and Face ID.

* For optimised display on a mobile phone

Online Banking – Parameters

Security	**2. SMS key** The code for logging in / signing the payment is sent by the Bank to the mobile phone designated by the User in the form of an SMS. The initiation password for the first login is sent by the Bank to the e-mail address specified by the User **3. Security key (calculator)** Code generated by the security key. Access to the security key is protected by a PIN code chosen by the User. In the event of three consecutive unsuccessful attempts to enter the correct PIN code, the security key will be blocked. **Unblocking a blocked User/security key** In the event of three consecutive unsuccessful attempts to enter the code from the security key, the Online Banking app will be blocked. The User can request unblocking by phone via the Client Line (after successful identification) or directly at the Bank's branch, or can use Face ID if the Bank allows it.
	User identification to communicate with the Bank by phone Identification by the operator after communicating the Password to communicate with the Bank by phone or other data as required by the Bank. The Password to communicate with the Bank is chosen by the User in the branch or when creating his/her client profile in the electronic environment.
Limits	
Daily limit	Recommended value EUR 20,000
Support	
Client Line	**+421 2 6920 2090**
	Opening hours (except holidays) 7:00 a.m. – 10:00 p.m.
Website	https://www.unicreditbank.sk/sk/obcania/digital/online-banking.html
Client Line standard activities	• Information on entering/changing/cancelling the client's orders • Blocking/unblocking the Security key, the User • Accepting the client's problem, solution and announcement of the result • Communication with clients via e-mails, apps
Other	
Export to CSV, XLS format	The Bank reserves the right to change the format of exported data.
Maximum number of accounts	Clients with a total of 300 associated accounts can be selected at login.
Maximum number of notifications	One User can place a maximum of 200 orders for sending information of one type.
Availability	On a 24/7 basis, except for technical closing

Online Banking – Services

Title	Description	Time limit
Associated accounts and products		
Current accounts	In all currencies	15 months
Overview of accounts and transactions	At least 15 months retroactively from the present banking day	
Payment cards	Debit, credit and prepaid	15 months
Informative overview of debit, credit and prepaid cards and card transactions. *Note:* • *The holder of the main card may have a main credit card attached, additional cards linked to the main card must be requested from the branch. Holders of additional cards have assigned only their additional credit cards.* • *Debit card transactions carried out abroad can result in an exchange difference between entries on the account and entries displayed in the card history.* • *The credit card accounting balance after the settlement of transactions of prior banking day.* • *If you need to know the available credit card balance, please call the Client Line on +421 2 6920 2090.*		
Savings accounts	With notice period, without notice period	15 months
Overview of accounts and transactions	At least 15 months retroactively from the present banking day	
Securities accounts	Pioneer products	15 months
Overview of accounts and transactions	At least 15 months retroactively from the present banking day	
Credit accounts	Retail mortgages and consumer credit	15 months
Overview of accounts and transactions	At least 15 months retroactively from the present banking day	
Information about accounts and products		
Balance	Accounting and available balance of current accounts, accounting balance of other accounts	
The available balance includes the overdraft on the account and transactions not settled. This type of balance is shown on the payer's account when the payment order is placed.		
Transaction history	Information about transactions on accounts	15 months
According to User specified filtering criteria, it is possible to display up to 1,000 transaction history records and export them in a predefined format to csv, xls formats.		
Overview of payments	Payments and their statuses before display in history of transactions	
Payments of a specific type (domestic/cross-border) are displayed in the payment overview and marked with a status according to the processing stage of the payment order.		
Statements and documents in PDF	PDF documents do not have the same requirements as the Bank's printed documents	15 months
Possibility of displaying and saving PDF documents related to the client's account and credit card statements. The PDF credit card statement is only available to the main credit card holder.		
Notifications	Setting up e-mail or SMS messages with banking information	
Orders are placed/cancelled by the User, SMS charges are paid by the account owner. The Bank reserves the rights to change the content and structure of information included in the message.		
Balance, term deposit	SMS, e-mail	
Transactions	SMS, e-mail, one-time on deposit / recurring on credit / debit	
Card transaction	SMS, e-mail, at the time of authorisation	

Online Banking – Services

Title	Description	Time limit
	Active operations	
Credit card repayment	SEPA payment order with predefined data for repayment of a credit card issued by UniCredit Bank. Maturity on a specified banking day. Debiting funds on the due date. Crediting the credit card account on the due date.	By 9:30 p.m.
Cancellation of a SEPA payment	Optional cancellation of a domestic payment in EUR, provided that the payment is not yet settled by the Bank.	By the moment of settlement
SEPA	**SEPA Credit Transfer**	
SEPA Credit Transfer from an account in EUR	Sending a payment order from an account in EUR to a bank in Slovakia or in an EEA country, Switzerland, San Marino and Monaco; with crediting a bank in Slovakia and EEA on the next banking day, a bank in Switzerland, San Marino and Monaco on the next following banking day.	By 9:30 p.m.
Accelerated SEPA Credit Transfer from an account in EUR	Sending a payment order for an accelerated payment from an account in EUR to a bank in Slovakia; with crediting the beneficiary's bank on the day of debiting the payer's bank.	By 4:00 p.m.
SEPA Credit Transfer from an account in foreign currency	Sending a payment order from an account in foreign currency to a bank in Slovakia or in an EEA country, Switzerland, San Marino and Monaco; with crediting a bank in Slovakia and EEA on the next banking day, a bank in Switzerland, San Marino and Monaco on the next following banking day.	By 3:00 p.m.
Accelerated SEPA Credit Transfer from an account in foreign currency	Sending a payment order for an accelerated payment from an account in foreign currency to a bank in Slovakia; with crediting the beneficiary's bank on the day of debiting the payer's bank.	By 3:00 p.m.
Cross-border and conversion payments	**Payment orders in foreign currency or from accounts denominated in foreign currency**	
Standard payment	Sending a payment order: a) in EUR from an account in EUR or in foreign currency to non-EEA countries, with crediting the beneficiary's bank on the next following banking day following the day on which the payer's account is debited b) in another currency from an account in EUR or foreign currency to EEA and non-EEA countries, with crediting the beneficiary's bank on the next following banking day after the day of debiting the payer's account.	By 3:00 p.m.
Urgent payment	Sending a payment order: a) in EUR from an account in EUR or in foreign currency to non-EEA countries, with crediting the beneficiary's bank on the banking day following the day on which the payer's account is debited b) in another currency from an account in EUR or foreign currency to EEA and non-EEA countries, with crediting the beneficiary's bank on the banking day following the day of debiting the payer's account.	By 1:00 p.m.
Conversion to a domestic bank	Sending a payment order in EUR from an account in foreign currency and with crediting the beneficiary's bank on the banking day following the day on which the payer's account is debited.	By 3:00 p.m.
Conversion within the Bank	Sending a foreign payment order between accounts within UniCredit Bank in foreign currency or EUR from/to a foreign currency account with maturity on a specified banking day, with the funds debited and the beneficiary's account credited on that day.	By 3:00 p.m.
Conversion between own accounts	Sending a payment order with conversion between own accounts held with UniCredit Bank with maturity on a specified banking day, with funds debited and credited to the client's account on that day.	By 3:00 p.m.

Online Banking – Services

Title	Description	Time limit
Direct Debit	**Direct Debit mandate**	
SEPA Direct Debit mandate	Entering/changing/cancelling SEPA Direct Debit mandate with effect from the next following banking day. When delivered to the bank on a non-banking day, entering, changing and cancelling the Direct Debit mandate will be valid on the next following banking day.	9:30 p.m. D-2
Request for refusal of SEPA Direct Debit	Request for refusal (non-execution) of an expected SEPA Direct Debit. The bank will not perform the Direct Debit, as instructed by the submitted parameters The beneficiary's bank will be notified that the payer refused to make the payment.	4:00 p.m. D-1
Request for refund of SEPA Direct Debit	Request for refund of financial funds from a settled SEPA Direct Debit. The Bank will return the withdrawn funds to the payer and request them from the beneficiary's bank.	4:00 p.m. D-1
Standing order	**Domestic (transfer of a fixed amount or an amount in excess of a fixed account balance), cross-border**	**By 9:30 p.m.**
SEPA Standing Payment Order – placing	The **"Validity from"** field must indicate at least 1 working day before the date of the first settlement of the standing order. If a due date of a regular payment under the standing order falls upon a non-banking day, then the payment is made as instructed by the client (on the preceding or the following banking day).	By 9:30 p.m. D-2
SEPA Standing Payment Order – changing/cancelling	If the change/cancellation date is identical with the banking day for a regular payment under an existing standing order, then the change/cancellation of the standing order will become valid from the following banking day. This shall not apply to standing orders with a 1 day period, i.e., a one-day standing order can be changed/cancelled on the banking day scheduled for the regular payment.	By 9:30 p.m. D-2
Cross-Border Standing Payment Order – placing	The **"Validity from"** field must indicate at least 1 working day before the date of the first settlement of the standing order. If a due date of a regular payment under the standing order falls upon a non-banking day, then the payment is made on the following banking day.	By 9:30 p.m. D-2
Cross-Border Standing Payment Order – changing/cancelling	If the change/cancellation date is identical with the banking day for a regular payment under an existing standing order, then the change/cancellation of the standing order will become valid from the following banking day. This shall not apply to standing orders with a 1 day period, i.e., a one-day standing order can be changed/cancelled on the banking day scheduled for the regular payment.	By 9:30 p.m. D-2
Term deposit	**One-off, recurring**	**By 9:30 p.m.**
Term deposit – opening	A term deposit can be opened no earlier than the beginning of the next banking day after the current banking day. The minimum amount of the term deposit is determined according to the Bank's interest rate tables.	By 9:30 p.m.
Templates, beneficiaries	**SEPA, Cross-Border**	
Payment order templates	Possibility of saving details of SEPA or cross-border payment in a template for later use.	
Beneficiaries	Possibility of saving a record of a bank link to a SEPA or cross-border trading partner for later use.	
	Other	
Mail	**Possibility of sending/receiving messages between the bank and the User**	
Requests	**Requests for the provision of new products, changes to products and services**	
Payment card activation request	The status of the card in the request is always indicated as **"Inactive"** for processing purposes. The current status of the card can be found in the Card Overview section. The request will be processed on the next working day no later than 8:00 p.m. and the User will be informed about the processing of the request by SMS to the specified phone number.	

Online Banking – Services

Title	Description	Time limit
Direct Debit	**Direct Debit mandate**	
Transfer from credit card	Transfer of funds from the credit card of the credit line holder in the amount of a maximum of 30% of the credit line granted by the Bank within one Card Cycle.	9:00 p.m. D-1
PDF account statement	Change in the way account statements are sent. Completing and submitting the form to the Bank cancels the previous method of sending statements	
Consumer credit application	Completing and submitting the form to the Bank does not automatically entitle the client to a credit in the amount requested. The client will be contacted by a Bank employee in the following days.	
Smart Key	Request for online change (without visiting a branch) of the authorisation tool from the original security (SMS, token to Smart Key. The request will be processed in the next few days and the User will be informed by SMS to the phone number provided.	
Effective account	The request will be forwarded to the selected branch of the Bank for processing, which will ensure the opening of the account and preparation of all contractual documents for signature and will contact the User.	
StickAir	After verification, the request will be processed and the card will be sent to the selected bank branch, which will ensure the preparation of all contractual documents for signature and will contact the User.	
PDF statement – prepaid card	Change in the way card statements are sent. Completing and submitting the form to the Bank cancels the previous method of sending statements	
PDF statements – credit card	Change in the way card statements are sent. Completing and submitting the form to the Bank cancels the previous method of sending statements	
Discrete data for information and services provided via the Client Line	Replaces the Control Data for blocking/unblocking the security tool. After identification, the account owner is entitled to draw passive operations within the scope defined by the Bank, the User can obtain information about the electronic banking settings.	
Transaction authorisations	**Method of signing payment orders**	**90 days**
To be signed	All created transactions must contain the User's signature, otherwise the Bank will not process them. A maximum of 10,000 transactions / 1 signature can be authorised. Only a User authorised to sign the transactions has access to transactions to be signed.	Within 90 days of payment/ instruction creation
Custom name of accounts	**Setting custom account naming**	
Map of branches and ATMs	**Displaying UniCredit Bank branches and ATMs**	
In order for the display to work properly, it is necessary to download data to the app via the HTTP protocol, and therefore, upon request of the browser, downloading data via this protocol must be enabled.		

