# Cash Management User Guide

## Czech Republic

Treasury and Trade Solutions

citi

# Table of Contents



*The version in the Czech language continues on page 27/ Verze v českém jazyce pokračuje na straně 27*

# I. Introduction

Thank you for choosing Citi's Treasury and Trade Solutions (TTS) for your cash management business needs. The objective of this Cash Management User Guide (the "**User Guide**") is to provide Customers with a manual containing detailed information of Services offered to Customers by the Bank and is to be read together with your Account terms and conditions. This User Guide may be updated in the way stipulated in the Local Conditions.

Capitalized terms used in this User Guide, but not defined herein, shall have the meaning defined in the Local Country Conditions for Accounts held and Services provided in the Czech Republic (the "**Local Conditions**") or, if such term is not defined in the Local Conditions, in the Master Account and Service Terms ("**MAST**").

In this User Guide the **Bank** or **Citi** means Citibank Europe plc, a company established and existing under Irish law, registered seat at North Wall Quay 1, Dublin, Ireland, registered in the Register of Companies in the Republic of Ireland, under the number 132781, conducting its business in the Czech Republic through Citibank Europe plc, organizační složka, registered seat at Prague 5, Stodůlky, Bucharova 2641/14, Postal Code 158 02, Reg. No. 28198131, registered in the Commercial Register with the Municipal Court in Prague, Section A, Insert 59288.

# II. Payment Services

## A. Types of Payments Services in Czech Republic

- Book Transfers: Transfers of funds between Citi Accounts in Czech Republic
- Domestic Funds Transfers: Funds transfers via the CERTIS (Czech Express Real Time Interbank Gross Settlement) system, the Czech National Bank's clearing system., which supports both high-value and low-value transfers, processed either in the standard regime (ACH) or as urgent transfers under the express regime.
- Single European Payments Area (SEPA): EUR clearing mechanism for low-value, high-volume payments, which includes both a mandate-based direct debit service and a credit transfer service for individual, bulk, same day, or a combination of bulk and same day credit transfers.
- Direct Debits: A means of collecting monies owed by a payer, where the beneficiary ("originator") generates the initiating transaction to be processed by the payer's bank against the payer's account. Direct debits, which are always subject to the payer's authorization, are typically used for recurring payments, such as credit card and utility bills, where the payment amounts vary from one payment to another.
- Cross Border Funds Transfers: Allow Customers to make international transfers in a wide range of currencies as outgoing telegraphic transfers, including international Czech currency payments.

## B. Sending a Payment

1. The Customer sends a Payment Order to Citi, formatted to market standards and as outlined at the time the payment service was implemented, via:
    - Citi e-banking channels, which include CitiDirect BE® and CitiConnect®,
    - A SWIFT interface, or
    - A manual request (restrictions apply)
2. Citi forwards the instruction to the relevant payment system for further processing.
3. The payment system forwards the instruction to the beneficiary bank based on the locally defined clearing cycle.
4. The beneficiary bank credits the beneficiary account.

## C. Receiving Direct Debits (Payments)

Citi, as the Customer's paying Bank, supports direct debit mandates or instructions received from other participating financial institutions.

1. Citi validates the transaction received against the direct debit mandate (or equivalent) previously communicated by the Customer to Citi before payments are made.

2. If the direct debit payment is in compliance with the direct debit authorization, Citi processes the instruction and debits the Customer's Account.

3. In the event there is no direct debit authorization or insufficient funds in the Customer's Account, Citi will not process the direct debit payment and sends the unsuccessful debit status back to the direct debit payment system or partner banks.

Citi will reverse any entry passed erroneously and debit or credit the relevant Account.

## D. Payable Cheques

Citi Czech Republic can issue WorldLink® cheques in any of the supported foreign currencies. WorldLink® cheques can be drawn on a Citi account with a local Citi entity or on a Citi account with a third-party bank. A WorldLink® cheque is cleared as a domestic cheque in the country where it is drawn. For instance, a WorldLink® cheque in SGD is drawn by Citi Singapore and is processed as a domestic cheque if deposited in Singapore. If this WorldLink® cheque in SGD is deposited outside Singapore, the beneficiary bank will clear it cross border.

The validity period of a payable cheque is determined by applicable laws and banking practices, from the date mentioned on the cheque upon its issuance. The last day of such period is known hereafter as the "expiry date". Subject to applicable local laws and banking practices, if any such payable cheque is not presented for payment on or before the expiry date, the Bank will not honor the cheque.

As there is no CZK cheque clearing mechanism in the Czech Republic, Citi will not issue CZK cheques.

### 1. Issuance and Processing of WorldLink® Cheques

1. The Customer communicates the instructions via the agreed Citi e-banking channel.

2. Citi debits the Customer's Account and prints the cheque(s).

3. Citi sends the cheque(s) to the payee(s)' address specified in the Customer's instruction or to the Customer address maintained at Citi.

4. The payee(s) deposit the cheque(s), which are presented back to Citi via local clearing arrangements.

5. Cheques are validated and funds will then be made available.

6. The Customer will be informed of any issues with the cheque(s) that have been presented.

7. Citi will not make a payment if it considers a cheque/draft to be materially altered, forged, counterfeit or stolen, or at the request of a competent judicial, quasi-judicial, regulatory, government or supervisory authority

   If a WorldLink® cheques is not presented for payment on or before the expiry date, the Bank will not honor the cheque and will, subject to applicable laws and banking practices, either upon the Customer's request or at the Bank's reasonable discretion and at a reasonable time after the expiry date, credit to the Account the amount of that payable cheque or otherwise return such amount to the Customer.

### 2. Stop Payment Requests on Payable Cheques

The Customer may request that the Bank put a stop payment on any payable cheque in case of lost, misplaced or cancelled cheques, in accordance with the Bank's procedures and applicable local laws. Citi recommends using the Citi standard form for stop payment, which can be obtained by contacting the Citi Service Desk.

1. The Customer communicates the stop payments instructions to Citi. The stop payment instructions will specify the serial number of the cheque, the date of issue, the payee's name and the amount. Stop payment on cheques will be effected based on the information specified in such instructions

2. For WorldLink® cheques, if the cheque to be stopped has not been paid, the Bank will refund the proceeds of all stop payment requests and cancellations to the Account from which the payments were derived, except in cases where the Customer requests that a replacement cheque to be issued.

3. If the lost, misplaced, or stolen cheque or draft is later found, the Customer is required to deliver the original cheque or draft to Citi immediately

The Bank will have the reasonable discretion on whether to accept the Customer's instructions to countermand or stop payment of cheques.

## E. Cash Delivery Service

Citi offers door-to-door delivery of cash in Czech Republic using a service provider acceptable to the Bank and the Customer and with which the Customer concluded a respective agreement on provision of such service. The Customer may use this service based on the cash processing and handover service application, which must be completed and signed on behalf of the Customer and delivered to the Bank (the "**Cash Application**"). The Agreement between the Bank and the Customer on provision of the Cash Delivery Service is concluded by the delivery of the completed Cash Application to the Bank (the "**Cash Delivery Agreement**") subject to the condition that the Customer has also entered into an agreement for the provision of the relevant services with a service provider acceptable to the Bank.

### Cash Delivery Process

1. The Customer submits, via the person entitled to act on its behalf, andvia the CitiDirect BE® electronic banking system, a request to withdraw and prepare cash for handover to the service provider, who arranges delivery of the physical cash to a chosen location at a pre-agreed time. The request must indicate the following:

   - Amount, including currency and split of banknotes denominations
   - Customer's Account to be debited
   - Name of the service provider who will pick up the cash at Citi premises
   - Date of the requested cash delivery pickup
   - Designated person (employee name and title)

The Request (herein after the “Request”) shall be delivered to the Bank at least two business days (until 9:30 a.m.) prior to the intended day of cash delivery.

2. According to the Request, the Bank shall duly and in a timely manner make a specific amount of cash in the required currency ready for transportation.

3. The selected service provider delivers the cash (under the conditions stipulated in the mutual agreement between the Customer and the service provider) to the Customer’s designated person at the specified address (as agreed between the Customer and the service provider). The Bank will hand over the cash required by the Customer for transportation to the authorized personnel of the respective service provider in accordance with the terms and conditions in the Request.

4. The designated person receives and verifies the following, before acknowledging the cash delivery:

    - The amount of cash delivered
    - That no soiled banknotes have been delivered
    - The photo identify card of the service provider representative

5. The Customer’s designated person must show his or her photo identity card to the service provider representative for validation, in line with the mutual agreement.

6. Delivery feasibility and turnaround time is based on the location and amount of cash to be delivered.

7. The Customer shall ensure that the cash amount that the Customer wishes to collect from the account is not higher than the account balance available on the account during the period starting on the second business day before the requested cash delivery date and ending upon the debit of the Customer’s account. The request will only be honoured whereby the Customer has ensured that the cash amount which the Customer wishes to collect from the account is not higher than the account balance.

8. The cash amount shall be debited from the Customer’s account with the Bank one business day before the requested cash amount delivery day.

9. The Customer or the Bank may terminate the Cash Delivery Agreement under the conditions set in the Master Account and Service Terms for the termination of the Service.

# III. Receivables Services

## A. Types of Payments Services in Czech Republic

- Domestic Incoming Payments: Domestic payments credited to the Customer's payment account in CZK that are accepted through the clearing centre of the Czech National Bank from other providers on the Czech market (i.e. the payer's provider or an intermediary provider).
- SEPA Incoming Payments: Payments credited in EUR, from payment service providers within the SEPA Area, transferred to the payer's provider via the SEPA channel.
- Foreign Incoming Payments: Foreign currency credit payments from providers in the Czech Republic and international foreign currency credit payments.

Any rejections or returns by Citi will be credited back to the payer's account or returned to the payer's bank. The reason for the return is communicated to the payer's bank.

## B. Direct Debits Collections

A direct debit collection is a financial transaction originated electronically from the Customer to Citi instructing the Bank to withdraw funds from a payer's bank account.

Direct Debit payments in CZK are made at the request of the beneficiary. The holder of the debited account must provide its payment service provider with a direct debit approval specifying the beneficiary's account number and authorising the provider to effect such a transfer of funds. This direct debit approval must be delivered before the collection cycle.

### Direct Debit Collection Process

1. The Customer ensures that the payer has the direct debit authorization in place before initiating a direct debit instruction to Citi.
2. The Customer initiates the transaction and communicates the bulk instruction file to Citi via the agreed Citi e-banking channel.
3. Citi validates that the transaction requests contain the information required to process them.
4. Citi communicates the direct debit transactions to the receiving payer banks via the clearing system.
5. Citi credits the funds to the Customer's Account on the same day the Bank's receipt of the incoming funds from clearing system.

The Customer should not initiate any further instructions with regard to a mandate if an instruction is returned for any of the following reasons:

- Account closed or transferred
- No such account
- Account description does not tally

- Insufficient funds in the account (for three preceding cycles)
- Underlying mandate has been revoked by the Customer

## A. Cheque Deposits

The Customer can deposit cheques at a Citi branch via the following options:

- Over the counter; or
- Via post

When depositing cheques, the Customer must complete a deposit slip to instruct with details of the Citi account to credit the cheque proceeds. The deposit slips can be obtained from a Citi branch.

All cheque deposits received by Citi on a working day (Monday – Friday) before the cut-off time are sent for cheque collection on the same day. A cheque deposited on a public holiday or weekend will be sent on the next working day.

Citi will credit the Customer's Account with the total cheque deposit amount on the second business day after the Bank receives the incoming funds. If the credit is revoked by the clearing system or payer bank, Citi will debit the Customer's Account for the amount originally credited for the dishonoured item

## B. Over-the-Counter Collections

The Bank offers over-the-counter services at Citi branches, where the Customer can deposit cheques and cash.

## C. Cash Collection Service

Citi offers door-to-door cash collection using a dedicated service provider. The services include the following:

- Cash Collection**:** Pickup of physical currency notes and coins from the Customer's premises at a pre-agreed time for delivery to cash collection/counting centres
- Cash Processing: Counting and processing (sorting and packaging) collected cash in designated cash counting centres and crediting the Customer's Account

### Cash Collection Process

1. The Customer must conclude an agreement directly with the service provider of its choice that is acceptable to the Bank and further agree to the:
    - Address where cash will be picked up
    - Approximate cash amount to be picked up
    - Customer's Account to be credited
2. The appointed service provider picks up cash from the Customer's designated location on the day agreed in the mutual agreement. The Customer counts the cash, places it in

a tamper-proof self-seal plastic bag and completes a paying-in slip (deposit slip) provided by the service provider.

3. Service provider representatives collect the cash.
4. The collected cash is transported to the designated cash counting centre(s).
5. The cash is inspected for defective, counterfeit or unacceptable notes and counted. The authenticity and condition of the currency notes and coins is verified by the service provider and the Customer's Account is credited accordingly.
6. Currency notes or coins found to be counterfeit will be dealt according to applicable laws and regulations; any related costs or consequences are the Customer's responsibility.

# IV. Other Provisions

1. Refusal to Execute Payment Orders and Other Instructions

   a. The Bank may refuse to execute a Payment Order if:

      i. the Payment Order does not reach the Bank in the form, time limit and manner defined by the Bank or agreed between the Customer and the Bank or if any data required by the Bank are missing from the particular Payment Order;

      ii. the Payment Order is not submitted by a person authorised to submit the Payment Order, or is not signed in accordance with the specimen signature kept by the Bank;

      iii. there are doubts regarding the content, creation or authorisation of persons authorised by the Customer to give the Payment Order;

      iv. the Payment Order is outside the usual manner of giving instructions by the Customer or is outside the usual manner of carrying out payment transactions for the Customer;

      v. there is any overdue debt owed by the Customer to the Bank;

      vi. grounds authorising the Bank to block the payment instrument exist;

      vii. the Customer's account lacks sufficient available funds;

      viii. in the case of a Payment Order initiated by the payee, the Bank is not provided with the Customer's consent to the transaction or the Customer's Payment Account is blocked against such Payment Order;

      ix. the Payment Order was delivered through a means of communication that has not been agreed;

      x. other conditions for execution of the Payment Order are not satisfied or the conditions defined in this User Guide or in another agreement or document between the Bank and the Customer allowing the rejection of a Payment Order are satisfied; or

      xi. a generally binding regulation provides so.

   b. Notwithstanding the provisions of the above, if there is any reason authorising the Bank to refuse to execute a Payment Order the Bank shall also be entitled not to refuse such a Payment Order, and:

      i. provided that the respective conditions are fulfilled no later than within five business days after the Bank has received the Payment Order, it may execute the Payment Order after the relevant conditions have been fulfilled; or

      ii. provided that the respective conditions are not fulfilled within five business days after the Bank has received the Payment Order, it may subsequently refuse to execute such order.

However, the above-specified provisions shall not restrict the right of the Bank to refuse to execute such a Payment Order at any time (i.e. even during the above-specified time limit of five business days).

c. If the Bank refuses to execute a Payment Order, the Bank shall inform the Customer by phone from the Bank's customer service or in any other manner of communication as may be agreed between the Bank and the Customer.

d. The Customer must pay a fee according to the List of Charges for the information concerning the refusal of a Payment Order.

e. The Bank may refuse to execute any Customer's instruction other than a Payment Order for the same reasons for which the Bank is entitled to refuse to execute a Payment Order under points i. to iv. of clause 1.a. above.

2. Blockage of Payment Instruments

a. The Bank may block at any time the payment instrument: (i) for payment instrument security reasons, especially when there is reason to believe that the payment instrument has been used without authorisation or fraudulently; or (ii) due to a significant increase in the risk that the Customer (or the holder of the payment instrument) might not be able to repay the credit available for use through the payment instrument.

b. The reasons for which the Bank may block the payment instrument specified in the terms and conditions for each payment instrument, or in any other documentation related to these payment instruments, do not preclude the Bank from blocking the payment instrument under a. of this Clause.

3. Return of Amounts of Authorised Payment Transactions

a. The Customer (payer) may request the return of an amount of an authorised Payment Transaction only if such Payment Transaction was initiated by the payee within the SEPA Direct Debit Core Scheme.

b. The Customer agrees that if the amount of any authorised transaction is returned from a transaction that was effected on the payee's initiative and where, the payee is the Customer and the payee's provider is the Bank, the Bank may debit funds from any of the Customer's accounts to return the amount of this authorised transaction if the payer demands a refund in accordance with generally binding legal regulations.

4. SEPA Direct Debit Conditions

a. SEPA direct debits are performed either within the SEPA Direct Debit Core Scheme or the SEPA Direct Debit B2B Scheme.

b. Unless the relevant legal regulations concerning SEPA collections require otherwise, all Payment Accounts of the Customer are open to SEPA collections performed within the SEPA Direct Debit Core Scheme, which means that the Bank effects all those orders for SEPA collection that were filed within the SEPA Direct Debit Core Scheme from the Customer's Payment Accounts. The Customer has the right to instruct the Bank to block all direct debits to the Customer's Payment Account performed within SEPA Direct Debit Core Scheme or to block any such direct debits initiated by one or more specified payees or authorise direct debits only initiated by one or more specified payees.

c. The Customer has the right to instruct the Bank to verify each direct debit transaction made under the SEPA Direct Debit B2B Scheme, and to check whether the amount and periodicity of the submitted direct debit transaction is equal to the amount and periodicity agreed in the mandate, before debiting its Payment Account, based on the mandate-related information.

d. For direct debits made under the SEPA Direct Debit Core Scheme and the SEPA Direct Debit B2B Scheme the Customer has the right to instruct the Bank to limit a direct debit collection to a certain amount or periodicity or both.

e. Any Customer instruction for the manual set up on the Bank side has to be delivered to the Bank no later than by 11 a.m. on the second business day before the commencement of the collection cycle.

# V. Statements of Accounts

1. The Bank provides the Customer with Account statements only if this is agreed upon between the Bank and the Customer in writing. However, if no payment transaction has been performed during the previous period for which the Account statement is to be provided pursuant to the agreement between the Bank and the Customer, the Account statement is not created for this period and is not provided for this period to the Customer.

2. Account statements can be sent by the Bank only in the English or Czech language, with or without transaction details, and they can only be sent daily, weekly, monthly or upon movement on the Account. Unless the Customer agrees with the Bank in writing otherwise, all Account statements shall be in the English language, contain transaction details and be sent upon movement on the Account.

3. If the Bank agrees in writing with the Customer in writing on delivery of Account statements then, unless agreed otherwise, the Bank provides the Customer with Account statements free of charge via electronic post (e-mail), the Bank's standard form of provision of Account statements. If the Bank and the Customer agree in writing on delivery of printed Account statements, the Bank sends such statements to the Customer's correspondence address and may charge the Customer in accordance with the current List of Charges.

4. Delivery of Account statements via electronic post (e-mail) is subject to the following additional provisions:

    a. the Bank starts to send Account statements to the Customer via electronic post (e-mail) only after the Customer has provided to the Bank in writing the contact information (i.e., name, e-mail address and telephone) of the persons to whom Account statements are to be sent and their e-mail addresses have been activated by the Bank via its CitiService department in accordance with internal regulations of the Bank. The Bank shall send Account statements in password-protected files. Passwords are set and may be changed in the future in accordance with the Bank's internal regulations via its CitiService department;

    b. the Customer can change contact information of the persons to whom Account statements are to be sent by delivering a written notice to the Bank. Any such change becomes effective upon its processing by the Bank via its CitiService department in accordance with the Bank's internal regulations;

# VI. Other Considerations

The Customer will make its own assessment of the legal, regulatory, tax and accounting implications of the services.

From time to time, the Bank shall deliver to the Customer fee schedules, procedures, requirements, guides, manuals and other materials describing the procedures, requirements and limitations surrounding the use of the services.

The clearing of payments is governed by the rules set by the corresponding clearing system. Both Citi and its customers must adhere to these clearing rules.

# VII. TTS Consolidated Security Procedures

As referenced in the Communications section of the Master Account and Service Terms (or other applicable account terms and conditions) ("MAST") that has been entered into between the Customer and the Bank the following is a description of the security procedures ("Procedures") used by Citi Treasury and Trade Solutions in connection with the following Services or connectivity channels.

- CitiDirect BE® (including Electronic Bank Account Management ("eBAM")), TreasuryVision®, and WordLink®)
- Interactive Voice Response ("IVR")
- Email/fax with the Bank excluding Manually Initiated Funds Transfer (MIFT)
- CitiConnect
- Other local electronic connectivity channels

Availability of the Services or connectivity channels will vary across local markets. These Procedures may be updated and advised to the Customer by electronic means or otherwise from time to time. Customer's continued use of any of the above noted services or connectivity channels after being advised of updated Procedures (which may include, but is not limited to, the posting of updated Procedures on CitiDirect BE®, in connection with the service or connectivity channel) shall constitute Customer's acceptance of such updated Procedures. These Procedures are to be read together with the MAST as such MAST may be amended from time to time. Capitalized terms not otherwise defined herein shall have the meanings ascribed to them in the MAST.