Smart Banking – Parameters

Minimum technical requirements	
App for smartphones	Operating system iOS 12.0 or higher, Android 5.0 or higher
	Free space for app storage min. 50 MB
Internet connection	• Active internet connection via mobile operator data services or Wi-Fi *Note: For security reasons, the Bank does not recommend the use of unsecured public wireless networks. We also recommend turning off your wireless connection when you're not using it.*
Security tools	
Authentication (login) to the app	The Smart Key app must be activated before use. Activation of the Smart Key and Smart Banking takes place simultaneously as part of a unified activation process after opening the app the Activate button. Activation requires two factors: a) Username, which can be chosen by the client (e-mail is also allowed). The User may change the Username at any time. b) PIN code (security PIN code), which is identical for both Smart Banking and Smart Key. The PIN code is chosen by the client when creating his/her client profile in the electronic environment or subsequently in the app. Changing the PIN in the app: The User can change the PIN code at any time in the app under Settings –Security – Change PIN code. If the User does not remember the PIN code or does not have it (existing client without digital identity), the PIN reset function is used to obtain a new PIN code. In this case, the User must be authenticated by one of the following methods: a) Authentication by a document, requiring: • scan of identification document (ID card for residents, passport for foreigners); • selfie photos of the face. After data verification and acceptance of the control code sent to the verified phone number, the Bank will allow the client to create a new PIN code, which will be valid for both Smart Banking and Smart Key. b) Authentication through a call centre or branch, which requires identification by the Password to communicate with the Bank. After successful authentication, the User receives a control code, which they enter during the PIN reset process. Upon successful completion of the process, the Bank will allow the User to create a new PIN. This procedure is intended primarily for non-residents and resident Users who have not been correctly authenticated despite repeated attempts to identify them according to point (a). As part of the activation process or at any later time, the User can also activate the biometric method in the settings (fingerprint – for mobile phones with iOS or Android operating system supporting this technology, Face ID – only for mobile phones with iOS operating system). The use of biometric methods is managed by the User. The methods are part of the mobile device. The Bank does not download or store fingerprints and Face ID. Upon successful completion of the activation process, the client can log in to the Smart Banking app using the selected security method (PIN, fingerprint or Face ID).
Authorisation (signing) of active operations	After clicking on the Confirm/Sign button for a payment, contract, document or any other operation enabled by the Bank, the operation is ready for authorisation. For iOS and Android mobile phones, authorisation is subject to a) Entering a PIN code; b) A selected biometric method in the settings (fingerprint – for mobile phones with iOS or Android operating system supporting this technology, Face ID – only for mobile phones with iOS operating system). In the Smart Banking app, the User enables the fingerprint / Face ID authorisation feature, which can be used for the next payment signature, document or any other transaction enabled by the Bank. The possibility of authorisation using one's own fingerprint / Face ID can be switched off in the app's settings; if fingerprint authorisation is enabled, PIN authorisation is always a possibility. Verification of the User's fingerprints / Face ID takes place on the User's mobile phone, the Bank does not download and store the fingerprints / Face ID. For more information about Smart Key, see Online Banking.
User identification to communicate with the Bank by phone	**1. Via Smart Key** • Username that can be chosen by the client. • Confirmation by PIN or selected biometric method (online). • Confirmation by PIN code or selected biometric method and a code generated by the Smart Key app (offline), which is entered when logging in to Online Banking.

Smart Banking – Parameters

User identification to communicate with the Bank by phone	**2. Via the security key (calculator)** • Username that can be chosen by the client in the Smart Banking / Smart Key app; otherwise the Username is the User ID assigned by the Bank. • Code generated by the security key. **3. Via SMS security key** • Username that can be chosen by the client in the Smart Banking / Smart Key app; otherwise the Username is the User ID assigned by the Bank. • Static security code (assigned by the Bank and changed by the User at first login). **4. Through the Password to communicate with the Bank via the call centre/branch when communicating by phone**
Limits	
Daily limit	Recommended value EUR 20,000
Client Line	**+421 2 6920 2090**
	Opening hours (except holidays) 7:00 a.m. – 10:00 p.m.
Website	https://www.unicreditbank.sk/sk/obcania/digital/smart-banking.html
Client Line standard activities	• Information on entering/changing/cancelling the client's orders • Blocking/unblocking the Security key, the User • Accepting the client's problem, solution and announcement of the result • Communication with clients via e-mails
Other	
Availability	On a 24/7 basis, except for technical closing

Smart Banking – Services

Title	Description	Time limit
Associated accounts and products		
Current accounts	In all currencies	12 months
Overview of accounts and transactions	12 months retroactively from the present banking day	
Savings accounts	With notice period, without notice period	12 months
Overview of accounts and transactions	12 months retroactively from the present banking day	
Payment cards	Debit, credit and prepaid	12 months
Informative overview of debit, credit and prepaid cards and card transactions *Note:* • *The holder of the main card may have a main credit card automatically attached, additional cards linked to the main card must be requested from the branch. Holders of additional cards have assigned only their additional credit cards.* • *Debit card transactions carried out abroad can result in an exchange difference between entries on the account and entries displayed in the card history.* • *The credit card accounting balance after the settlement of transactions of prior banking day.*		
Credit accounts	Retail mortgages and consumer credit	12 months
Overview of accounts and transactions	12 months retroactively from the present banking day	
Term deposits	Displaying current term deposits	
Information about accounts and products		
Balance	Accounting and available balance of current accounts, accounting balance of other accounts	
The available balance includes the overdraft on the account and transactions not settled. This type of balance is shown on the payer's account when the payment order is placed.		
Transaction history	Information about transactions on accounts	12 months
Payments	Order archive	12 months
Templates	Possibility of saving details of domestic payment in a template for later use	
Order history	Order archive	15 months
Order archive	List of authorised transactions; At least 15 months retroactively from the present banking day	15 months
Active operations		
SEPA payments	**Payment orders in EUR from accounts denominated in EUR**	**By 9:30 p.m.**
SEPA Credit Transfer	Sending a domestic payment order in EUR to a bank in Slovakia or in an EEA country, Switzerland and Monaco; with crediting a bank in Slovakia and EEA on the next banking day, a bank in Switzerland and Monaco on the next following banking day.	By 9:30 p.m.
Credit card repayment	SEPA payment order with predefined data for repayment of a credit card issued by UniCredit Bank. Maturity on a specified banking day. Debiting funds on the due date. Crediting the credit card account on the due date.	By 9:30 p.m.
Scanner	Uploading a domestic payment order in EUR by scanning a barcode or QR code from a postal order or invoice.	By 9:30 p.m.
Standing order	**Domestic (transfer of a fixed amount)**	**By 9:30 p.m.**
SEPA Standing Payment Order – placing	If a due date of a regular payment under the standing order falls upon a non-banking day, then the payment is made on the following banking day.	By 9:30 p.m. D-1
SEPA Standing Payment Order – changing/cancelling	If the change/cancellation date is identical with the banking day for a regular payment under an existing standing order, then the change/cancellation of the standing order will become valid from the following banking day. This shall not apply to standing orders with a 1 day period, i.e., a one-day standing order can be changed/cancelled on the banking day scheduled for the regular payment.	By 9:30 p.m. D-1

Smart Banking – Services

Title	Description	Time limit
	Other	
Mail	**Possibility of sending/receiving messages between the Bank and the User**	
Requests	**Requests for the provision of new products, changes to existing products and services**	
Credit card issuance request	Completing and submitting the form to the Bank does not automatically entitle the client to a credit card with the requested limit. The client then visits the selected branch, where the client enters into a written Credit Card Agreement.	
Online interest in credit	Completing and submitting the form to the Bank does not automatically entitle the client to a credit in the requested credit amount at the given interest rate. The client then visits the selected branch, where the client enters into a written credit application.	
Map of branches and ATMs	**Displaying UniCredit Bank branches and ATMs**	
Exchange rates	**Overview of foreign currency exchange rates: foreign exchange – sell, buy and middle rate, and exchange rate calculator**	

In order for the display to work properly, it is necessary to download data to the app via the HTTP protocol, and therefore, upon request of the browser, downloading data via this protocol must be enabled.

Private Investment – Parameters

Minimum technical requirements	
App for smartphones	Operating system iOS 11.3 or higher, Android 6.0 or higher
	Free space for app storage min. 90 MB
Internet connection	Active internet connection via mobile operator data services or Wi-Fi *Note: For security reasons, the Bank does not recommend the use of unsecured public wireless networks. We also recommend turning off your wireless connection when you're not using it.*
Security tools	
Mobile app activation	The app must be activated before first use. Activating the app together with setting one's own PIN code and User settings must be properly authorised by entering a one-time password* sent by SMS to the client's mobile number registered in the Bank's system. The app is activated on the mobile device by scanning the QR code or by retrieving the activation link generated from the Bank's system or a previously activated app. Once successfully activated, the app can also be used on multiple mobile devices.
Authentication (login) to the app	**First login** PIN (8-digit numeric code selected by the User) **Second and subsequent logins** PIN chosen by the User or via biometric features. If the client activates the app on more than one mobile device, the PIN chosen when activating the first app is used for login. In the event of three consecutive unsuccessful attempts to enter the correct PIN code or biometric feature, the security tool will be blocked. Unblocking can be requested directly from the mobile app or from your private banker.
Authorisation (signing) of active operations	Authorisation is carried out using security tools (PIN code or biometric features).
Support	
By phone	Private banker or +421 2 594 280 19
Website	https://www.unicreditbank.sk/sk/private-banking.html#home
Other	
Availability	On a 24/7 basis, except for technical shutdown. Some of the services in the app can only be used by the User for a certain period of time.

Private Investment – Services

Title	Description of the service
Overview of accounts	Informative overview of all open accounts and balances
Overview of securities	Informative overview of selected securities with the possibility of tracking their price development
Overview of financial assets	An overview of the portfolio, including its development, performance and transaction history
Overview of cards	Informative overview of debit, credit and prepaid cards
Overview of credit products	Informative overview of mortgage and consumer credit granted
Communication	Sending/receiving messages between the Bank and the User, including promotion of product news within the client's positive target market and related notifications
Market indices	Current values of selected market indices
FX rates	Current values of selected FX rates
Media news	Current news from selected media
Trading in financial instruments	The following types of orders can be placed with regard to selected financial instruments: • Order to buy securities • Order to sell securities The order must contain mandatory elements and must meet the conditions required in the mobile app otherwise the Bank will not allow the order to be placed. An order is deemed to have been placed and accepted by the Bank at the moment when the Client confirms it with the authorisation tool. Orders can be entered daily from 6:00 a.m. to 9:00 p.m., with the exception of technical shutdowns on the part of the Bank. The client can also submit a request to cancel an order submitted electronically via the mobile app. The client's request will not be granted if the request for cancellation of the order has already been submitted at the time when the Bank's irreversible steps to execute the order have been initiated.
Authorisation of a draft order	Confirmation of an order entered into the Bank's system by the Client at the Client's request
Offers to buy financial instruments	Accepting offers for the purchase of financial instruments - investment advice as part of the investment advisory service

Note: *Open accounts and products are made available in the app automatically without the possibility of changing them.*