## A. Security Manager Roles and Responsibilities*

For the applications accessible in CitiDirect BE®,, the Bank requires two separate individuals to input and authorize instructions; therefore a minimum of two Security Managers are required. Any two Security Managers, acting in concert, are able to give instructions and/or confirmations through the connectivity channels in relation to any Security Manager function or in connection with facilitating our communication via the Internet. Any such Communications, when authorized by two Security Managers, will be accepted and acted on by the Bank. The Bank recommends the designation of at least three Security Managers to ensure adequate backup. The Customer shall designate its Security Managers on the TTS Channels Onboarding Form. A Security Manager of the Customer may also act as the Security Manager for a third party entity (for instance, an affiliate of the Customer) and exercise all rights relating thereto (including the appointment of users for that third party entity's Account(s)), without any further designation, if that third party entity executes a Universal Access Authority form (or such other form of authorization acceptable to the bank) granting the Customer access to its Account(s). This only applies in relation to Account(s) covered under the relevant authorization.

*Security Manager Roles and Responsibilities may be prohibited in certain local market. Please contact your Customer Service representative for further information

The Security Manager function includes, but is not limited to:

1. Establishing and maintaining the access and entitlements of users (including the Security Managers themselves), including activities such as:

    a. creating, deleting or modifying User Profiles (including Security Manager Profiles) and entitlement rights (please note that user name must align with supporting identification documents)

    b. building access profiles that define the functions and data available to various users; and

    c. enabling and disabling user log-on credentials.

2. Creating and modifying entries in Customer maintained libraries (such as preformatted payments and beneficiary libraries) and authorizing other users to do the same

3. Modifying payment authorization flows.

4. Allocating dynamic password credentials or other system access credentials or passwords to the Customer's users

5. Notifying the Bank if there is any reason to suspect that security has been compromised.

Security Managers also assign transaction limits to users for those Bank products to which the Customer has access. These limits are not monitored or validated by the Bank; Customer should monitor these limits to ensure in compliance with Customer's internal policies and requirements, including but not limited to, those established by Customer's Board of Directors or equivalent.

Specifically related to the **eBAM Application**, the following roles are required:

The initial set-up on the eBAM Service requires the designation of three Security Officers and one Corporate Secretary. Two separate Senior Administrative Roles act in concert as maker/checker to set up and assign User function/data entitlements and Workflows. These arrangements are not monitored or validated by Bank; Workflows and User activity are monitored by the Customer to ensure compliance with Customer's (and Account Owners') internal policies, requirements, and authorization and approval levels, including but not limited to those established by the Customer's (and Account Owners') Board of Directors or equivalent governing body.

The following roles are required for the eBAM Service:

1. **Security Officer:** Fulfil the functions described in 1. a-c above within the roles of Security Managers;

2. **Corporate Secretary:** Ensures that Workflows, Users set up as Designated Authorizers, and their assignment to Workflows meet internal policies, requirements, authorization and approval levels, as established by the Customer's (and Account Owners') Board of Directors or equivalent governing authority

3. **Designated Authorisers:** Have broad, senior authority to initiate and authorise workflow activities; and

4. **Request Initiators:** are individuals authorized to perform administrative activities such as entering account and signer management requests into the eBAM system.

The Security Officers, Corporate Secretary and Designated Authorisers are responsible for:

1. defining and administering hierarchy setup and site/flow control, such as establishing Workflows and identifying Users and levels of approval;

2. creating additional Senior Administrative Roles and appointing Users thereto (who may or may not be employed by the Customer)

3. notifying Bank if there is any reason to suspect that security or confidentiality of any User (including Senior Administrative Roles) credentials has been breached or compromised; and

4. where relevant, completing, amending, approving and/or supplementing such Customer implementation forms as may be reasonably requested by Bank from time to time in connection with the provision of services and/or products to Customer

## B. Authentication Methods

The Procedures include certain secure authentication methods ("Authentication Methods") which are used to uniquely identify and verify the authority of the Customer and/or any of its users typically through mechanisms such as User ID / password pairs, digital certificates, and security tokens (deployed via hardware or software) which generate a dynamic password used to access the services or connectivity channels each time the Customer or a user logs in or authenticates themselves. Please note that availability of the Authentication Methods described below varies based on local markets.

Security Managers and all users who want to (a) initiate or approve transactions (and whose User Profile permits them to do so) and/or (b) access the systems in accordance with entitlements must use the available Authentication Methods (which may be updated from time to time as described above).

The following Authentication Methods are available to access the above-noted services or connectivity channels in combination with a User ID:

| **Authentication Method** | **Description** |
|---|---|
| Token: Challenge Response | Either a (i) mobile application based soft token (e.g. MobilePASS) or (ii) physical token (e.g. SafeWord Card, Vasco) which in each case is used to generate a dynamic password after authenticating with a 4 digit pin. When accessing CitiDirect BE, the system generates a challenge, and a response passcode is generated by the utilized token and entered into the system. |
| Token: One Time Password | Either a (i) mobile application based soft token (e.g. MobilePASS) or (ii) physical token (e.g. SafeWord Card, Vasco) which is used to generate a dynamic password after authenticating with a 4 digit pin. This dynamic password is entered into the system to gain access. |
| SMS One-Time-Code | A dynamic password is delivered to a user via SMS, after which the user enters the dynamic password and a secure password to gain access to the system |
| Voice One-Time-Code | A dynamic password is delivered to a user via an automated voice call, after which the user enters the dynamic password and a secure password to gain access to the system |
| MultiFactor Authentication | A dynamic password is generated via a SafeWord Card or MobilePASS token, after which such dynamic password is entered along with a secure password to gain access to the system. |
| Digital Certificates | A Digital Certificate issued by an approved certificate authority which is used for authentication. Digital Certificates utilize a Key Storage Mechanism and a |

| | |
|---|---|
| | corresponding PIN, and may be issued by IdenTrust, SWIFT (3SKey) or other agreed-upon providers. |
| Secure Password | A user enters their secure password to access the system. A Secure Password typically limits a user's capabilities on the system, such that information can be viewed and no transaction capabilities are enabled. |
| Interactive Voice Response ("IVR") & email | Users contacting the bank will be prompted to enter a PIN number or provide other information to validate authorized access over the phone or over email. |
| Fax | Correspondence received by the Bank, excluding MIFT requests, will be signature verified based on the information that is contained in the Customer's board resolution. |
| MTLS | Mandatory Transport Layer Security (MTLS) creates a secure, private email connection between Citi and the external party. An email transmitted sent using this channel is sent over the Internet through an encrypted TLS tunnel created by the connection. |
| Secure PDF | Encrypted emails are delivered to a regular mailbox as a PDF Document that is opened by entering a private password, both the message body and any attached files are encrypted. A private password can be set up upon receipt of the first Secure Email received. |

To learn more about any of these Authentication Methods, please refer to the Login Help page on CitiDirect BE (https://portal.citidirect.com/portalservices/forms/loginHelp.pser)

### For CitiConnect®

- If the Customer chooses to use a public Internet connection to connect to Citi, including HTTPS, secure FTP, and FTPs, the Bank and the Customer will exchange security certificates to ensure both the communication channel and the messages exchanged are fully encrypted and protected. The Bank will only accept Communications originating from the Customer's secured using the exchanged security certificates, and vice versa, and the Bank will only transmit Communications to the Customer's using the exchanged security certificates.

- If the Customer chooses to use CitiConnect via SWIFT, then for any payment orders and instructions involving SWIFT, including amending or cancelling such orders, the Procedures that will be used to authenticate that a payment order or instruction is that of the Customer and authorized by the Customer shall be those as provided for in the SWIFT Contractual Documentation (as such term is defined by SWIFT and as may be amended or supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in any other terms and conditions that may be established by SWIFT. The Bank is not responsible for any errors or delays in the SWIFT system. Communications to the Bank are to be provided in the format and type required and specified by SWIFT.

- If using a VPN, both the Customer and the Bank will designate a single IP address from which Communications between the Customer and Bank will be sent and/or received. The Bank will only accept Communications originating from the Customer's designated IP address, and vice versa, and the Bank will only transmit Communications to the Customer's designated IP address, and vice versa.

- The Customer and the Bank may also use a Hardware Security Module Authentication to accompany VPN Authentication. This requires the Bank and the Customer each to install a device on the servers designated for Communications between the Bank and the Customer.

The Bank requires:

- Customer's safeguarding of the Authentication Methods including any log-on credentials and/or security certificates associated with the Authentication Methods (collectively, the "Credentials") and ensuring that access to and distribution of the Credentials are limited only to authorized persons of the Customer. The Authentication Methods and associated Credentials are the methods by which the Bank verifies the origin of Communications issued by the Customer to the Bank.

- The Customer should take all reasonable steps to protect the Credentials. Accordingly, the Bank strongly recommends that the Customer does not share the Credentials with any third party.

Certain jurisdictions may require individuals (and their corresponding credentials) to be identified as compliant with applicable AML legislation requirements before granting access to perform certain functions.

The Bank understands that the Customer may, in some cases, wish to share the Customer's Credentials with a third party entity or service provider (including without limitation any third party payroll provider) designated by the Customer to have access to the Customer's Credentials (such third party entity or service provider shall be referred to herein as an "Authorized Third Party") for the purpose of accessing and utilizing CitiConnect on the Customer's behalf. In the event that the Customer elects to share its Credentials with an Authorized Third Party, the Bank strongly recommends that the Customer takes, and ensure that any Authorized Third Party takes, all reasonable steps to protect the Credentials from being disclosed to any non-Authorized Third Party personnel. The Bank is authorized to act upon any Communication that it receives from an Authorized Third Party on behalf of the Customer in compliance with these Procedures.

## C. Data Integrity and Secured Communications

- The Customer will be transmitting data to and otherwise exchanging Communications with the Bank, utilizing the Internet, email and/or fax, which are not necessarily secure communication and delivery systems. The Bank, utilizes industry leading encryption methods (as determined by the Bank), which help to ensure that information is kept confidential and that it is not changed during transit.

- If the Customer suspects or becomes aware of, a technical failure or any improper access to or use of the Bank's services, connectivity channels or the Authentication Methods by any person (whether an authorized person or not), the Customer shall promptly notify the Bank of such occurrence. In the event of improper access or use by an authorized person, the Customer should take immediate actions to terminate such authorized person's access to and use of the Bank's services or connectivity channels.

- If Customer utilizes file formatting, encryption software (whether provided by the Bank or a third party), to support the formatting and recognition of the Customer's data and instructions and acts upon Communications with Citi, then the Customer will use such software solely for the purpose for which it has been installed.

# VIII. Further Information on Payment Processing

## A.Cut-Off Times for Delivery of Payment Orders

| **Standard Outgoing Payment Order Delivery Cut-Off Times** | | | |
|---|---|---|---|
| **Payment product** | | **Electronic transactions** | **Manual transactions (mail, fax, personal delivery)** |
| Domestic Funds Transfers | | 6:30 p.m. | 11:00 a.m. |
| Domestic Funds Transfers – Express* | | 12:00 p.m. | 9:00 a.m. |
| Cross Border Funds Transfers | | 3:00 p.m. | 11:00 a.m. |
| SEPA Credit Transfers SEPA Credit Transfers - Bulk | | 5:00 p.m. | - |
| SEPA Credit Transfers–Same Day/SEPA Credit Transfers–Same-Day Bulk | | 1:00 p.m. | - |
| Direct Debits | | 6:30 p.m. | 11:00 a.m. |
| Book Transfers | In a domestic currency | 6:30 p.m. | 11:00 a.m. |
| | In a foreign currency | 3:00 p.m. | 11:00 a.m. |
| Note:<br>* One of the conditions for processing of Domestic Funds Transfers-Express is to arrange sufficient available balance on the relevant Customer's account by the end of the Delivery Cut-Off Time period. | | | |

| **Standard Incoming Payment Order Delivery Cut Off Times and Payment Processing Flow** | |
|---|---|
| **Payment product** | **Funds Received by the Bank** |
| Domestic Incoming Payment | On the day on which the funds are received (D) |
| Foreign Incoming Payment<br>– Beneficiary account in IBAN format<br>– Beneficiary account in other format | <br>On the day on which the funds are received (D) 5:00 p.m.*<br>On the day on which the funds are received (D) 3:00 p.m.* |
| SEPA Incoming Payment | On the day on which the funds are received (D) 5:00 p.m.* |
| **Crediting the funds to the Customer's account with the Bank** | **D + 0*** |
| Notes:<br>"D" is the day on which the Bank receives the transferred amount from the payer's provider/correspondent bank.<br>* In case of Foreign Incoming Payments and SEPA Incoming Payments, the transferred amount shall be credited to the Customer's account with the Bank on the day on which the Bank receives the amount as long as the Bank obtains a confirmation no later than 3:00 p.m. or 5:00 p.m. respectively of the same day that the transferred amount was received in the Bank's account (payment cover). If the Bank obtains this confirmation later, the funds shall be credited to the Customer's account on the following business day. | |

| **Standard Cash Payment Order Cut-Off Times** | |
|---|---|
| **Transfer type** | **Delivery of the order to the Bank** |
| Cash Deposit in the Customer's account | During opening hours of the branch (cash desk)* |
| Cash Withdrawal from the Customer's account | During opening hours of the branch (cash desk)* |
| Note:<br>* Information about opening hours of the branches is published on www.citibank.cz | |

The above cut-off times for delivery of a payment order are deemed to be the moment near the end of opening hours of the Bank within the meaning of Section 158(3) of the Payment Systems Act.

## B. Maximum Time Limit for Processing Cross Border Funds Transfers in Currencies Other Than CZK or EUR

A cross border funds transfer in a currency other than CZK or EUR shall always be credited to the account of the payee's provider no later than two business days after the funds have been debited from the Customer's payment account, i.e. the Bank shall credit such cross border funds transfer to the account of the payee's provider in the D+2 regime at the latest.

## C. Manual Payment Orders for Funds Transfers

To enable the capability to submit manual payment Orders for fund transfers, the Customer must complete and provide to the Bank the Global Manual Transaction Authorization (GMTA) form, which supplements the Master Account and Service Terms (MAST), and any other applicable account terms and conditions.

The Customer who does not provide a GMTA form to the Bank understands and agrees that manual Payment Orders for fund transfers submitted by the Customer may be rejected

## D. NSTP Fee

If the Customer initiates a Cross Border Funds Transfer that is directed to a Member State bank via electronic banking, the **Customer is obliged, when entering the Payment Order, to specify the payee's bank BIC and IBAN,** irrespective of the transaction currency. If the Payment Order delivered to the Bank does not include this information, the Customer shall be charged with the "NSTP Fee" ("Non-Straight Through Processing") as per the current List of Charges of Bank. The "NSTP Fee" shall be charged to the Customer within 5 business days after the day the payment order is processed by the Bank. For this fixed charge, the Bank assumes liability for all costs relating to manually processing a Cross Border Funds Transfer delivered via electronic banking, which does not include the data required by Member State banks. These costs include, in particular, the fees charged by the Bank and the payees' banks for an incorrectly structured payment order.

For the Customer to avoid this fee, the Cross Border Funds Transfer delivered via electronic banking must specify the bank details of the beneficiary with the following data:

- BIC* (SWIFT) of the payee's bank selected from the SWIFT library (CitiDirect) or, stated in the first row of the "Payee's Bank" field; this is a stand-alone string of 8 or 11 characters (e.g. CITICZPX).
- IBAN* (the payee's account number in the IBAN format), which is a stand-alone number without spaces and additional characters at the beginning and at the end.

The aforementioned rules apply to all Cross Border Funds Transfers that are initiated via electronic banking and which are remitted to a bank in the Member State, regardless of the currency of the transaction and the SHA/BEN/OUR charges indicator.

**** The Customer should contact its business partners for information about their BIC and IBAN. If the payee's bank is specified by its BIC (SWIFT) code, no other information on the payee's bank needs to be provided. If the BIC code differs from the name of the payee's bank provided by the Customer, the BIC code shall be deemed decisive by the Bank for the purposes of execution of the payment transaction. The***

***same rule applies in general to all types of payment transactions processed by the Bank.***

# IX. AML Information Duty in Relation to Processing of Personal Data

As per the Czech Republic Act No. 253/2008 Coll. on selected measures against legitimization of proceeds of crime and financing of terrorism as amended (the "**AML Act**"), the Bank is required to collect and process personal data of customers, persons acting on behalf of customers, the beneficial owners, members of the statutory body, representatives of the legal person (customer) in this body or in a similar position of statutory body or other people within the business relationship or transaction outside business relationship, in order to prevent abuse of the financial system against legitimization of proceeds of crime and financing of terrorism and to create conditions for the detection of such a conduct.

To meet the Bank's obligations under the AML Act, the Bank generally collects and processes the following personal data:

1. all names and surnames
2. birth identification number (for a person with no birth identification number, a date of birth
3. place of birth
4. gender
5. permanent or other residence and citizenship
6. for a natural person as an entrepreneur it shall also mean the business name, an appendix to the business name, or any other identification features, place of business, and business identification number of the person

If justified by the risk assessment under the AML Act, in addition to personal data above, the Bank may collect and process other identification data for natural persons, such as a telephone number, e-mail address, and data about employment or employer.

Personal data is collected and processed for the business relationship period with the customer and at least 10 years from the end of the year in which such a business relationship was terminated.

The Bank, to perform its duties according the AML Act, may hand over the personal data to third parties. The personal data can be transmitted in this case to the jurisdiction of other countries, which do not have strict data protection laws or do not have personal data protection regulation. A list of the personal data processors the Bank uses to meet its obligations under the AML Act can be found on the website of the Bank (www.citibank.cz).

Providing appropriate personal data is voluntary, but failure to provide it for the purposes of meeting the Bank's obligations under the AML Act will generally mean that the Bank will not be able to provide the services or enter the appropriate deal or be forced to terminate an existing contractual relationship with the Customer.

The data subject has the right to the access to his or her personal data collected by the Bank as specified in § 21 of the Czech Republic Act no. 101/2000 Coll., on protection of personal data, as amended.

# X. Claims about Services, Complaints

Claims about services and Customer complaints shall be settled by the Bank pursuant to the current Bank's Rules for Processing of Complaints for Legal Entities and Entrepreneuring Individuals, which are published on the website of the Bank (www.citibank.cz) and are also available at the registered seat of the Bank's branch in the Czech Republic - Citibank Europe plc, organizační složka and at every branch of the Bank in the Czech Republic.

# XI. Conclusion

Thank you for choosing Citi Treasury and Trade Solutions (TTS) for your cash management needs. Please feel free to contact your Citi relationship manager with any additional questions that you have regarding TTS services.

This User Guide shall become valid and effective on 13 January 2018.

# XII. Definitions

In this User Guide, the following terms have the meaning ascribed to them below:

"**EEA**" means the European Economic Area;

"**EEA Transaction**" means a Payment Transaction which is provided (i) by the payee's provider in a Member State in the case of outgoing payment transactions of the Customer where the Bank acts as the payer's provider; or (ii) by the payer's provider in a Member State in the case of incoming payment transaction of the Customer where the Bank acts as the payee's provider;

"**Member State**" means a member state of the European Union or any other state that is a party to the European Economic Area Treaty;

"**Payment Account**" is an Account for making Payment Transactions;

"**Payment Order**" means a direction to the Payment Service provider whereby the payer or the payee requests that a Payment Transaction be made;

"**Payment Service**" means a payment service as defined by the Payment Systems Act;

"**Payment Transaction**" means depositing money to a Payment Account, withdrawing money from a Payment Account or the transfer of money if such transaction is made within the framework of Payment Service;

"**Payment Systems Act**" means the Czech Republic Act No. 370/2017 Coll., on Payment Systems, as amended;

"**SEPA Area**" means an area comprising the states involved in the EU project "Single Euro Payments Area Project".

# Cash Management User Guide

## Česká republika

Treasury and Trade Solutions

citi

# Obsah

# I. Úvod

Děkujeme, že jste si vybrali Citi Treasury and Trade Solutions (TTS) k řešení Vašich potřeb týkajících se cash managementu. Cílem této uživatelské příručky (dále jen „**Uživatelská příručka**“) je poskytnout Klientům manuál obsahující detailní informace o Službách nabízených Bankou Klientům. Tuto Uživatelskou příručku je třeba číst společně s podmínkami aplikujícími se na Vaše Účty. Tato Uživatelská příručka může být měněna způsobem stanoveným v Místních podmínkách.