Online Card – Parameters

Minimum technical requirements	
Operating system	MS Windows Vista, 7, MaC OS X or higher
	Android 1.x.x or higher, iOS, RIM, Symbian*
Internet browser	MS Internet Explorer 7.0 or higher, Mozilla Firefox 3.0 or higher, Google Chrome
	Native browser for Android*, iOS, Symbian, Opera Mini/Mobile
JavaScript, Cookies	Enabled
Other	Adobe Acrobat Reader 6.0 or higher
Security tools	
Security	**User ID is assigned by the Bank**
	Security key **1. Online Banking Key (token in a mobile phone)** Code generated by the Online Banking Key mobile app. Access to the app is protected by a PIN code chosen by the User. The code for the first login to the app is sent by the Bank in the form of an SMS to the User's mobile phone. **2. SMS key** The code for logging in / signing the payment is sent by the Bank to the mobile phone designated by the User in the form of an SMS. The initiation password for the first login is sent by the Bank to the e-mail address specified by the User. **3. Security key (calculator)** Code generated by the security key. Access to the security key is protected by a PIN code chosen by the User. In the event of three consecutive unsuccessful attempts to enter the correct PIN code, the security key will be blocked. **Unblocking a blocked User/security key** In the event of three consecutive unsuccessful attempts to enter the code from the security key, the Online Banking app will be blocked. The User can request unblocking by calling the Client Line (after successful identification) or directly at the Bank's branch.
Support	
Client Line	**+421 2 6920 2090**
	Opening hours (except holidays) 7:00 a.m. – 10:00 p.m.
UniTel Line standard activities	• Information on entering/changing/cancelling the client's orders • Blocking/unblocking the Security key, the User • Accepting the client's problem, solution and announcement of the result • Communication with clients via e-mails, apps
Other	
Availability	On a 24/7 basis, except for technical closing

* For optimised display on a mobile phone

Online Card – Services

Title	Description	Time limit
	Associated accounts and products	
Credit cards	Credit card information	
Informative overview of credit cards and card transactions *Note:* • *The holder of the main card has a main credit card automatically attached, additional cards linked to the main card must be requested from the branch. Holders of additional cards have assigned only their additional credit cards.* • *The credit card accounting balance after the settlement of transactions of prior banking day.* • *If you need to know the available balance, please call the line on 2 6920 2090.*		
	Credit card information	
Transaction history	Information on all credit card transactions	15 months
According to User specified filtering criteria, it is possible to display up to 1,000 transaction history records and export them in a predefined format to csv, xls formats.		
Statements and documents in PDF	PDF documents have the same requirements as the Bank's printed documents	15 months
	Other	
Mail	**Possibility of sending/receiving messages between the Bank and the User**	
Requests	**Requests for the provision of new products, changes to current products and services**	
Request to change the sending of card statements	Change in the way credit or prepaid card statements are sent. Completing and submitting the form to the Bank cancels the previous method of sending statements	By 12:00 a.m. (midnight)
Map of branches and ATMs	**Displaying UniCredit Bank branches and ATMs**	
In order for the display to work properly, it is necessary to download data to the app via the HTTP protocol, and therefore, upon request of the browser, downloading data via this protocol must be enabled.		

Sending Information – Parameters

Minimum technical requirements	
Mobile phone	Available function to receive and display SMS messages
Electronic mailbox	Verification of the Bank certificate with which mail messages are marked
Support	
Client Line	**+421 2 6920 2090**
	Opening hours (except holidays) 7:00 a.m. – 10:00 p.m.
UniTel Line standard activities	• Information on entering/changing/cancelling the client's orders • Accepting the client's problem, solution and announcement of the result • Communication with clients via e-mails, apps
Other	
Availability	On a 24/7 basis, except for technical closing

Sending Information – Services

Title	Description	Time limit
	Notifications	
Notifications	**Setting up e-mail or SMS messages with banking information**	
Orders are placed/cancelled by the User, SMS charges are paid by the account owner. The Bank reserves the rights to change the content and structure of information.		
Balance, term deposit	SMS, e-mail	
Transactions	SMS, e-mail, one-time on deposit, recurring on credit / debit	
Card transactions	SMS, e-mail, at the time of authorisation, debit card transactions only	
Term deposit	SMS, e-mail, renewal of the term deposit or final maturity date	
In order for the display to work properly, it is necessary to download data to the app via the HTTP protocol, and therefore, upon request of the browser, downloading data via this protocol must be enabled.		

BusinessNet Professional – Parameters

Minimum technical requirements	
Operating system	MS Windows 10
	Mac OS X or higher
	Android 1.x.x or higher, iOS*
Internet browser	MS Internet Explorer 7.0 or higher, MS Edge, Mozilla Firefox 3.0 or higher, Google Chrome 4.0 or higher, Safari 3.0 or higher
	Native browser for Android*, iOS, Opera Mini/Mobile
Screen resolution	1024×768 for PC
	For display on a mobile phone, the app adapts to its resolution
Font size	Normal
JavaScript	Enabled
Java	Optional for greater convenience when retrieving data from the accounting system: Java accessible, MS Java or JDK 1.4 applet version
Cookies	Enabled
Other	Adobe Acrobat Reader 6.0 or higher
Note: For operating systems and browsers other than the recommended ones, the Bank does not guarantee the proper functioning of the Internet Banking Services.	

Security tools and identifiers when communicating with the Bank	
Security – Primary identification Authentication (login) to the app Authorisation (signing) of active operations	**User ID – User ID is assigned by the Bank** The Bank is entitled to unilaterally change the User ID; the Bank shall notify the User of such change via the relevant Internet Banking Service. The Account Owner agrees that the Bank will notify the User directly of the change of User ID. The receipt of the User ID change notice by the User in question also changes the content of the Agreement to the relevant extent.
	Security tool: **1. Smart Key** • Code generated by the Smart Key mobile app **2. Security key (Electronic token)** • Code generated by the security key (token) **3. SMS key** • Static security code (assigned by the Bank and changed by the User at first login) • SMS code sent by the Bank to the User's mobile phone *Note: Access to the Smart Key / Electronic token is protected by a PIN code chosen by the User. In the event of three consecutive unsuccessful attempts to enter the correct PIN code, the security key will be blocked. The User can request its unblocking by phone after successful identification or directly at the Bank's branch.*
Secondary identification (data for blocking/ unblocking the security tool)	• User ID (User ID is assigned by the Bank) • User's name and surname • Control data (answer to control question) • Additional data as required by the Bank The User can change the control data for blocking/unblocking the security tool agreed in the Agreement via the Internet Banking Services. If the control data has not been agreed in the Agreement, the User may add it via the Internet Banking Services. If the User changes or adds a control data agreed in the Agreement (if it was not agreed in the Agreement) via the Internet Banking Services, the control data for blocking/ unblocking the security tool shall be the control data added by the User via the Internet Banking Services.

* For optimised display on a mobile phone

BusinessNet Professional – Parameters

Blocking a security tool/ access to internet banking services	The Bank will block the Security Tool: • **at the request of the User, the Account Owner.** If the Account Owner or User correctly provides the relevant data required by the Bank, namely: the User's first and surname, User ID and the control data for blocking/unblocking the Security Tool. If the Account Owner or User fails to provide the required information, the Bank will temporarily block the Security Tool. The Bank will only block the Security Instrument completely if it has received a written request from the Account Owner to block the Security Tool. In the event that the Bank does not receive a written request from the Account Owner to unblock the Security Tool, the Bank will lift the temporary blocking if the Account Owner or the User requests the unblocking of the Security Tool by phone and provides the Bank with the requested information. • **if the Security Code is repeatedly entered incorrectly in combination with the User ID during authentication.** • **if the User repeatedly (3 times or more) enters an incorrect input PIN into the Electronic token.** The Bank will unblock access to the Electronic Banking Services on the basis of the User's telephone identification. If the User does not provide the control data, the Bank is not obliged to unblock access to the Internet Banking Services. In such case, only the Account Owner may request unblocking of the Security Tool upon written request delivered to the Bank. The Bank is not responsible for any misuse of the Security Tool during the period between the temporary blocking of the Security Tool and the receipt of the Account Owner's written request to block the Security Tool.
Limits	
Daily limit	Unlimited, unless otherwise agreed in the Agreement for the User
Transaction limit	Unlimited, unless otherwise agreed in the Agreement for the User
Support	
Client Line	**+421 2 6920 2090** *Note: The User pays standard telephone charges when making a call.* Daily (Mon – Sun) 7:00 a.m. – 10:00 p.m.
Client Line standard activities	• Notification of performance of the instruction/amendment/cancellation of the client's orders. • Blocking/unblocking the Security key, the User • Receiving the client's problem, solution and announcement of the result
Technical support	mail: **EB@unicreditgroup.sk** **+421 2 6920 2097** Banking days (Mon – Fri) 8:00 a.m. – 5:00 p.m.
Technical support standard activities	• Communication with clients via e-mails / electronic forms • Receiving the client's problem, solution and announcement of the result
Website	http://www.unicreditbank.sk/businessnet
Other	
International User profile	Setup of the User ID as an internationally usable. This User ID can be used to access selected apps of other UniCredit Group banks that support this service. A list of these banks is available on the Bank's website. The User has an International User profile if the Account Owner has agreed it in the Agreement with the Bank. Such User is entitled to use the same User ID and the same Security Tool in other countries and banks within the Bank Group that provide access to accounts held with them via the same online platform as the Bank. However, the actual access to such account(s) must be agreed in a separate agreement between the relevant Account Owner and the bank in question in the other country.
Export of the content to CSV, XLS format	The Bank reserves the right to change the format of exported data.
Maximum number of connected accounts	The maximum number of associated accounts is 300. A maximum of 200 accounts can be selected for display and export to PDF.

BusinessNet Professional – Parameters

Availability	24/7, except for the signing (authorisation) of requests at the time of the technical closing – daily from approximately 10:30 p.m. to 11:15 p.m., the last day of the month from approximately 11:30 p.m. to 1:30 a.m.
SEPA Convertor – responsibility	The Account Owner or User is responsible for the data in the input file (SKI, CLEARING, CSV or GEMINI) and is also responsible for checking that the data in the output file (pain.001.001.03) corresponds to the content of the payments in the input file. The Bank is not responsible for any misuse of the SEPA Convertor.
Multisignature service information	
Description	The Multisignature service applies to the following payment/instruction types: SEPA payment, Cross-border payment, Conversion/Transfer between own accounts, SEPA direct debit order, SEPA direct debit mandate, Standing order. Instructions (ordering/changing/cancelling) referring to term deposits are not subject to the Multisignature authorisation. Each User with signature authorisations (irrespective of the Multisignature authorisation) who has access to a given term deposit account may sign the instruction relating to the term deposit on its own.
User's signature authorisation	Signature means the authorisation of a transaction by a security key code. A single transaction may or may not require multiple authorisations, depending on the rules specified in the relevant contractual document. The client (Account Owner) authorises the User (authorised person) to use the funds in the account and at the same time determines the level of signature of the authorised person in the form of assignment to the so-called signature class. Following the signature class thus assigned and the signature rules (combination of signatures) set out in the relevant contractual document, the signature authorisation of a given person may thus be: • partial (i.e., only in combination with the signature of another person); • standalone.
Signature class	A signature class defines a group of Users with the same privileges to use the funds in a given account in accordance with contractually established limits and rules. For the respective account, a signature rule is set, the required combination of signatures of persons with the respective signature class, which is necessary to execute a transaction within the defined transaction limit. There can also be no limit specified. Any signature class can be assigned to an unlimited number of authorised persons. Above the limits at the level of the Multisignature authorisation is the transaction limit of each authorised person – User (the User's limit is set to the value WITHOUT LIMIT by default, unless otherwise agreed in the agreement). The cancellation of a pending transaction is not subject to the rules of the Multisignature authorisation.
Fees	
Charging fees	The service activation fee and the account(s) access fee shall be paid by the Account Owner on whose Account these services are established and provided. The service activation fee is payable upon conclusion of the Agreement; the account(s) access fee is payable on the last working day of the relevant calendar month. The amount of the Fee is set out in the Price List applicable to the market segment in which the Bank classifies the Account Owner. The fee includes all accounts that the Bank has agreed with the Account Owner in the Internet Banking Product Agreement.
A description of the technical requirements and functionality as well as the terms and conditions of use are set out and described in detail in the User Manual, which is published in electronic form on the Bank's Website.	

BusinessNet Professional – Services

Title	Description of the service	Time limit
Associated accounts and products		
Current accounts	In all currencies, displaying account details and balances	
Payment cards	Summary information on debit and credit cards	
Securities	Allows to manage securities accounts	
Information about accounts and products		
Overview and history	**Accounting and available balance of current and other accounts**	
Account overview and history	Informative overview of accounts and account transactions. A maximum of 1,000 records can be displayed in the selection. The complete overview can be exported without limiting the number of records.	At least 15 months retroactively from the present banking day
Card overview and history	Informative overview of debit and credit cards and card transactions *Note:* • *The EB service User has a main credit card/additional card attached based on contractual documentation signed by the Account Owner.* • *The EB service User has automatically linked all debit cards issued to accounts to which the EB service User has access via EB services.* • *Debit card transactions carried out abroad can result in an exchange difference between entries on the account and entries displayed in the card history.* • *The credit card accounting balance after the settlement of transactions of prior banking day.* • *If you need to know the available balance, please call the Client Line on 800 14 00 14.*	At least 15 months retroactively from the present banking day
Electronic statements	**Possibility of displaying and downloading daily statements in standard formats**	
Daily electronic statements – preview	Display, print and export daily electronic account statements	At least 15 months retroactively from the present banking day
Daily electronic statements – download	Possibility of downloading daily electronic statements in standard formats – MultiCash MT940 structured, MultiCash MT940 non-structured, Gemini, Clearing, ABO, CSV	At least 15 months retroactively from the present banking day
MT942 messages – preview	Overview of turnovers settled on the current day on accounts held with the Bank (display of MT942 messages) with the possibility of printing/exporting	–
MT942 messages – download	Possibility of downloading MT942 messages in standard formats – MultiCash MT942 structured and MultiCash MT942 non-structured	–
XML statements	Possibility of downloading electronic statements in XML format; XML statements are provided in the CAMT.053 / CAMT.052 formats	–
Cash management	**Overview of account balances held at UCB and other banks**	
Cash management	Overview of closing balances on bank accounts with the possibility of totalling balances	At least 15 months retroactively from the present banking day
Archive records	**Order history, record of activities**	
Order history	List of authorised (signed) transactions submitted to the Bank for processing	At least 15 months retroactively from the present banking day
Record of activities	List of activities performed by individual Users in the system; the time limit may vary according to the type of banking operation performed.	At least 6 months retroactively from the present banking day

BusinessNet Professional – Services

Payments – Active operations		
SEPA	**SEPA Credit Transfer, SEPA Direct Debit**	
SEPA payment from EUR account	Sending a SEPA payment order in EUR within the EU27 and other European countries with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on the following banking day	By 9:30 p.m.
SEPA payment within UniCredit Bank	Sending a SEPA payment order between accounts within UniCredit Bank in EUR with maturity on a specified banking day, with funds debited from the client's account and credited to the beneficiary's account on that day	By 9:30 p.m.
SEPA payment from a foreign currency account	Sending a SEPA payment order in EUR from a foreign currency account within the EU27 and other European countries with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on the following banking day	By 3:00 p.m.
SEPA payment from EUR account – Urgent	Sending a SEPA payment order in EUR with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on that day *Note: The beneficiary's bank is responsible for crediting the express payment on the day the payment is sent from the Bank. In case of non-compliance with the time limit, the beneficiary's bank should be contacted.*	By 2:30 p.m. urgent payment From 2:30 p.m. until 4:00 p.m. urgent payment via Target2
SEPA payment from a foreign currency account – Urgent	Sending a SEPA payment order in EUR with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on that day *Note: The beneficiary's bank is responsible for crediting the express payment on the day the payment is sent from the Bank. In case of non-compliance with the time limit, the beneficiary's bank should be contacted.*	By 2:30 p.m. urgent payment From 2:30 p.m. until 3:00 p.m. urgent payment via Target2
SEPA Direct Debit B2B order	Sending an order for SEPA Direct Debit B2B. The order must be submitted to the Bank 2 banking days before the due date. The Bank sends the order to the payer's bank the day before the due date (D-1) in order to comply with SEPA rules	By 9:30 p.m. D-2
SEPA Direct Debit CORE order	Sending an order for SEPA Direct Debit CORE. The order must be submitted to the Bank 6 banking days (First Recurring, One-Time), 3 banking days (additional Recurring) before the due date. The Bank sends the order to the payer's bank the day before the due date (D-1) in order to comply with SEPA rules	By 9:30 p.m. D-6 D-3
Cancellation of a SEPA payment	Optional cancellation of a SEPA payment, provided that the payment is not yet settled by the Bank.	Until the payment is settled by the Bank
Cross-border payments and conversions	**Standard, domestic in foreign currency, foreign currency within the Bank, conversions, cheque payments**	
Transfer between the client's own accounts in the same foreign currency	Sending a payment order between accounts made available to the User and held with UniCredit Bank in the same foreign currency, with maturity on a specified banking day, with the funds debited and credited to the client's account on that day	By 3:00 p.m.
Conversion between the client's own accounts	Sending a payment order between accounts made available to the User and held with UniCredit Bank in different foreign currencies or between an account in EUR and an account in a foreign currency with maturity on a specified banking day, with the funds debited and credited to the client's account on that day	By 3:00 p.m.
Cross-border order – standard payment abroad / foreign currency at home	Sending a cross-border payment order to the beneficiary's bank with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on the next following banking day	By 3:00 p.m.
Cross-border order – payment in foreign currency within UniCredit Bank	Sending a cross-border payment order (with or without conversion) in a foreign currency between accounts within UniCredit Bank with maturity on a specified banking day	By 3:00 p.m.

BusinessNet Professional – Services

Cross-border payments and conversions	**Standard, domestic in foreign currency, foreign currency within the Bank, conversions, cheque payments**	
Cross-border order – urgent payment abroad / foreign currency at home	Sending a foreign payment order to the beneficiary's bank with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on the following working day	By 1:00 p.m.
Standing order	**SEPA, Cross-border (transfer of amount, balance, allocation for a default balance)**	
SEPA Standing Payment Order – placing	The **"Validity from"** field must indicate at least 1 working day before the date of the first settlement of the standing order. If a due date of a regular payment under the standing order falls upon a non-banking day, then the payment is made as instructed by the client (on the preceding or the following banking day).	By 9:30 p.m. D-1
SEPA Standing Payment Order – changing/cancelling	If the change/cancellation date is identical with the banking day for a regular payment under an existing standing order, then the change/cancellation of the standing order will become valid from the following banking day. This shall not apply to standing orders with a 1 day period, i.e., a one-day standing order can be changed/cancelled on the banking day scheduled for the regular payment.	By 9:30 p.m. D-1
Cross-Border Standing Payment Order – placing	The **"Validity from"** field must indicate at least 1 working day before the date of the first settlement of the standing order. If a due date of a regular payment under the standing order falls upon a non-banking day, then the payment is made on the following banking day.	By 9:30 p.m. D-1
Cross-Border Standing Payment Order – changing/ cancelling	If the change/cancellation date is identical with the banking day for a regular payment under an existing standing order, then the change/cancellation of the standing order will become valid from the following banking day. This shall not apply to standing orders with a 1 day period, i.e., a one-day standing order can be changed/cancelled on the banking day scheduled for the regular payment.	By 9:30 p.m. D-1
Sweeping standing order in EUR – placing	The **"Validity from"** field must indicate at least 1 working day before the date of the first settlement of the standing order. If a due date of a regular payment under the standing order falls upon a non-banking day, then the payment is made as instructed by the client (on the preceding or the following banking day).	By 9:30 p.m. D-1
Sweeping standing order in EUR – changing/cancelling	If the change/cancellation date is identical with the banking day for a regular payment under an existing standing order, then the change/cancellation of the standing order will become valid from the following banking day. This shall not apply to standing orders with a 1 day period, i.e., a one-day standing order can be changed/cancelled on the banking day scheduled for the regular payment.	By 9:30 p.m. D-1
Import	**SEPA, cross-border payment orders, custom data format**	
Uploading payment files	Possibility of uploading payment files with SEPA payments (XML pain format) or Cross-border (non SEPA) orders (MultiCash format, Gemini, CSV)	–
SEPA Convertor	A tool enabling conversion of import formats for domestic payments (SKI, GEMINI, CSV, CLEARING) into SEPA format (pain.001.001.03); The Bank provides technical support for this tool until 31 March 2017	Possibility of access upon request
Transaction authorisation	**To be signed, partially signed**	
To be signed (transaction authorisation)	All created transactions must contain the User's signature, otherwise the Bank will not process them. A maximum of 10,000 transactions / 1 signature can be authorised. Only a User authorised to sign the transactions under the Agreement (signature classes, transaction limit, shared signing, ...) has access to transactions to be signed.	Within 90 days of payment/instruction creation
Templates, beneficiaries	**SEPA, cross-border**	
Payment order templates	Possibility of saving details of SEPA or cross-border payment in a template for later use. Possibility of setting the template as private or shared by multiple Users.	–
Beneficiaries	Possibility of saving a record of a bank link to a domestic foreign trading partner for later use. Possibility of setting the template as private or shared by multiple Users.	–

BusinessNet Professional – Services

Overview of payments	Payments and their statuses before settlement and display in order history	
Payment statutes	• With the Bank – an order accepted by the Bank for processing • To be signed – an order waiting for authorisation by the User • Partially signed – an order waiting for authorisation by another User (under contractually agreed signature rules)	–
	Other banking operations	
SEPA Direct Debit	**Authorisation, refusal, return**	
SEPA Direct Debit mandate	Entering/changing/cancelling SEPA Direct Debit mandate with effect from the next following banking day. When delivered to the bank on a non-banking day, entering, changing and cancelling the Direct Debit mandate will be valid on the next following banking day.	9:30 p.m. D-2
Request for refusal of SEPA Direct Debit	Request for refusal (non-execution) of an expected SEPA Direct Debit. The bank will not perform the Direct Debit, as instructed by the submitted parameters The beneficiary's bank will be notified that the payer refused to make the payment.	4:00 p.m. D-1
Request for refund of SEPA Direct Debit	Request for refund of financial funds from a settled SEPA Direct Debit. The Bank shall refund the funds withdrawn and inform the beneficiary's bank of the reason for cancelling the transaction.	4:00 p.m. D-1
Term deposit	**One-off, recurring**	
Term deposit – opening	A term deposit can be opened on the current banking day. The minimum amount of the term deposit is determined in accordance with the Bank's Basic Business Terms and Conditions For Accepting Deposits published on the Bank's website. It is only possible to open term deposits if a Deposit Account Agreement has been concluded between the Account Owner and the Bank. The Account Owner must request the Bank to make the deposit account available to the EB service. The User opens a term deposit by selecting an account held with the Bank, to which funds will be transferred to the credit of the deposit account designated by the User. The User is entitled to designate a current account to which the Bank will credit funds and interest upon expiry of the term deposit fixed period. The Deposit Agreement is concluded and the term deposit is established at the moment of acceptance of the Bank's proposal/conditions for the deposit by the client, through the Security Tool. The Bank does not allow early withdrawals from deposit accounts through Internet Banking Services. The Account Owner is informed about the establishment of the term deposit in the account statement.	By 9:30 p.m.
Term deposit – changing/ cancelling	A term deposit can be opened on the current banking day. The minimum amount of the term deposit is determined in accordance with the Bank's Basic Business Terms and Conditions For Accepting Deposits published on the Bank's website. A one-time term deposit cannot be changed or cancelled during the applicable period without penalty interest. A change or cancellation of an automatically recurring term deposit will be effective from the next period and can be made no later than 1 banking day before the maturity date.	By 9:30 p.m.
Cards	**Card payment, additional services**	
Credit card repayment	Sending a SEPA payment order with predefined data for repayment of a credit card issued by UniCredit Bank with maturity on a specified banking day, with the funds debited from the client's account and credited to the credit card account on that day	By 9:30 p.m.
TPP	**Access to account – TPP Consents**	
Granting consent to the Fund Check Service (FCS)	In order for the bank to allow access to the client's account via a third party app, the client must consent to this. With valid consent, a third party can be informed of the availability of a specific amount in the account.	The consent is valid indefinitely.
Granting consent to the Indirect Payment Initiation Service (PIS)	One-time consent to the Indirect Payment Initiation Service is always given at the same time as signing a payment procured through a third party.	Consent is valid for the specific payment under which it was granted.
Granting consent to the Payment Account Information Service (AIS)	In order for the Bank to allow access to the client's account via a third party app, the client must consent to this. With valid consent, a third party can obtain information about the current balance and a statement of transactions for the selected period.	The consent is valid for 90 days from the date of signing.