Pojmy s velkým počátečním písmenem, které jsou v této Uživatelské příručce použity a které zde nejsou definovány, mají význam určený v Místních státních podmínkách pro vedení Účtů a poskytování Služeb v České republice (*Local Country Conditions for Accounts held and Services provided in the Czech Republic*) (dále jen „**Místní podmínky**“) nebo, pokud takový termín není definovaný v Místních podmínkách, v Hlavních podmínkách pro účty a služby (*Master Account and Service Terms*) (dále jen “**MAST**”).

V této Uživatelské příručce termíny **Banka** a **Citi** znamenají Citibank Europe plc, společnost založenou a existující podle irského práva, se sídlem Dublin, North Wall Quay 1, Irsko, registrovanou v rejstříku společností v Irské republice, pod číslem 132781, provozující svou obchodní činnost v České republice prostřednictvím Citibank Europe plc, organizační složka, se sídlem na adrese Praha 5, Stodůlky, Bucharova 2641/14, PSČ: 158 02, IČ 28198131, zapsané v obchodním rejstříku vedeném Městským soudem v Praze, oddíl A, vložka 59288.

# II. Platební služby – Klient v postavení plátce

## A. Typy platebních služeb v České republice

- Interní platba: Převody finančních prostředků mezi účty Citi v České republice
- Odchozí tuzemská platba: Převody finančních prostředků prostřednictvím systému CERTIS (Czech Express Real Time Interbank Gross Settlement), tj. systémem mezibankovního zúčtování České Národní Banky, který provozuje veškeré převody bez ohledu na jejich hodnotu, zpracované buď ve standardním režimu (ACH), nebo v rámci režimu expresního zpracování.
- Jednotná oblast pro platby v eurech (SEPA): Mechanismus zúčtování měny EUR pro platby s nízkou hodnotou a vysokým objemem, zahrnující jak službu přímého inkasa, tak i službu převodu peněžních prostředků pro jednotlivé a hromadné převody a převody v režimu expresního zpracování nebo kombinaci těchto převodů.
- Přímá inkasa: Prostředek pro zinkasování dlužné částky od plátce, kdy příjemce v roli iniciátora převodu vytváří podnět k transakci zpracované bankou plátce z účtu plátce. Přímé inkaso, které vždy podléhá autorizaci ze strany plátce, se obvykle používá pro pravidelné platby, jako jsou vyúčtování za kreditní karty a za služby, kde se částky těchto pravidelných plateb liší.
- Zahraniční odchozí platba: Umožňuje Klientům provádět mezinárodní převody v celé řadě měn formou bezhotovostních převodů, včetně mezinárodních plateb v české měně.

## B. Odeslání platby

1. Klient pošle Citi Platební příkaz, formátovaný dle tržních standardů a způsobem dohodnutým v době implementace platební služby, a to prostřednictvím:
    - kanálů elektronického bankovnictví Citi, kam patří CitiDirect BE® a CitiConnect®,
    - rozhraní SWIFT , nebo
    - manuální žádosti (zde platí omezení)
2. Citi odešle příkaz do příslušného platebního systému k dalšímu zpracování.
3. Platební systém doručí příkaz bance příjemce prostřednictvím místně definovaného zúčtovacího systému.
4. Banka příjemce připíše platbu na účet příjemce.

## C. Přijetí žádosti o inkaso z účtu plátce

Citi, v postavení banky plátce Klienta, přijímá zmocnění k inkasu a inkasní příkazy obdržené od ostatních členských finančních institucí.

1. Citi ověřuje přijatý příkaz oproti zmocnění k inkasu (nebo jeho ekvivalentu), které Klient poskytl Citi před provedením platby.

2. Je-li ipříkaz k inkasuv souladu se zmocněním k inkasu, Citi příkaz zpracuje a odepíše platbu z účtu Klienta.

3. V případě, že na účtu Klienta neexistuje zmocnění k inkasu nebo na něm není dostatek finančních prostředků, Citi platbu inkasem nezpracuje a vrátí ji s příslušným statusem zpět do inkasního zúčtovacího systému nebo členským bankám.

Jakoukoli chybně zprocesovanou položku Citi napraví odepsáním či připsáním částky na příslušný Účet.

## D. Platba šekem

Citi Česká republika může vydávat šeky WorldLink® v jakékoli podporované zahraniční měně. Šeky WorldLink® mohou být proplaceny na Citi účet u místní pobočky Citi nebo prostřednictvím účtu Citi u externí banky. Šek WorldLink® je zúčtován jako domácí šek v té zemi, kde je vystaven. Například šek WorldLink® v SGD je proplacen společností Citi Singapur a je zpracován jako domácí šek, pokud je předložen k inkasu v Singapuru. Pokud je tento šek WorldLink® v SGD předložen k inkasu mimo Singapur, banka příjemce jej zúčtuje formou zahraničního příkazu.

Doba platnosti proplatitelného šeku je stanovena příslušnými předpisy a bankovními zvyklostmi od data uvedeného na šeku při jeho vystavení. Poslední den tohoto období je dále označován jako „datum vypršení platnosti“. S výhradou platných místních zákonů a bankovních zvyklostí platí, že pokud takový proplatitelný šek není předložen k proplacení do data vypršení platnosti (včetně), Banka šek neproplatí.

Vzhledem k tomu, že v České republice neexistuje mechanismus zúčtování šeků v Kč, Citi nevydává šeky v Kč.

### 1. Vydávání a zpracování šeků WorldLink®

1. Klient předává příkazy prostřednictvím sjednaného kanálu elektronického bankovnictví Citi.

2. Citi odepíše částku z účtu Klienta a vytiskne šek(y).

3. Citi zašle šek(y) na adresu příjemce uvedenou v příkazu Klienta nebo na adresu Klienta vedenou u Citi.

4. Příjemce předloží šek(y) k inkasu a ty jsou předány zpět Citi prostřednictvím místních zúčtovacích zvyklostí.

5. Šeky jsou ověřeny a finanční prostředky následně zpřístupněny.

6. Klient bude informován o všech problémech s šeky, které byly předloženy.

7. Citi neprovede platbu, pokud považuje šek za podstatně pozměněný, padělaný nebo odcizený, nebo na žádost příslušného soudního, kvazisoudního, regulačního, státního či dozorčího orgánu.

   Pokud šek WorldLink® není předložen k platbě do data vypršení platnosti (včetně), Banka jej neproplatí a v souladu s platnými zákony a bankovními zvyklostmi buď na žádost Klienta nebo dle uvážení Banky, v přiměřené lhůtě po datu vypršení platnosti, připíše na účet částku tohoto splatného šeku nebo jinak vrátí částku Klientovi.

### 2. Žádost o storno proplacení šeku

Klient může požadovat, aby Banka v případě ztracených nebo zrušených šeků v souladu s postupy Banky a příslušnými místními zákony stornovala proplacení takového proplatitelného šeku. Citi doporučuje použít standardní formulář Citi pro storno platby, který lze získat prostřednictvím zákaznického oddělení Citi (Citi Service Desk).

1. Klient předá Citi žádost o storno platby. Žádost musí obsahovat sériové číslo šeku, datum vystavení, jméno příjemce a částku. Storno proplacení šeku bude provedeno na základě informací uvedených v těchto příkazech.

2. V případě šeků WorldLink®, které mají být stornovány a nebyly doposud proplaceny, Banka vrátí hodnotu každého šeku za všechny žádosti o storno platby šeku na účet, z něhož byly platby odeslány, s výjimkou případů, kdy Klient požaduje vystavení náhradního šeku.

3. Pokud je ztracený nebo odcizený šek později nalezen, Klient je povinen tento původní šek okamžitě doručit Bance.

Banka může dle svého uvážení rozhodnout, zda přijme příkaz Klienta ke zrušení nebo stornu proplacení šeku.

## E. Služba doručení hotovosti

Citi nabízí doručování hotovosti na adresu v České republice prostřednictvím poskytovatele služeb přijatelného pro Banku a Klienta, s nímž Klient uzavřel příslušnou smlouvu o poskytování takové služby. Klient může tuto službu využít na základě žádosti o službu přípravy a předání hotovosti, která musí být vyplněna a podepsána jménem Klienta a doručena Bance („**Žádost o hotovost**“). Smlouva mezi Bankou a Klientem o poskytování služby doručování hotovosti je uzavřena doručením vyplněné Žádosti o hotovost Bance („**Smlouva o doručování hotovosti**“) za podmínky, že Klient také uzavřel smlouvu o poskytování příslušných služeb s poskytovatelem služeb přijatelným pro Banku.

### Proces doručování hotovosti

1. Klient podá prostřednictvím osoby oprávněné za něj jednat a prostřednictvím elektronického bankovního systému CitiDirect BE® žádost o výběr a přípravu hotovosti k předání poskytovateli služeb, který zajišťuje doručení hotovosti na zvolené místo v předem dohodnutý čas. Žádost musí obsahovat následující údaje:

   - Částku, včetně měny a skladby požadovaných bankovek
   - Účet Klienta, z něhož má být částka odepsána
   - Název poskytovatele služeb, který vyzvedne hotovost v prostorech Citi
   - Datum požadovaného vyzvednutí hotovosti k doručení
   - Oprávněnou osobu (jméno a funkce pracovníka)

   Uvedená žádost (dále jen „Žádost“) musí být doručena do Banky nejpozději dva pracovní dny (do 9:30) před plánovaným dnem doručení hotovosti.

2. Na základě Žádosti Banka řádně a včas připraví k přepravě požadovanou částku hotovosti v požadované měně.

3. Vybraný poskytovatel služeb doručí hotovost (za podmínek stanovených ve vzájemné smlouvě mezi Klientem a poskytovatelem služeb) oprávněné osobě Klienta na určenou adresu (podle dohody mezi Klientem a poskytovatelem služeb). Banka vydá k převozu hotovost požadovanou Klientem jen oprávněným pracovníkům příslušného poskytovatele služeb, a to v souladu s podmínkami stanovenými v Žádosti.

4. Oprávněná osoba před potvrzením doručení hotovosti obdrží a ověřuje následující:

   - Výši doručené hotovosti
   - To, že nebyly doručeny žádné znečištěné bankovky
   - Doklad totožnosti obsahující fotografii poskytovatele služeb

5. Oprávněná osoba Klienta musí předložit svůj doklad totožnosti obsahující fotografii zástupci poskytovatele služeb pro ověření, v souladu se vzájemnou smlouvou.

6. Možnost a doba doručení závisí na místě doručení a výši hotovosti, která má být doručena.

7. Klient zajistí, aby částka hotovosti, kterou chce Klient vybrat z účtu, nebyla vyšší než zůstatek na účtu, který je k dispozici na účtu v období od druhého pracovního dne před požadovaným datem doručení hotovosti do odepsání částky z účtu Klienta. Žádosti bude vyhověno pouze v případě, že Klient zajistí, aby částka hotovosti, kterou chce Klient vybrat z účtu, nebyla vyšší než zůstatek na účtu.

8. Částka hotovosti bude odepsána z účtu Klienta u Banky jeden pracovní den před požadovaným dnem doručení hotovosti.

9. Klient nebo Banka mohou ukončit Smlouvu o doručování hotovosti za podmínek stanovených pro ukončení služby v Hlavních podmínkách pro účty a služby (*Master Account and Service Terms*).

# III. Platební služby – Klient v postavení příjemce

## A. Typy platebních služeb v České republice

- Příchozí tuzemská platba: Příchozí platby na platební účet Klienta v českých korunách přijaté prostřednictvím zúčtovacího centra České národní banky od ostatních poskytovatelů na českém trhu (tj. poskytovatele plátce nebo zprostředkujícího poskytovatele).

- Příchozí platba SEPA: Příchozí platby v měně EUR od poskytovatelů platebních služeb v rámci SEPA prostoru, které byly odeslány poskytovatelem plátce prostřednictvím kanálu SEPA.

- Zahraniční příchozí platba: Příchozí platby v cizí měně od poskytovatelů v rámci České republiky a mezinárodní příchozí platby v cizí měně.

Jakékoli odmítnuté nebo vrácené platby ze strany Citi budou připsány zpět na účet plátce nebo vráceny bance plátce. Důvod vrácení se sděluje bance plátce.

## B. Platby z podnětu příjemce

Přímé inkaso je finanční transakce elektronicky iniciovaná Klientem, instruující Banku k výběru prostředků z bankovního účtu plátce.

Platby prostřednictvím Prímého inkasa v českých korunách jsou uskutečňovány z podnětu příjemce platby. Majitel debetovaného platebního účtu musí svému poskytovateli platebních služeb doručit souhlas s inkasem, v němž identifikuje číslo účtu příjemce a v němž zároveň tohoto poskytovatele zmocňuje k takovému převodu prostředků. Tento souhlas musí být doručen před inkasním cyklem.

### Proces platby z podnětu příjemce

1. Klient zajistí, aby plátce udělil souhlas s inkasem před tím, než Klient doručí žádost o Přímé inkaso Bance.

2. Klient iniciuje žádost o Přímé inkaso a předává Bance soubor hromadných příkazů prostřednictvím dohodnutého kanálu elektronického bankovnictví Banky.

3. Banka ověří, že žádosti o Přímé inkaso obsahují informace potřebné k jejich zpracování.

4. Banka doručí žádosti o Přímé inkaso bankám plátců prostřednictvím zúčtovacího systému.

5. Citi připíše prostředky na účet Klienta ve stejný den, kdy Banka obdrží finanční prostředky ze zúčtovacího systému.

Klient by neměl iniciovat žádné další žádosti o Přímé inkaso, pokud je žádost vrácena z některého z následujících důvodů:

- Účet byl zrušen nebo převeden

- Žádný takový účet neexistuje

- Neodpovídající název účtu
- Nedostatečné prostředky na účtu (po tři předcházející cykly)
- Povolení k inkasu bylo plátcem zrušeno

## C. Předložení šeku k inkasu

Klient může na pobočce Banky předložit šeky k inkasu následujícím způsobem:

- Prostřednictvím přepážky Banky; nebo
- Prostřednictvím pošty

Při předkládání šeků k inkasu musí Klient vyplnit vkladový doklad, v němž uvede podrobnosti o účtu u Banky, kam mají být připsány prostředky z vkladu šeku. Vkladové doklady jsou k dispozici na pobočce Banky.

Všechny Bance předložené šeky k inkasu doručené v pracovní den (pondělí až pátek) v rámci lhůty pro doručení, jsou odeslány k inkasu ve stejný den. Šek předložený ve státní svátek nebo o víkendu bude odeslán příští pracovní den.

Citi připíše na účet Klienta celkovou částku šeků k inkasu druhý pracovní den poté, co Banka obdrží finanční prostředky. Jsou-li připsané finanční prostředky zúčtovacím systémem nebo bankou plátce odvolány, Citi odepíše původně připsanou částku takového odvolaného šeku z Účtu Klienta.

## D. Vklad na pobočce

Banka nabízí služby přímo na pobočce Banky, kde může Klient vkládat šeky a hotovost.

## E. Služba svozu hotovosti

Citi nabízí svoz hotovosti přímo z provozovny Klienta prostřednictvím specializovaného poskytovatele služeb. Mezi tyto služby patří:

- Svoz hotovosti: Vyzvednutí fyzických bankovek a mincí z provozovny Klienta v předem dohodnutém termínu k převozu do určených svozových/zpracovatelských center.
- Zpracování hotovosti: Počítání a zpracování (třídění a balení) svezené hotovosti v určených centrech zpracování hotovosti a připsání na účet Klienta.

### Proces služby svozu hotovosti

1. Klient musí uzavřít smlouvu přímo s poskytovatelem služeb podle svého výběru, který je pro Banku přijatelný, a dále se dohodnout na:
    - Adrese, kde bude hotovost vyzvednuta
    - Přibližné částce hotovosti, která má být vyzvednuta
    - Účtu Klienta, na který má být částka připsána
2. Vybraný poskytovatel služeb vyzvedne hotovost z určeného místa Klienta v den dohodnutý ve vzájemné smlouvě. Klient hotovost přepočítá, umístí do uzavíratelného plastového sáčku odolného proti manipulaci a vyplní vkladový doklad poskytnutý poskytovatelem služby.

3. Zástupci poskytovatele služeb vyzvednou hotovost.
4. Vyzvednutá hotovost je převezena do určeného centra (center) pro zpracování hotovosti.
5. Hotovost je zkontrolována, zda bankovky nejsou vadné, padělané nebo nepřijatelné, a přepočítána. Pravost a stav bankovek a mincí ověří poskytovatel služby a na účet Klienta je připsána příslušná částka.
6. Padělané bankovky nebo mince budou řešeny v souladu s příslušnými předpisy; veškeré související náklady nebo následky jdou k tíži Klienta.

# IV. Další ustanovení

1. Odmítnutí provést Platební příkaz nebo jiný pokyn

   a. Banka může odmítnout provést platební příkaz:

      i. pokud není Platební příkaz Bance předán ve formě, lhůtách a způsobem stanovenými Bankou nebo dohodnutými mezi Klientem a Bankou nebo neobsahuje údaje stanovené Bankou nebo dohodnuté mezi Klientem a Bankou;

      ii. pokud není podán osobou oprávněnou k podání takového Platebního příkazu nebo není podepsán v souladu s podpisovými vzory uloženými u Banky;

      iii. existují pochybnosti o obsahu, vzniku či o oprávnění osob tento Platební příkaz za Klienta podat;

      iv. Platební příkaz vybočuje z obvyklého způsobu při zadávání pokynů či provádění platebního styku s Klientem

      v. pokud má Klient vůči Bance dluh po splatnosti;

      vi. z důvodů, pro které je Banka oprávněna zablokovat platební prostředek;

      vii. pokud na účtu Klienta není dostatek použitelných peněžních prostředků;

      viii. pokud, v případě Platebního příkazu z podnětu příjemce, není Bance předán souhlas Klienta s touto transakcí;

      ix. byl doručen bez použití dohodnutých prostředků komunikace;

      x. pokud nejsou splněny další podmínky pro provedení Platebního příkazu, popřípadě jsou splněny podmínky pro odmítnutí provedení Platebního příkazu, stanovené v této Uživatelské příručce nebo v jiné dohodě nebo dokumentu platícím mezi Bankou a Klientem; nebo

      xi. pokud tak stanoví obecně závazný právní předpis.

   b. Bez ohledu na výše uvedená ustanovení tohoto článku platí, že pokud nastane nějaký důvod umožňující Bance odmítnout provedení Platebního příkazu, je Banka oprávněna takový Platební příkaz neodmítnout a:

      i. pokud ke splnění příslušných podmínek dojde nejpozději do pěti pracovních dnů poté, co Banka obdrží Platební příkaz, provést takový Platební příkaz až po splnění těchto podmínek; nebo

      ii. pokud ke splnění příslušných podmínek do pěti pracovních dnů po obdržení Platebního příkazu Bankou nedojde, provedení takového Platebního příkazu následně odmítnout.

      Výše uvedenými ustanoveními však není omezeno právo Banky provedení takového Platebního příkazu odmítnout kdykoli (tedy i během výše uvedené lhůty pěti pracovních dnů).

c. Odmítne-li Banka provést Platební příkaz, bude Klienta informovat telefonicky prostřednictvím zákaznického centra Banky nebo jinými způsoby komunikace dohodnutými mezi Bankou a Klientem.

d. Za informace o odmítnutí provedení Platebního příkazu může Banka Klientovi účtovat úplatu dle aktuálního Sazebníku.

e. Kterýkoli jiný Klientův pokyn než Platební příkaz může Banka odmítnout provést ze stejných důvodů, pro něž je Banka oprávněna odmítnout provést Platební příkaz podle odstavců i. až iv. článku 1.a. výše.

2. Blokace platebního prostředku

a. Banka má právo kdykoliv a bez jakýchkoliv následků zablokovat platební prostředek z důvodu (i) bezpečnosti platebního prostředku, zejména při podezření na neautorizované nebo podvodné použití platebního prostředku; nebo (ii) významného zvýšení rizika, že Klient (nebo držitel platebního prostředku) nebude schopen splácet úvěr, který lze čerpat prostřednictvím tohoto platebního prostředku.

b. Důvody, pro které může Banka zablokovat platební prostředek uvedené v podmínkách jednotlivých platebních prostředků a dalších dokumentech týkajících se těchto platebních prostředků, nijak nevylučují možnosti Banky platební prostředek zablokovat podle odstavce a. tohoto článku.