BusinessNet Professional – Services

TPP	Access to account – TPP Consents	
Overview of consents to Open Banking services	An informative overview of all valid and invalid Open Banking consents. One-time consents to the Indirect Payment Initiation Service are not displayed.	–
Extending the validity of consent to the Indirect Payment Initiation Service (PIS)	It is not possible to extend the consent to the Indirect Payment Initiation Service, as the consent is always granted only for a specific payment at the same time as the payment is procured.	–
Extending the validity of consent to the Payment Account Information Service (AIS)	It is not possible to extend the consent to the Payment Account Information Service.	–
Extending the validity of consent to the Fund Check Service (FCS)	It is not possible to extend the consent to the Fund Check Service because it is valid indefinitely until withdrawn.	The consent is valid indefinitely.
Temporarily deactivating and reactivating consent to the Fund Check Service (FCS)	It is not possible to temporarily deactivate the consent to the Fund Check Service; the consent can only be withdrawn.	–
Temporarily deactivating and reactivating consent to the Indirect Payment Initiation Service (PIS)	It is not possible to temporarily deactivate the consent to the Indirect Payment Initiation Service.	–
Temporarily deactivating and reactivating consent to the Payment Account Information Service (AIS)	It is not possible to temporarily deactivate the consent to the Payment Account Information Service; the consent can only be withdrawn.	–
Withdrawing consent to the Fund Check Service (FCS)	The client may permanently withdraw the granted FCS consent at any time during its validity.	The consent shall cease to be valid from the moment of withdrawal.
Withdrawing consent to the Indirect Payment Initiation Service (PIS)	It is not possible to withdraw the consent to the Indirect Payment Initiation Service, as the consent is granted only for a specific payment at the same time as the payment is procured.	–
Withdrawing consent to the Payment Account Information Service (AIS)	The client may permanently withdraw the granted AIS consent at any time during its validity.	The consent shall cease to be valid from the moment of withdrawal.
History of requests made in the Fund Check Service	An informative overview of what funds availability requests have been performed on client's accounts as part of the Fund Check Service. The following information is available to the client: • the request date; • the name of the third party and the name of its app; • the amount and currency: • the availability of funds sent by the Bank to a third party.	Maximum 6 months retroactively from the present day
Trade Finance	**Documentary credit, Documentary collection, guarantees**	
Documentary credit / Amendment of documentary credit / Acceptance of documents submitted under the documentary credit	Sending an Order to open a Documentary Credit or a Request to amend a Documentary Credit or an Approval/Disapproval to defective documents supporting the documentary credit	A period usual for processing an order for opening/amendment of a documentary credit / acceptance of documents submitted to support the documentary credit
Bank guarantee / amendment of Bank guarantee	Sending a Request for issuance of a Bank guarantee or Request for amendment of a Bank guarantee	A period usual for processing a Request for issuance of a Bank guarantee/amendment of a Bank
Documentary and non-documentary collection	Creation of an order for provision of a documentary and non-documentary collection. A form designed to be printed and personally delivered to the bank.	A period usual for processing an order for provision of a documentary and non-documentary collection
BusinessNet Securities	**Overview of account balances held at UCB and other banks**	
BusinessNet Securities (BNS)	The app is made available to the User on the basis of an agreement with the Account Owner. Through the BNS app, the client can access securities account information, including securities account balances and corporate events related to securities held by the client. The BNS app also allows placing orders for transactions in securities.	–

BusinessNet Professional – Services

Other		
Mailbox	**Sending/receiving messages within the app**	
Mail (incoming / outgoing)	Possibility of sending/receiving messages between the bank and the User	–
Information	**Exchange rates, interest rates, network of branches and ATMs**	
Exchange rate list	The exchange rate list is provided as non-binding information. If, in the course of a banking day, the exchange rate undergoes a significant change (e.g., owing to an intervention), the Bank reserves the right to amend the exchange list during the business day. A payment shall always be cleared using the exchange rate valid at the moment of the payment.	–
Interest rates	Interest rates are always valid for the current banking week.	–
Map of branches and ATMs	Displaying UniCredit Bank branches and ATMs *Note:* *In order for the display to work properly, it is necessary to download data to the app via the HTTP protocol, and therefore, upon request of the browser, downloading data via this protocol must be enabled.*	–
Settings	**General settings, Bank settings, accounts arrangements**	
Preferred arrangement of accounts and cards	Possibility of defining in the settings the account and card arrangements on overview screens and in the selection menu. Possibility of hiding an account/card on overview screens.	–
General settings	Setting contact details, setting the control data for blocking/unblocking the security tool. User's setting via the EB service is superior to the contractual arrangement with the Account Owner.	–
Bank settings	Possibility of setting the preferred account, card; show/hide transaction history.	–
Notifications[1]	**Automatic sending of banking information by e-mail or SMS**	
Login	SMS or e-mail notification of successful login.	–
Balance	SMS or e-mail notification of the selected account balance. Notifications are sent periodically (daily/weekly/monthly) or after a defined event (e.g., when the selected limit is dropped/exceeded).	–
Transactions	SMS or e-mail notification of transactions on the selected account after a defined event, i.e.: incoming/outgoing/all, if >/</= the specified amount for a specific beneficiary/payer account, bank code, transaction detail, etc. Possibility of selecting a summary notification of the number of incoming and outgoing transactions and their amount, sent at 4 hourly intervals (8:00 a.m., 12:00 noon, 4:00 p.m., 8:00 p.m.).	–
Debit cards	SMS or e-mail notification, at the moment of authorisation, of payment card transactions made but not yet settled.	–
Term deposit	E-mail notification of an automatically rolled-over term deposit and the end of the original period, the start of the next period and the final maturity date.	–
Multisignature	SMS or e-mail notification of transaction signature status after a defined event, i.e.: • Payment/batch ready for signature; • Payment/batch finally signed; • Payment/batch deleted.	–
Statements	E-mail with PDF attachment, sent once a day (in the morning) on the working day following the previous banking day for which the statement is made.	–

[1] The Account Owner shall indicate the requirement to receive Notifications in the Agreement. SMS charges are paid by the account owner. The Bank reserves the rights to change the content and structure of information included in the message.

BusinessNet Connect – Parameters

Minimum technical requirements	
Operating system	MS Windows 10
	Mac OS X or higher
	Linux
Supported protocol	WebDAV – freeware https protocol used for Document management system Web Distributed Authoring and Versioning
Other	**PGP encryption** For optional encryption of statement downloads or for signing payment files, an OpenPGP digital certificate with a validity of less than 365 days. **KLEOPATRA** – a plugin recommended by the Bank that allows working with PGP, supports command line commands, **Total Commander**.
Security tools and identifiers when communicating with the Bank	
Authentication (login) to the app	**Using the password:** • User ID (User ID is assigned by the Bank) • Password – Static security code assigned by the Bank and changed by the User at the first login (password change must be made within 72 hours of receipt) The Bank is entitled to unilaterally change the User ID; the Bank will notify the User of such change through the relevant Internet Banking Service. The Account Owner agrees that the Bank will notify the User directly of the change of User ID. The receipt of the User ID change notice by the User in question also changes the content of the Agreement to the relevant extent.
Authorisation (signing) of active operations	If automatic processing of payment order files is set up, the Bank will only process files that are digitally signed by one of the key holders. Another prerequisite is that this key holder has a separate signature authorisation.
Users and electronic signature	
Users	**Technical User** It is a type of Passive User and is intended only for setting up the connection and exchange of files between the Account Owner's systems and the Bank's systems. **Signature User** User designated only for signing Orders (payment file) on the Account Owner's side. Orders can be signed with up to one Signature User key. Multisignature can only be achieved in combination with BNP. There may be more than one Technical/Signature User, each of whom must be authorised by the Account Owner to perform such acts on a separate form of the Bank (Confirmation of Assignment of Authorisations for Users of Electronic Banking Services – BussinesNet Connect Services).
Electronic signature – digital keys in the file exchange process via WebDAV	**User's Public Key** A freely distributable PGP key generated by the Account Owner for the Technical and/or Signature User. It is used to encrypt the contents of the file to be delivered by the Bank to the Account Owner. The contents of the file become unreadable after encryption. The encrypted file can only be decrypted with the User's Private Key. **User's Private Key** It is the Security Tool for BusinessNet Connect. Under no circumstances may the User provide it to anyone else. The key is used to sign the Orders file, decrypting the contents of files that have been encrypted using the secret part of its key on the Bank's side. **Bank's Public Key** It is used to encrypt the payment file on the client's side and the Bank sends it by e-mail (as an attachment) to the Account Owner at the agreed e-mail address. **Bank's Private Key** It is used on the Bank's side to digitally sign the file to be delivered by the Bank to the Account Owner. Before the data is stored on the Account Owner's side in the ERP system, the correctness of the signature is checked using the Bank's Public Key.
Limits	
Daily limit	Unlimited
Transaction limit	Unlimited

BusinessNet Connect – Parameters

Support	
Technical support	mail: **EB@unicreditgroup.sk**
	+421 2 6920 2097 Banking days (Mon – Fri) 8:00 a.m. – 5:00 p.m.
Technical support standard activities	• Information on entering/changing/cancelling the client's orders • Blocking/unblocking the Security key, the User • Communication with clients via e-mails / electronic forms • Receiving the client's problem, solution and announcement of the result
Website	http://www.unicreditbank.sk/businessnet
Other	
Available statement formats	• XML Camt.053 / 052 • MT94x MultiCash structured, MT94x MultiCash non-structured • Gemini, Clearing, ABO, CSV
Accepted payment file formats	**SEPA Credit Transfers:** XML **Foreign payments:** MultiCash, Gemini, CSV, client's custom format
Fees	
Charging fees	The implementation fee and the monthly fee shall be paid by the Account Owner on whose Account these services are established and provided. The implementation fee is payable upon conclusion of the Agreement; the monthly fee is payable on the last working day of the relevant calendar month. The amount of the fee is set out in the Price List applicable to the market segment in which the Bank classifies the Account Owner. The fee includes all accounts that the Bank has agreed with the Account Owner in the Internet Banking Product Agreement.

A description of the technical requirements and functionality as well as the terms and conditions of use are set out and described in detail in the User Manual, which is published in electronic form on the Bank's website.

BusinessNet Connect – Services

Title	Description of the service	Time limit
Associated accounts and products		
Electronic statements	**Possibility of displaying and downloading daily statements in standard formats**	
Daily electronic statements – download	Possibility of downloading daily electronic statements in standard formats – MultiCash MT940 structured, MultiCash MT940 non-structured, Gemini, Clearing, ABO, CSV	At least 15 months retroactively from the present banking day
MT942 electronic statements	Downloading electronic statements with intraday movements (MT942 format)	–
CSV statements	Downloading account balance information files (CSV format)	–
XML statements	Possibility of downloading electronic statements in XML format. XML statements are provided in CAMT.053 / CAMT.052 format.	–
Import	**SEPA, cross-border payment orders, custom data format**	
Uploading payment files	Possibility of uploading payment files with SEPA payments (XML pain format) or Cross-border (non SEPA) orders (MultiCash format, Gemini, CSV)	–
Transaction authorisation	**Automated signing process**	
Automated signature	Only 1 signature is possible via BN Connect. Multisignature can only be achieved in combination with BNP.	–

Business Smart Banking – Parameters

Minimum technical requirements	
Smartphone app	Operating system iOS 12.0 or higher, Android 5.0 or higher
Internet connection	• Active internet connection via mobile operator data services or Wi-Fi *Note: For security reasons, the Bank does not recommend the use of public unsecured wireless networks. We also recommend turning off your wireless connection when you're not using it.*
Security tools and identifiers when communicating with the Bank	
Authentication (login) to the app	**First login** • Activation code (16 digits, sent by the Bank via SMS and valid for 72 hours) • User ID (assigned by the Bank) • PIN (User selects a 6 to 8 digit PIN) **Second and subsequent logins** a) PIN To log in, the User will use the PIN chosen when first logging in. After successful login, the User can change the PIN. In the event of three consecutive unsuccessful attempts to enter the correct PIN code, the security tool will be blocked. The User can request unblocking by phone (after successful identification) or directly at the Bank's branch. b) Fingerprint (only for iOS and Android mobile phones and tablets that support this technology). The User stores their own fingerprints in the relevant section of the phone (Touch ID for iOS or Finger print for Android). In the Smart Banking app, the User enables fingerprint login, which can be used the next time they log in. The possibility of fingerprint login can be switched off in the app's settings; if fingerprint login is enabled, PIN login is always a possibility. Verification of the fingerprints takes place on the User's mobile phone, the Bank does not download and store the fingerprints.
Authorisation (signing) of active operations	The transaction is authorised by pressing the button to send the payment. For iOS and Android mobile phones, authorisation is subject to: a) entering a PIN code; b) the User's fingerprint. The User stores their own fingerprints in the relevant section of the phone (Touch ID for iOS or Finger print for Android). In the Smart Banking app, the User enables the Fingerprint Payment Signature feature, which can be used the next time the payment is signed. The possibility of fingerprint payment signature can be switched off in the app's settings; if fingerprint payment signature is enabled, PIN signature is always a possibility. Verification of the fingerprints takes place on the User's mobile phone, the Bank does not download and store the fingerprints. Fingerprint transaction authorisation is limited. When the limit is exceeded, the User signs the payments by entering the PIN by default.
Primary identification to communicate with the Bank	**Automatic identification when entering the User ID and security key code/password:** **1. via Smart Key** • User ID (assigned by the Bank) • Code generated by the Smart Key mobile app, or **2. via the security key (calculator)** • User ID (assigned by the Bank) • Code generated by the security key, or **3. via SMS security key** • User ID (assigned by the Bank) • Static security code (assigned by the Bank and changed by the User at first login)
Secondary identification to communicate with the Bank	• User ID – User ID is assigned by the Bank. • Password for secondary identification (alphanumeric), or additional data as required by the Bank. The password for telephone communication with the Bank is chosen by the User in the branch.