3. Vrácení částky autorizované Platební transakce

a. Klient (plátce) je oprávněn požadovat vrácení částky autorizované Platební transakce pouze, pokud taková Platební transakce byla iniciována příjemcem v rámci SEPA Direct Debit Scheme ("*Systém SEPA pro Inkasa*").

b. Klient souhlasí s tím, že v případě vrácení částky autorizované transakce provedené z podnětu příjemce, kde je Klient v postavení příjemce platby a Banka v postavení poskytovatele příjemce platby, je Banka oprávněna odepsat z kteréhokoliv jeho účtu prostředky za účelem vrácení částky autorizované transakce provedené z podnětu příjemce, kterou plátce požaduje vrátit v souladu s příslušnými obecně závaznými právními předpisy.

4. Podmínky přímých inkas SEPA

a. Přímá inkasa SEPA jsou činěna buď v rámci tzv. SEPA Direct Debit Core Scheme nebo tzv. SEPA Direct Debit B2B Scheme.

b. Pokud příslušné právní předpisy týkající se SEPA inkas nestanoví jinak, jsou všechny platební účty Klienta otevřené vůči SEPA inkasům činěným v rámci SEPA Direct Debit Core Scheme, tzn. že Banka provede všechny příkazy k SEPA inkasu z Klientových platebních účtů, které byly podány v rámci SEPA Direct Debit Core Scheme. Na pokyn Klienta Banka zablokuje veškerá taková inkasa z platebního účtu Klienta nebo inkasa z podnětu jednoho nebo více určených příjemců nebo povolí taková inkasa pouze z podnětu jednoho nebo více určených příjemců.

c. Klient má právo dát Bance pokyn, aby před odepsáním částky z platebního účtu Klienta ověřila každou inkasní transakci podanou v rámci SEPA Direct Debit B2B Scheme a zkontrolovala, zda částka a periodicita zadané inkasní transakce odpovídá částce a

periodicitě stanovené ve zmocnění k inkasu, a to na základě informací týkajících se zmocnění k inkasu.

d. Jak v případě inkas činěných v rámci SEPA Direct Debit Core Scheme, tak v případě inkas činěných v rámci SEPA Direct Debit B2B Scheme má Klient právo dát Bance pokyn, aby Banka omezila inkaso na určitou částku nebo periodicitu, případně obojí.

e. Každý Klientův pokyn vyžadující manuální nastavení na straně Banky musí být Bance doručen nejpozději do do 11. hod. druhého pracovního dne před začátkem inkasního cyklu.

# V. Výpisy z účtu

1. Banka poskytuje Klientovi výpisy z Účtu, pouze pokud se na tom s Klientem písemně dohodne. Pokud však v předchozím období, za které má být dle dohody mezi Bankou a Klientem výpis z Účtu poskytnut, nebyly provedeny žádné platební transakce, výpis z Účtu za takové období se nevytváří a nebude za toto období Klientovi poskytnut.

2. Výpisy z Účtu mohou být Bankou zasílány pouze v anglickém nebo českém jazyce, mohou být s detaily transakcí nebo bez těchto detailů a mohou být Bankou zasílány pouze s denním, týdenním nebo měsíčním intervalem nebo mohou být zasílány na základě pohybu na Účtu. Pokud se Klient písemně nedohodne s Bankou jinak, veškeré výpisy z Účtu zasílané Bankou Klientovi budou v anglickém jazyce, budou s detaily transakcí a budou zasílány na základě pohybu na Účtu.

3. Pokud se Banka s Klientem písemně dohodne na zasílání výpisů z Účtu, pak, není-li dohodnuto jinak, Banka poskytuje Klientovi zdarma výpis elektronickou poštou (e-mailem), což je považováno za standardní způsob poskytování výpisu ze strany Banky. V případě, že se Banka a Klient písemně dohodnou na zasílání výpisu z Účtu v tištěné formě, bude Klientovi takový tištěný výpis Bankou odesílán na korespondenční adresu Klienta a může být zpoplatněn dle aktuálního Sazebníku.

4. Pro poskytování výpisu z Účtu jeho zasláním elektronickou poštou (e-mailem) dále platí následující ustanovení:

    a. Banka začne zasílat výpisy z Účtu Klientovi až poté, co Klient písemně Bance sdělí kontaktní údaje (tj. jméno, e-mailovou adresu a telefon) osob, jímž mají být výpisy z Účtu zasílány a e-mailové adresy těchto osob byly aktivovány Bankou prostřednictvím jejího oddělení CitiService v souladu s vnitřními předpisy Banky. Výpisy z Účtu budou Bankou zasílány v souborech chráněných heslem. Toto heslo bude nastaveno, a případně v budoucnosti měněno, v souladu s vnitřními předpisy Banky prostřednictvím jejího oddělení CitiService.

    b. Klient je oprávněn změnit kontaktní údaje osob, kterým mají být zasílány výpisy z Účtu, prostřednictvím doručení písemného oznámení Bance. Každá taková změna se stane účinnou na základě jejího zpracování Bankou prostřednictvím jejího oddělení CitiService v souladu s vnitřními předpisy Banky.

# VI. Další faktory

Klient provede své vlastní vyhodnocení právních, regulačních, daňových a účetních důsledků služeb.

Příležitostně Banka doručí Klientovi sazebníky, postupy, požadavky, příručky, manuály a další materiály, které popisují postupy, požadavky a omezení týkající se využívání služeb.

Zúčtování plateb se řídí pravidly stanovenými příslušným zúčtovacím systémem. Citi i její klienti se těmito pravidly musí řídit.

# VII. Konsolidované bezpečnostní postupy TTS

Jak je již uvedeno v části Komunikace Hlavních podmínek pro účty a služby (*Master Account and Service Terms*) (nebo jiných platných podmínek účtu) (dále jen „**MAST**“), které byly uzavřeny mezi Klientem a Bankou, níže jsou popsány bezpečnostní postupy (dále jen „**Postupy**“) používané Citi Treasury and Trade Solutions v souvislosti s následujícími službami nebo komuničními kanály.

- CitiDirect BE® (včetně vedení elektronických bankovních účtů (dále jen „**eBAM**“)), TreasuryVision®, a WordLink®)
- Interaktivní hlasový informační systém (dále jen „**IVR**“)
- E-mail/fax s Bankou s výjimkou manuálně iniciovaného převodu peněžních prostředků (MIFT)
- CitiConnect
- Jiné místní elektronické komunikační kanály

Dostupnost služeb nebo komunikačních kanálů se bude na místních trzích lišit. Tyto Postupy mohou být aktualizovány a sdělovány Klientovi elektronickými prostředky nebo jinak. Bude-li Klient pokračovat ve využívání kterékoli z výše uvedených služeb nebo komunikačních kanálů poté, co byl informován o aktualizovaných Postupech (což může zahrnovat mimo jiné zveřejňování aktualizovaných Postupů na CitiDirect BE® v souvislosti se službou nebo komunikačním kanálem), znamená to, že Klient tyto aktualizované Postupy přijímá. Tyto Postupy je třeba číst společně s MAST v platném znění. Výrazy s velkými počátečními písmeny, které v tomto dokumentu nejsou jinak definovány, mají význam, který jim byl určen v MAST.

## A. Role a úkoly bezpečnostního manažera*

Pro nastavení oprávnění v rámci CitiDirect BE® Banka požaduje dvě samostatné osoby pro zadávání a schvalování příkazů; vyžadují se tedy minimálně dva bezpečnostní manažeři. Libovolní dva bezpečnostní manažeři jednající ve shodě mohou přiřazovat a schvalovat oprávnění prostřednictvím komunikačních kanálů v souvislosti s výkonem funkce bezpečnostního manažeranebo v souvislosti s usnadněním komunikace přes internet. Takové Komunikace, schválené dvěma bezpečnostními manažery, budou přijaté a Banka na jejich základě bude jednat. Banka doporučuje zvolit nejméně tři bezpečnostní manažery, aby byla zajištěna odpovídající zastupitelnost. Klient určí svého bezpečnostního manažera prostřednictvím formuláře TTS Aktivační formulář pro elektronické bankovnictví . Bezpečnostní manažer Klienta může také vykonávat funkci bezpečnostního manažera pro třetí stranu (například přidruženou společnost Klienta) a vykonávat všechna práva, která s tím souvisejí (včetně jmenování uživatelů pro účty takové třetí strany), bez dalšího určení, jestliže tato třetí strana vystavítzv. Universal Access Authority form (formulář univerzálního oprávnění k přístupu) (nebo jinou formu zmocnění přijatelnou pro Banku), který poskytuje přístup jiné osobě k jeho účtům. To platí pouze pro účty, na které se vztahuje příslušné oprávnění.

*Role a povinnosti bezpečnostního manažera mohou být na některých místních trzích zakázány. Pro více informací se obraťte na svého zástupce klientského servisu.

Funkce bezpečnostního manažera zahrnuje mimo jiné:

1. Vytváření a spravování přístupu a oprávnění uživatelů (včetně samotných bezpečnostních manažerů), včetně činností, jako jsou:

a. vytváření, odstraňování nebo změna uživatelských profilů(včetně profilů bezpečnostních manažerů ) a oprávnění (vezměte prosím na vědomí, že uživatelské jméno musí být v souladu s identifikačními dokumenty)

b. vytváření přístupových profilů, které definují funkce a data dostupné různým uživatelům; a

c. aktivace a deaktivace uživatelských přihlašovacích údajů.

2. Vytváření a úpravy záznamů v knihovnách spravovaných Klientem (jako jsou předdefinované platby a knihovny příjemců) a udělování práv ostatním uživatelům, aby mohli vykonávat stejnou činnost

3. Změna úrovní autorizace plateb.

4. Přidělování dynamických hesel nebo jiných zabezpečovacích údajů či hesel pro přístup do systému uživatelům Klienta

5. Oznámení Bance, pokud existuje důvod k podezření, že došlo k ohrožení bezpečnosti.

Bezpečnostní manažeři rovněž přiřazují uživatelům limity transakcí pro ty bankovní produkty, ke kterým má Klient přístup. Tyto limity Banka nesleduje ani neověřuje; Klient by měl ověřovat tyto limity, aby zajistil dodržování interních zásad a požadavků Klienta, mimo jiné těch, které stanoví představenstvo Klienta, nebo jeho jiný rovnocenný orgán.