Business Smart Banking – Parameters

Limits	
Daily limit	Unlimited, with the possibility of setting a limit
Support	
Client Line	**+421 2 6920 2090** *Note: The User pays standard telephone charges when making a call.* Daily (Mon – Sun) 7:00 a.m. – 10:00 p.m.
Client Line standard activities	• Information on entering/changing/cancelling the client's orders • Blocking/unblocking the Security key, the User • Receiving the client's problem, solution and announcement of the result
Technical support	mail: **EB@unicreditgroup.sk** **+421 2 6920 2097** Banking days (Mon – Fri) 8:00 a.m. – 5:00 p.m.
Technical support standard activities	• Communication with clients via e-mails / electronic forms • Receiving the client's problem, solution and announcement of the result
Website	https://www.unicreditbank.sk/sk/podnikateliaamensiefirmy/digital/business-smart-banking.html
Other	
Availability	On a 24/7 basis, except for technical closing
Responsibility	The Bank is not responsible for the compatibility of banking apps with other app equipment on the User's device. The Bank is not responsible for damage and malfunctions or loss of functionality of the User's device or the User's mobile phone app equipment resulting from the fact that the device was damaged or had other defects, did not meet the characteristics specified by the manufacturer or contained app equipment incompatible with the Bank's app. The Bank is not responsible for damage caused by a device that has been tampered with (device is rooted/jailbroken), as its use may result in a reduction in the security of the use of the Business Smart Banking service and may make it more susceptible to misuse.

A description of the technical requirements and functionality as well as the terms and conditions of use are set out and described in detail in the User Manual, which is published in electronic form on the Bank's website.

Business Smart Banking – Services

Title	Description of the service	Time limit
Associated accounts and products		
Current accounts	**In all currencies, displaying account details and balances**	
Payment cards	**Summary information on debit and credit cards**	
Information about accounts and products		
Overview and history	**Accounting and available balance of current and other accounts**	
Account overview and history	Informative overview of accounts and account transactions	Maximum 12 months retroactively from the present banking day
Card overview and history	Informative overview of debit and credit cards and card transactions *Note:* • *The holder of the main card has a main credit card automatically attached, additional cards linked to the main card must be requested from the branch.* • *Holders of additional cards have assigned only their additional credit cards.* • *Debit card transactions carried out abroad can result in an exchange difference between entries on the account and entries displayed in the card history.* • *The credit card accounting balance after the settlement of transactions of prior banking day.* • *If you need to know the available balance, please call the Client Line on +421 2 6920 2090.*	Maximum 12 months retroactively from the present banking day
Archive records	**Order history, record of activities**	
Order history	List of authorised (signed) transactions submitted to the Bank for processing	Maximum 12 months retroactively from the present banking day
Payments – Active operations		
SEPA	**SEPA Credit Transfer, SEPA Direct Debit**	
SEPA payment from EUR account	Sending a SEPA payment order in EUR within the EU27 and other European countries with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on the following banking day	By 9:30 p.m.
SEPA payment within UniCredit Bank	Sending a SEPA payment order between accounts within UniCredit Bank in EUR with maturity on a specified banking day, with the funds debited from the client's account and credited to the beneficiary's account on that day	By 9:30 p.m.
SEPA payment from a foreign currency account	Sending a SEPA payment order in EUR from a foreign currency account within the EU27 and other European countries with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on the following banking day	By 3:00 p.m.
SEPA payment from EUR account – Urgent	Sending a SEPA payment order in EUR with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on that day *Note: The payee's bank is responsible for crediting the express payment on the day the payment is sent from the Bank. In case of non-compliance with the time limit, the beneficiary's bank should be contacted.*	By 2:30 p.m. urgent payment From 2:30 p.m. until 4:00 p.m. urgent payment via Target2

Business Smart Banking – Services

SEPA	**SEPA Credit Transfer, SEPA Direct Debit**	
SEPA payment from a foreign currency account – Urgent	Sending a SEPA payment order in EUR with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on that day *Note: The beneficiary's bank is responsible for crediting the express payment on the day the payment is sent from the Bank. In case of non-compliance with the time limit, the beneficiary's bank should be contacted.*	By 2:30 p.m. urgent payment From 2:30 p.m. until 3:00 p.m. urgent payment via Target2
QR payment	Creating a payment order based on a QR code (QR code scanning)	–
Postal order	Creating a payment order based on a postal order (postal order scanning)	–
Barcode	Creating a payment order based on a barcode (barcode scanning)	–
Cancellation of a SEPA payment	Optional cancellation of a SEPA payment, provided that the payment is not yet settled by the Bank.	Until the payment is settled by the Bank
Cross-border payments and conversions	**Standard, domestic in foreign currency, foreign currency within the Bank, conversions, cheque payments**	
Transfer between the client's own accounts in the same foreign currency	Sending a payment order between accounts made available to the User and held with UniCredit Bank in the same foreign currency, with maturity on a specified banking day, with the funds debited and credited to the client's account on that day	By 3:00 p.m.
Conversion between the client's own accounts	Sending a payment order between accounts made available to the User and held with UniCredit Bank in different foreign currencies or between an account in EUR and an account in a foreign currency with maturity on a specified banking day, with the funds debited and credited to the client's account on that day	By 3:00 p.m.
Cross-border order – standard payment abroad / foreign currency at home	Sending a cross-border payment order to the beneficiary's bank with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on the next following banking day	By 3:00 p.m.
Cross-border order – payment in foreign currency within UniCredit Bank	Sending a cross-border payment order (with or without conversion) in a foreign currency between accounts within UniCredit Bank with maturity on a specified banking day	By 3:00 p.m.
Cross-border order – urgent payment abroad / foreign currency at home	Sending a foreign payment order to the beneficiary's bank with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on the following banking day	By 1:00 p.m.
Standing order	**SEPA, cross-border (transfer of amount, balance, allocation for a default balance)**	
SEPA Standing Payment Order – placing	The **"Start Date"** field must indicate at least 1 working day before the date of the first settlement of the standing order. If a due date of a regular payment under the standing order falls upon a non-banking day, then the payment is made as instructed by the client (on the preceding or the following banking day).	By 9:30 p.m. D-1
SEPA Standing Payment Order – changing/cancelling	If the change/cancellation date is identical with the banking day for a regular payment under an existing standing order, then the change/cancellation of the standing order will become valid from the following banking day. This shall not apply to standing orders with a 1 day period, i.e., a one-day standing order can be changed/cancelled on the banking day scheduled for the regular payment.	By 9:30 p.m. D-1
Transaction authorisation	**To be signed, partially signed**	
To be signed (transaction authorisation)	All created transactions must contain the User's signature, otherwise the Bank will not process them. A maximum of 10,000 transactions / 1 signature can be authorised. Only a User authorised to sign the transactions under the Agreement (signature classes, transaction limit, shared signing, ...) has access to transactions to be signed.	Within 90 days of payment/ instruction creation

Business Smart Banking – Services

Transaction authorisation	**To be signed, partially signed**	
3DS card payment verification	Delivery of the confirmation message for 3DS card payments to the mobile app	–
Templates, beneficiaries	**SEPA, cross-border**	
Payment order templates	Possibility of saving details of SEPA or cross-border payment in a template for later use. Possibility of setting the template as private or shared by multiple Users.	–
Beneficiaries	Possibility of saving a record of a bank link to a domestic foreign trading partner for later use. Possibility of setting the template as private or shared by multiple Users.	–
	Other banking operations	
SEPA Direct Debit	**Authorisation, refusal, return**	
Request for refusal of SEPA Direct Debit	Request for refusal (non-execution) of an expected SEPA Direct Debit. The bank will not perform the Direct Debit, as instructed by the submitted parameters. The beneficiary's bank will be notified that the payer refused to make the payment.	4:00 p.m. D-1
Cards	**Card payment, additional services**	
Credit card repayment	Sending a SEPA payment order with predefined data for repayment of a credit card issued by UniCredit Bank with maturity on a specified banking day, with the funds debited from the client's account and credited to the credit card account on that day	By 9:30 p.m.
Displaying PIN	Possibility of displaying the PIN code to the company payment card	–
Card activation	Activating debit card	–
Card blocking	Temporary blocking of the card	–
TPP	**Access to account – TPP Consents**	
Granting consent to the Fund Check Service (FCS)	In order for the Bank to allow access to the client's account via a third party app, the client must consent to this. With valid consent, a third party can be informed of the availability of a specific amount in the account.	The consent is valid indefinitely.
Granting consent to the Indirect Payment Initiation Service (PIS)	One-time consent to the Indirect Payment Initiation Service is always given at the same time as signing a payment procured through a third party.	Consent is valid for the specific payment under which it was granted.
Granting consent to the Payment Account Information Service (AIS)	In order for the Bank to allow access to the client's account via a third party app, the client must consent to this. With valid consent, a third party can obtain information about the current balance and a statement of transactions for the selected period.	The consent is valid for 90 days from the date of signing.
Overview of consents to Open Banking services	An informative overview of all valid and invalid Open Banking consents. One-time consents to the Indirect Payment Initiation Service are not displayed.	–
Extending the validity of consent to the Indirect Payment Initiation Service (PIS)	It is not possible to extend the consent to the Indirect Payment Initiation Service, as the consent is always granted only for a specific payment at the same time as the payment is procured.	–
Extending the validity of consent to the Payment Account	It is not possible to extend the consent to the Payment Account Information Service.	–
Information Service (AIS)	It is not possible to extend the consent to the Fund Check Service because it is valid indefinitely until withdrawn.	The consent is valid indefinitely.
Temporarily deactivating and reactivating consent to the Fund Check Service (FCS)	It is not possible to temporarily deactivate the consent to the Fund Check Service; the consent can only be withdrawn.	–

TPP	Access to account – TPP Consents	
Temporarily deactivating and reactivating consent to the Indirect Payment Initiation Service (PIS)	It is not possible to temporarily deactivate the consent to the Indirect Payment Initiation Service.	–
Temporarily deactivating and reactivating consent to the Payment Account Information Service (AIS)	It is not possible to temporarily deactivate the consent to the Payment Account Information Service; the consent can only be withdrawn.	–
Withdrawing consent to the Fund Check Service (FCS)	The client may permanently withdraw the granted FCS consent at any time during its validity.	The consent shall cease to be valid from the moment of withdrawal.
Withdrawing consent to the Indirect Payment Initiation Service (PIS)	It is not possible to withdraw the consent to the Indirect Payment Initiation Service, as the consent is always granted only for a specific payment at the same time as the payment is procured.	–
Withdrawing consent to the Payment Account Information Service (AIS)	The client may permanently withdraw the granted AIS consent at any time during its validity.	The consent shall cease to be valid from the moment of withdrawal.
History of requests made in the Fund Check Service	An informative overview of what funds availability requests have been performed on client's accounts as part of the Fund Check Service. The following information is available to the client: • the request date; • the name of the third party and the name of its app; • the amount and currency: • the availability of funds sent by the Bank to a third party.	Maximum 6 months retroactively from the present day
	Other	
Mailbox	**Sending/receiving messages within the app**	
Messages	Displaying messages sent by the Bank	–
Information	**Exchange rates, interest rates, network of branches and ATMs**	
Exchange rate list	The exchange rate list is provided as non-binding information. If, in the course of a banking day, the exchange rate undergoes a significant change (e.g., owing to an intervention), the Bank reserves the right to amend the exchange list during the business day. A payment shall always be cleared using the exchange rate valid at the moment of the payment.	–
Map of branches and ATMs	Displaying UniCredit Bank branches and ATMs *Note:* *In order for the display to work properly, it is necessary to download data to the app via the HTTP protocol, and therefore, upon request of the browser, downloading data via this protocol must be enabled.*	–
Settings	**General settings, Bank settings, accounts arrangements**	
General settings	Setting contact details, setting the control data for blocking/unblocking the security tool. User's setting via the EB service is superior to the contractual arrangement with the Account Owner.	–
Bank settings	Possibility of setting a preferred account, card. Show/hide transaction history.	–
Notifications	**Automatic sending of banking information by Push notification**	
Notifications	A Push notification about transactions on the selected account after a defined event. Possibility of setting alerts for balance change, incoming payments and deposits, outgoing payments, card payments.	–

MultiCash – Parameters*

System requirements – minimum technical equipment	
Hardware	2GHz processor
	2GB RAM
	500 MB of hard disk space reserved for MultiCash
	CD-ROM, USB port (for installation purposes)
	Colour monitor with 1024×768 resolution, 8 MB graphics card
	Connected printer (for initiation procedure), keyboard, mouse
	Communication equipment (modem – analogue or ISDN, fixed internet connection)
Software	Windows Vista (Business or higher), Windows 7 or higher
	Adobe Acrobat Reader 8.0 or higher
	Internet Explorer 8.0 or higher installed
	TCP/IP protocol installed
Other	Installation CD ROM from the Bank
Data transmission – minimum technical equipment to carry out the transmission	
TCP/IP transmission	This type of communication uses the Internet as a communication medium. The communication is directly to the specific IP address and port of the Bank server. In the case of communication through a firewall (proxy server), it is necessary to allow access to the IP address and port defined by the Bank. This also applies when using a software firewall (BlackICE, ZoneAlarm, etc.) installed on the PC where MultiCash will be installed.
Security tools and identifiers when communicating with the Bank	
Electronic signature	Electronic signature (hereinafter referred to as ES) is used for authentication (verification of identity) of the User and authorisation (verification of content) of payment files sent to the Bank via the MultiCash system. The ES will be issued on the basis of the Agreement with the Account Owner. The User indicated on this application is required to generate his/her public and secret key to the ES in the MultiCash system, including the security password, and at the same time make an initiation connection to the bank server. At the same time, the Account Owner is obliged to deliver to the Bank a printed and signed document with the public key to the ES. Only on the basis of the delivered public key the Bank will activate the User. ES may only be used by the User named in the Agreement. In the event that such User can no longer or no longer wishes to use the relevant ES, the Account Owner is obliged to request cancellation of access to the ES features. The new User indicated by the Account Owner in the Agreement is required to generate his/her public and secret key to the ES in the MultiCash system, including the security password, and at the same time make an initiation connection to the Bank server. At the same time, the Account Owner is obliged to deliver to the Bank a public key to the ES printed and signed by him/her. Only on the basis of the delivered public key the Bank will activate the new User. Blocking of access to ES features will be carried out by the Bank solely at the request of the User and/or the Account Owner, provided that all instructions of the Bank's employee providing the above specified cancellation of access are complied with. Cancellation of access to ES features by the client shall be made by the Bank only upon a request signed by the Account Owner and delivered in writing, provided that all instructions of the Bank employee providing the cancellation of access are complied with. In case of blocking of access to EP functions by the client, the Bank will unblock only upon the written request of the Account Owner, provided that all instructions of the Bank's employee providing the unblocking are followed.
Working with the client app	The owner of the account/app shall set out in writing the access and signature authorisations for individual Users to individual accounts. The scope of authorisations for working inside the MultiCash system is set by the client administrator. The User logs into the MultiCash application using the Username and Password, and uses an electronic signature for authentication and authorisation. During transmission, the data is protected by special DES/RSA algorithms.
Transaction authorisation	The User authorises the sent active Orders with an electronic signature, which is registered in the Bank's electronic banking system. The electronic signature can be delivered from a single MultiCash app or from multiple (different) MultiCash apps/installations (distributed electronic signature functionality).

MultiCash – Parameters*

Secondary identifiers (when communicating with the Bank by phone)	Secondary identification: • User identification number (ID) (assigned by the Bank) • User's name and surname • the number of the account made available
Limits	
Daily limit	Unlimited, unless otherwise agreed in the Agreement for the User
Transaction limit	Unlimited, unless otherwise agreed in the Agreement for the User
Support	
Technical support	mail: **EB@unicreditgroup.sk** **+421 2 6920 2097** Banking days (Mon – Fri) 8:00 a.m. – 5:00 p.m.
Technical support standard activities	• Communication with clients using the MultiCash service via phone and e-mail • Blocking/unblocking* safety features • Blocking/unblocking a digital certificate • Receiving the client's problem, solution and announcement of the result • Communication with clients via e-mails, apps • Activating** safety features *)On the basis of an original written instruction from the User/Account Owner **)On the basis of an original written instruction from the Account Owner
Website	http://www.unicreditbank.sk/multicash
Software	
License	If the software is installed by the Bank for the Account Owner or another natural or legal person authorised by the Account Owner to operate the software (hereinafter referred to as the **"Authorised Operator"**), the Account Owner receives the right (license) to use the software for the purposes set out in the Manual. Neither the Account Owner nor the Authorised Operator shall thereby acquire ownership of the software, copies thereof or other materials supplied with the software. The Account Owner may not transfer this license to third parties without the Bank's consent.
Copying	If the software is not equipped with technical copy protection, the Account Owner or Authorised Operator is entitled to: • make a single copy of the software solely as a backup or for archiving purposes; or • transfer the software to a single hard drive, unless the original is retained solely for security or archiving purposes. Neither the Account Owner nor the Authorised Operator may copy the Product Manuals or other materials. It shall carefully store both the software and the materials to protect them against unauthorised use, reproduction, distribution or disclosure. Violation of these provisions constitutes a material breach of the Agreement.
Tampering with the software	Neither the Account Owner nor the Authorised Operator is authorised to decompile the software, decode it from machine code, reverse engineer (Reverse engineering) or remove or bypass the initiation system. If the software has been delivered on different data carriers, the Account Owner or Authorised Operator is entitled to use only one set of the delivered data carriers. Other carriers may not be used on another computer or computer network or rented, loaned or otherwise given to third parties. Violation of these provisions constitutes a material breach of the Agreement.
Installation	If the Bank installs the software, it is the responsibility of the Bank to ensure that the software operates in accordance with the Manual upon delivery. If the Account Owner nonetheless files a claim with the Bank for the software within 6 months of delivery, the Bank will remedy any curable defects that are technically feasible to repair by substitutable commercial means or provide a refund of the installation fees paid. Unless the software has been installed for the Account Owner by the Bank, the Account Owner represents and warrants that he/she uses the MultiCash software in accordance with applicable law.

MultiCash – Parameters*

Responsibility	The Bank is not responsible for damage caused by accident, misuse or improper handling of the software. In no event will the Bank reimburse direct or indirect damage, in particular not damage from loss of data that occur during the use of the software or from the inability to use the software for any reason whatsoever. If the SEPA Convertor tool is used, the Account Owner or Authorised Operator is responsible for the data in the input file (SKI file format) and is also responsible for checking that the data in the output file (pain.001.001.03) corresponds to the content of the payments in the input file (SKI format). The Bank is not responsible for any misuse of the SEPA Convertor.
Third party copyrights	If software is installed by the Bank for the Account Owner or the Authorised Operator, the Bank is responsible for ensuring that the Account Owner's and the Authorised Operator's use of the software does not infringe the copyrights and industrial property rights of third parties. The Account Owner and the Authorised Operator are obliged to notify the Bank without delay of any claims by third parties arising from the use of the software that the industrial property rights and copyrights of third parties have been infringed.
Termination of use	In the event of termination of the Agreement under which the Bank installed the software, the Account Owner or the Authorised Operator shall, on the date of termination of the contractual relationship, discontinue the use of the MultiCash software and remove the software from all computers on which it was installed.
Software update	The Bank is entitled to unilaterally make the MultiCash software update (hereinafter referred to as **"software update"**). The Bank will notify the Account Owner of this update in accordance with business practices and will deliver the new MultiCash software to the Account Owner. The Bank is entitled to make updates in the area of remote data transmission at any time in connection with technical progress as well as the introduction of additional security measures.
Entering/Changing Users	The Account Owner is not entitled to enter and change Users who identify themselves when entering the MultiCash system without the User or the change being made in the Agreement.
Fees	
Charging fees	**Service activation fees** are paid by the Account Owner and are payable upon conclusion of the Agreement. **The fee for accessing the account(s) via MultiCash** is paid by the Account Owner for each license (i.e., the right to use the relevant software for the MultiCash Electronic Banking Service, which allows one group of Users with different access rights to work with one common set of accounts (database), encrypted with a unique key), by which any of the Account Owner's accounts is made accessible via MultiCash to the Account Owner or to any other person. The fee for accessing the account(s) is payable on the last working day of the relevant month. **The new/additional payment module software installation fee** is paid by the Account Owner and is due upon installation. The amount of the fees is set out in the Price List applicable to the market segment in which the Bank classifies the Account Owner. The total amount of fees collected depends on the contractually agreed number of modules/functionalities.

* A description of the technical requirements and functionality as well as the terms and conditions of use are set out and described in detail in the User Manual, which is included in electronic form in the MultiCash installation (MSSWIN/DOC directory).

MultiCash – Services

Title	Description of the service	Time limit
Associated accounts and products		
Current accounts	**In all currencies, displaying account details and balances offline**	
Electronic statements	**Possibility of displaying and downloading daily statements in standard formats**	
Daily electronic statements – preview	Display, print and export daily electronic account statements	At least 15 months retroactively from the present banking day
Daily electronic statements – download	Possibility of downloading daily electronic statements in the format – MultiCash MT940 structured	At least 15 months retroactively from the present banking day
MT942 messages – preview	Overview of turnovers settled on the current day on accounts held with the Bank (display of MT942 messages) with the possibility of printing/ exporting	–
MT942 messages – download	Possibility of downloading MT942 messages in the MultiCash MT942 structured format	–
XML statements	Possibility of downloading electronic statements in XML format. Upon the Account Owner's request, the Bank will ensure the delivery of XML statements in the CAMT.053/CAMT.052 format. MultiCash may also require a software update	–
Cash management	**Overview of account balances held at UCB and other banks**	
Cash management	Overview of closing balances on accounts held at the Bank and closing balances on accounts held at other banks (view MT940 messages sent from other banks) with the possibility of totalling balances	At least 15 months retroactively from the present banking day
Archive records	**Order history, record of activities**	
Order history	List of authorised (signed) transactions submitted to the Bank for processing.	At least 15 months retroactively from the present banking day
Record of activities	List of activities performed by individual Users in the system. The time limit may vary according to the type of banking operation performed.	At least 6 months retroactively from the present banking day
Modules		
MCC module	A basic module that enables the connection of the client app with the Bank's server and the transmission of data (statements, payments, or other information prepared by the Bank for transmission to the client).	–
SKA module	The module for Slovak Foreign Payment (SKA) is an additional module of MultiCash. The foreign payments module can be used to create and send payment orders to one or more banks. The SKA module is based on the SWIFT international banking format.	Possibility of installing as part of an MCC installation (to be selected when starting the installation)
SPA module	The module for SEPA (SPA) is an additional module of MultiCash. The SEPA module can be used to create and send SEPA payment orders to one or more banks.	Possibility of installing as part of an MCC installation (to be selected when starting the installation)
Payments – Active operations		
SEPA	**SEPA Credit Transfer, SEPA Direct Debit**	
SEPA payment from EUR account	Sending a SEPA payment order in EUR within the EU27 and other European countries with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on the following banking day	By 9:30 p.m.
SEPA payment within UniCredit Bank	Sending a SEPA payment order between accounts within UniCredit Bank in EUR with maturity on a specified banking day, with funds debited from the client's account and credited to the beneficiary's account on that day	By 9:30 p.m.

MultiCash – Services

SEPA	SEPA Credit Transfer, SEPA Direct Debit	
SEPA payment from a foreign currency account	Sending a SEPA payment order in EUR from a foreign currency account within the EU27 and other European countries with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on the following banking day	By 3:00 p.m.
SEPA payment from EUR account – Urgent	Sending a SEPA payment order in EUR with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on that day *Note: The payee's bank is responsible for crediting the express payment on the day the payment is sent from the Bank. In case of non-compliance with the time limit, the beneficiary's bank should be contacted.*	By 2:30 p.m. urgent payment From 2:30 p.m. until 4:00 p.m. urgent payment via Target2
SEPA payment from a foreign currency account – Urgent	Sending a SEPA payment order in EUR with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on that day *Note: The beneficiary's bank is responsible for crediting the express payment on the day the payment is sent from the Bank. In case of non-compliance with the time limit, the beneficiary's bank should be contacted.*	By 2:30 p.m. urgent payment From 2:30 p.m. until 3:00 p.m. urgent payment via Target2
SEPA Direct Debit B2B order	Sending an order for SEPA Direct Debit B2B. The order must be submitted to the Bank 2 banking days before the due date. The Bank sends the order to the payer's bank the day before the due date (D-1) in order to comply with SEPA rules	By 9:30 p.m. D-2
SEPA Direct Debit CORE order	Sending an order for SEPA Direct Debit CORE. The order must be submitted to the Bank 6 banking days (First Recurring, One-Time), 3 banking days (additional Recurring) before the due date. The Bank sends the order to the payer's bank the day before the due date (D-1) in order to comply with SEPA rules	By 9:30 p.m. D-6
Cross-border payments and conversions	**Standard, domestic in foreign currency, foreign currency within the Bank, conversions, cheque payments**	
Transfer between the client's own accounts in the same foreign currency	Sending a payment order between accounts made available to the User and held with UniCredit Bank in the same foreign currency, with maturity on a specified banking day, with the funds debited and credited to the client's account on that day	By 3:00 p.m.
Conversion between the client's own accounts	Sending a payment order between accounts made available to the User and held with UniCredit Bank in different foreign currencies or between an account in EUR and an account in a foreign currency with maturity on a specified banking day, with the funds debited and credited to the client's account on that day	By 3:00 p.m.
Cross-border order – standard payment abroad / foreign currency at home	Sending a cross-border payment order to the beneficiary's bank with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on the next following banking day	By 3:00 p.m.
Cross-border order – payment in foreign currency within UniCredit Bank	Sending a cross-border payment order (with or without conversion) in a foreign currency between accounts within UniCredit Bank with maturity on a specified banking day	By 3:00 p.m.
Cross-border order – urgent payment abroad / foreign currency at home	Sending a foreign payment order to the beneficiary's bank with maturity on a specified banking day, with funds debited from the client's account on that day and credited to the beneficiary's bank on the following banking day	By 1:00 p.m.
Standing order	**SEPA, cross-border (transfer of amount, balance, allocation for a default balance)**	
Standing payment order – SEPA	Entering a standing order is only valid for the MultiCash client app. Execution is conditional upon the transfer order generated on the basis of this standing order in the Multicash client app being sent to the Bank's server on the due date of this transfer order. The standing order is entered in the SPA module.	–

MultiCash – Services

Standing order	**SEPA, cross-border (transfer of amount, balance, allocation for a default balance)**	
Standing payment order – Cross-border	Entering a standing order is only valid for the MultiCash client app. Execution is conditional upon the transfer order generated on the basis of this standing order in the Multicash client app being sent to the Bank's server on the due date of this transfer order. The standing order is entered in the SKA module.	–
Import	**SEPA, cross-border payment orders, custom data format**	
Uploading payment files	Possibility of uploading payment files with SEPA Credit Transfers (XML pain format via the SPA module) or Cross-border (non SEPA) orders (MultiCash format via the SKA module)	–
SEPA Convertor	Tool to convert SKI import format to SEPA format (pain.001.001.03). The Bank provides technical support for this tool until 30 June 2017.	Possibility of access upon request
Transaction authorisation	**Remote signature**	
To be signed (transaction authorisation)	All created transactions must contain the User's signature, otherwise the Bank will not process them and will return an error message to the User about the incorrect signature of the file.	–
Distributed signature Remote signature	The MultiCash User creates a payment file (containing payment orders) and adds their first signature. After it is sent to the Bank server, the file is ready to be picked up by the second (additionally signing) MultiCash app. Once the file has been transferred to the second MultiCash app, the file can be further signed and submitted to the Bank for processing.	Payment files for which only the first signature has been received are registered on the Bank's communication server for a maximum of 30 calendar days – including the date of delivery of the payment file with the first electronic signature. If the second (confirming) electronic signature is not received within this period, the Bank will cancel the payment file.
Templates, beneficiaries	**SEPA, cross-border**	
Payment order templates	Possibility of saving details of SEPA or cross-border payment in a template for later use. Possibility of setting the template as private or shared by multiple Users.	–
Beneficiaries	Possibility of saving a record of a Bank link to a domestic foreign trading partner for later use. Possibility of setting the template as private or shared by multiple Users.	–
Other banking operations		
SEPA Direct Debit	**Authorisation, refusal, return**	
SEPA Direct Debit mandate	Entering/changing/cancelling SEPA Direct Debit mandate with effect from the next following banking day. When delivered to the Bank on a non-banking day, entering, changing and cancelling the Direct Debit mandate will be valid on the next following banking day.	9:30 p.m. D-2
Request for refusal of SEPA Direct Debit	Request for refusal (non-execution) of an expected SEPA Direct Debit. The Bank will not perform the Direct Debit, as instructed by the submitted parameters The beneficiary's bank will be notified that the payer refused to make the payment.	4:00 p.m. D-1
Request for refund of SEPA Direct Debit	Request for refund of financial funds from a settled SEPA Direct Debit. The Bank shall refund the funds withdrawn and inform the beneficiary's bank of the reason for cancelling the transaction.	4:00 p.m. D-1

MultiCash – Services

Other		
Mailbox	**Sending/receiving messages within the app**	
Mail (incoming / outgoing)	Possibility of sending/receiving messages between the Bank and the User	–
Information	**Exchange rates, interest rates (offline)**	
Exchange rate list	The exchange rate list is provided as non-binding information. If, in the course of a banking day, the exchange rate undergoes a significant change (e.g., owing to an intervention), the Bank reserves the right to amend the exchange list during the business day. A payment shall always be cleared using the exchange rate valid at the moment of the payment.	–

European Gate – Parameters

Access to accounts	
Passive connection	The Bank is defined in the Agreement as the **"Account-Keeping Bank"** and is able to **"receive"** transfer orders sent via the EuropeanGate channel from a UniCredit Group Bank, defined in the Agreement as the **"Sending Bank"**, which has an active connection to EuropeanGate.
Payment orders	Payment orders sent to the Bank via the EuropeanGate service must comply with the GBTC as well as the Bank's Business Terms and Conditions for the Provision of Payment Services. Payment orders sent to the Bank via the EuropeanGate service must be delivered to the Bank in the required format necessary for the settlement of payment orders.
Responsibility	The Bank is not responsible for any damage resulting from the failure to settle payment orders received by the Bank in the incorrect format.
Support	
Technical support	mail: **EB@unicreditgroup.sk**
	+421 2 6920 2097 Banking days (Mon – Fri) 8:00 a.m. – 5:00 p.m.
Technical support line standard activities	• Support and testing of transfer orders, in a contractually agreed format • Receiving the client's problem, solution and announcement of the result
Fees	
Charging fees	The fees for the EuropeanGate service are paid by the Account Owner. The amount of the fees is set out in the Price List applicable to the market segment, the fee is payable on the last working day of the relevant month.

SWIFTNET – Parameters

Access to accounts	
Description of the service	The SWIFTNET service allows corporate customers who are SWIFT members to communicate with the Bank via the SWIFT network by sending transfer orders via the SWIFT FIN service (SWIFT MT message format) or the SWIFT FileAct service (communication in the form of files in contractually agreed formats for payment files and statements) directly from their SWIFT address to the Bank's SWIFT address. In addition, through the EuropeanGate service, the client can deliver transfer orders in this way to any UniCredit Group Bank that is connected to EuropenGate. The SWIFTNET service is thus the entry point for the delivery of transfer orders to the UniCredit Bank Group group of banks by a corporate client.
Payment orders	Payment orders sent to the Bank via the SWIFT FIN / SWIFT FilleAct service must comply with the GBTC as well as the Bank's Business Terms and Conditions for the Provision of Payment Services. Payment orders sent to the Bank via the SWIFT FIN / SWIFT FilleAct service must be delivered to the Bank in the required format necessary for the settlement of payment orders.
Responsibility	The Bank is not responsible for any damage resulting from the failure to settle payment orders received by the Bank in the incorrect format.
Support	
Technical support	mail: **EB@unicreditgroup.sk**
	+421 2 6920 2097 Banking days (Mon – Fri) 8:00 a.m. – 5:00 p.m.
Technical support line standard activities	• Support and testing of payment orders, in a contractually agreed format • Receiving the client's problem, solution and announcement of the result
Fees	
Charging fees	The fees for the SWIFTNET service are paid by the Account Owner. The amount of the fees is set out in the Price List applicable to the market segment, the fee is payable on the last working day of the relevant month.

UniCredit Bank

PRINCIPLES OF SECURE COMMUNICATION AND DATA PROTECTION

Following these simple rules will allow you to securely control your accounts via internet banking products and minimise the risk that your personal data will be misused by unauthorised persons.

Login details, passwords, PINs

- Never disclose your security information (User ID, password, PIN, security code) to another person.
- Avoid using Internet Banking products in public (such as while using public transportation) and in monitored rooms (such as in the sight of security cameras).
- Be conscientious about your privacy and check that other people cannot observe your login data, especially when logging in.
- Do not work with Internet Banking using computers you cannot ensure do not contain malware (e. g. in public internet cafés).
- Do not leave your computer or mobile phone unattended; use keyboard locks and device access codes.

E-mail

- The Bank never sends e-mails calling for disclosure of identification information, passwords, PINs, etc. Do not respond to such calls and please inform the UniTel client line.
- Open only trustworthy e-mails from known and expected senders. If an e-mail seems suspicious, it is risky to open it and to work with the attachments and links.

Internet

- You should only visit known and trustworthy websites on the Internet.
- Avoid downloading unknown files from the Internet to your computer. They can conceal dangerous programs and viruses.
- Be especially cautious when using open wireless networks (use only trustworthy Wi-Fi connections).
- If the login screen for your direct banking products seems suspicious in any way, do not log in and contact the UniTel client line.

Mobile app

- You should only install apps from official app stores to your mobile phones – Google Play (Android), App Store (iOS).

Viruses

- You should update the program regularly.
- We recommend using up-to-date versions of anti-virus programs that also include malware detectors.
- We also recommend using a firewall on your computer.
- Even smartphones and tablets should be provided with anti-virus protection.

Operating system, web browser

- Update your computer's operating systems with security patches or by using update packages issued by the manufacturer.
- You should also update your programs regularly; it is especially important to update your web browser and its plugins (e. g. Flash Player).
- For smartphones and tablets, we also recommend using the current versions of firmware officially offered by the manufacturer for the device.

You should check your account balances and transactions regularly – for example, by text messages or e-mails with the appropriate content.

In the event of suspected fraud, or security threat, the Bank shall inform the client in a suitable manner, using primarily the contact details specified by the client when entering into the contractual relationship with the Bank, taking into account the security of the information shared among the parties.