Zvláště v souvislosti s **aplikací eBAM** jsou vyžadovány následující role:

Počáteční nastavení služby eBAM vyžaduje určení tří bezpečnostních pracovníků a jednoho pracovníka vnitřní kontroly. Dvě oddělené hlavní administrativní role jednají ve shodě jako zadavatel/autorizátor, za účelem nastavení a přidělení uživatelských funkcí/oprávnění a pracovních postupů. Tato uspořádání Banka nesleduje ani neověřuje. Pracovní postupy a uživatelská aktivita jsou sledovány Klientem pro zajištění dodržování interních zásad, požadavků a úrovní autorizace a schválení Klienta (a majitelů účtů), mimo jiné včetně těch stanovených představenstvem Klienta (a majitelů účtů) nebo rovnocenným řídícím orgánem.

Pro službu eBAM jsou požadovány následující role:

1. **Bezpečnostní pracovník:** Plnění funkcí popsaných výše v bodě 1. a-c v rámci rolí bezpečnostních manažerů;

2. **Pracovník vnitřní kontroly:** Zajišťuje, že pracovní postupy, nastavení uživatelů jako určených osob provádějících autorizaci a jejich přiřazení k pracovním postupům splňují interní zásady, požadavky a úrovně autorizace a schválení, které jsou stanoveny představenstvem Klienta (a majitelů účtů) nebo rovnocenným řídícím orgánem

3. **Určené osoby provádějící autorizaci:** Mají rozsáhlou, vyšší pravomoc iniciovat a schvalovat činnosti v rámci pracovního postupu; a

4. **Iniciátoři žádostí:** jsou osoby oprávněné provádět administrativní činnosti, jako je zadávání požadavků na vedení účtů a podepisujících subjektů do systému eBAM.

Bezpečnostní pracovníci, pracovníci vnitřní kontroly a určené osoby provádějící autorizaci odpovídají za:

1. definování a správu nastavení oprávnění a úrovní kontroly, jako je vytvoření pracovních postupů a určení uživatelů a úrovně schválení;

2. vytváření dalších seniorských administrativních rolí a jmenování uživatelů (kteří mohou nebo nemusí být zaměstnáni Klientem)

3. oznámení Bance, pokud existují důvody k podezření, že byla porušena nebo ohrožena bezpečnost či důvěrnost zabezpečovacích údajů uživatelů (včetně seniorských administrativních rolí); a

4. je-li to relevantní, vyplnění, změnu, schvalování a/nebo doplnění takových formulářů Klienta, které mohou být v přiměřeném rozsahu požadovány Bankou v souvislosti s poskytováním služeb a/nebo produktů Klientovi

## B. Metody ověření

Postupy zahrnují určité zabezpečené metody ověření (dále jen „Metody ověření“), které slouží k jednoznačné identifikaci a ověření oprávnění Klienta a/nebo jakéhokoli jeho uživatele, obvykle prostřednictvím mechanismů, jako jsou kombinace uživatelské jméno/heslo, digitální certifikáty a bezpečnostní prvky (používané prostřednictvím hardwaru nebo softwaru), které generují dynamické heslo pro přístup ke službám nebo komunikačním kanálům vždy, když se Klient nebo uživatel přihlásí nebo ověří. Upozorňujeme, že dostupnost níže popsaných Metod ověření se liší podle místních trhů.

Bezpečnostní manažeři a všichni uživatelé, kteří chtějí (a) iniciovat nebo schválit transakce (a jejichž uživatelský profil jim to umožňuje) a/nebo (b) přistupovat k systémům v souladu s oprávněními, musí používat dostupné Metody ověření (které mohou být čas od času aktualizovány, jak je popsáno výše).

Pro přístup k výše uvedeným službám nebo komunikačním kanálům v kombinaci s uživatelským jménem jsou k dispozici následující Metody ověření:

| **Metoda ověření** | **Popis** |
|---|---|
| Token: Odpověď na výzvu | Buď (i) softwarový token založený na mobilních aplikacích (např. MobilePASS) nebo (ii) fyzický token (např. SafeWord karta, Vasco), který se v každém případě použije k vygenerování dynamického hesla po ověření pomocí čtyřmístného pinu. Při přístupu ke službě CitiDirect BE systém vygeneruje výzvu a použitý token následně vygeneruje přístupový kód, který je zadán do systému. |
| Token: Jednorázové heslo | Buď (i) softwarový token založený na mobilních aplikacích (např. MobilePASS) nebo (ii) fyzický token (např. SafeWord karta, Vasco), který se použije k vygenerování dynamického hesla po ověření pomocí čtyřmístného pinu. Toto dynamické heslo je zadáno do systému pro získání přístupu. |
| Jednorázový kód SMS | Dynamické heslo je uživateli doručeno prostřednictvím SMS, a uživatel zadá dynamické heslo a heslo zabezpečení pro přístup do systému |
| Jednorázový hlasový kód | Dynamické heslo je uživateli doručeno prostřednictvím automatizovaného hlasového volání, a uživatel zadá pro přístup do systému dynamické heslo a heslo zabezpečení |
| Ověření MultiFactor | Dynamické heslo je generováno pomocí SafeWord karty nebo tokenu MobilePASS, a takové dynamické heslo je pro přístup do systému zadáno spolu s osobním heslem . |
| Digitální certifikáty | Digitální certifikát vydaný schválenou certifikační autoritou, který se používá k ověření. Digitální certifikáty využívají mechanismus ukládání klíčů a příslušný kód PIN a mohou být vydávány společností IdenTrust, SWIFT (3SKey) nebo jinými dohodnutými poskytovateli. |

| | |
|---|---|
| Bezpečné heslo | Uživatel zadá své heslo pro přístup do systému. Bezpečné heslo obvykle omezuje možnosti uživatele v systému, například že lze zobrazovat informace, ale nejsou aktivovány žádné funkce pro transakce. |
| Interaktivní hlasový informační systém (IVR) a e-mail | Uživatelé kontaktující banku budou vyzváni k zadání čísla PIN nebo k poskytnutí dalších informací k ověření autorizovaného přístupu prostřednictvím telefonu nebo přes e-mail. |
| Fax | Korespondence přijatá Bankou, s výjimkou žádostí MIFT, bude ověřena podpisem na základě informací, které jsou obsaženy v usnesení představenstva, nebo jiného řídícího orgánu Klienta. |
| MTLS | Mandatory Transport Layer Security (MTLS) vytváří zabezpečené soukromé e-mailové spojení mezi Citi a externím účastníkem. E-mail odeslaný pomocí tohoto kanálu je odeslán přes internet prostřednictvím šifrovaného tunelu TLS vytvořeného tímto spojením. |
| Zabezpečené PDF | Šifrované e-maily jsou doručovány do běžné e-mailové schránky jako dokument PDF, který je otevřen zadáním osobního hesla; text zprávy i všechny přiložené soubory jsou zašifrovány. Po obdržení prvního přijatého zabezpečeného e-mailu lze nastavit osobní heslo. |

Více informací o těchto Metodách ověření viz stránka nápovědy ohledně přihlašování v rámci CitiDirect BE (https://portal.citidirect.com/portalservices/forms/loginHelp.pser)

### Pro CitiConnect®

- Pokud se Klient rozhodne pro připojení k síti Citi prostřednictvím veřejného internetového připojení, včetně HTTPS, zabezpečeného FTP a FTPs, Banka a Klient si vymění bezpečnostní certifikáty s cílem zajistit, že jak komunikační kanál, tak vyměněné zprávy jsou plně šifrovány a chráněny. Banka bude akceptovat pouze Komunikace pocházející od Klienta zabezpečené pomocí bezpečnostních certifikátů a naopak, a Banka bude předávat Klientovi pouze Komunikace zabezpečené pomocí bezpečnostních certifikátů.

- Pokud se Klient rozhodne používat CitiConnect přes SWIFT, pak u jakýchkoli platebních příkazů a pokynů týkajících se SWIFT, včetně změn nebo rušení takových příkazů, se budou Postupy použité k ověření, že platební příkaz nebo pokyn je příkazem Klienta a schválený Klientem, řídit smluvní dokumentací SWIFT (jak definují podmínky SWIFT v platném znění), která zahrnuje mimo jiné Všeobecné obchodní podmínky a popis služby FIN, nebo jak je uvedeno v jakýchkoli jiných podmínkách, které může společnost provozující SWIFT stanovit. Banka neodpovídá za žádné chyby nebo zpoždění v systému SWIFT. Komunikace do Banky musí být poskytovány ve formátu a typu požadovaném a specifikovaném SWIFT.

- Pokud se používá VPN, Klient a Banka určí jednu IP adresu, ze které budou Komunikace mezi Klientem a Bankou odesílány a/nebo přijímány. Banka bude akceptovat pouze Komunikace pocházející z Klientovy určené IP adresy a naopak, a Banka bude předávat Klientovi pouze Komunikace na Klientovu určenou IP adresu a naopak.

- Klient a Banka mohou rovněž používat ověření pomocí hardwarového modulu zabezpečení kromě ověření VPN. To vyžaduje, aby Banka a Klient instalovali zařízení na serverech určených pro Komunikace mezi Bankou a Klientem.

Banka požaduje:

- Zabezpečení Metod ověření Klientem včetně případných přihlašovacích údajů a/nebo bezpečnostních certifikátů spojených s Metodami ověření (dále společně jen „Zabezpečovací údaje“) a zajištění, že přístup k Zabezpečovacím údajům a jejich distribuce jsou omezeny pouze na oprávněné osoby Klienta. Metody ověření a související

Zabezpečovací údaje představují metody, kterými Banka ověřuje původ Komunikací doručených Bance ze strany Klienta.

- Klient musí učinit veškeré přiměřené kroky k ochraně Zabezpečovacích údajů. V souladu s tím Banka důrazně doporučuje, aby Klient nesdílel Zabezpečovací údaje s třetí stranou.

Některé jurisdikce mohou před udělením přístupu k výkonu určitých funkcí požadovat, aby byly fyzické osoby (a jejich odpovídající Zabezpečovací údaje) identifikovány v souladu s platnými právními předpisy proti legalizaci výnosů z trestné činnosti.

Banka bere na vědomí, že Klient může v některých případech chtít sdílet Zabezpečovací údaje Klienta s třetí stranou nebo externím poskytovatelem služeb (mimo jiné včetně externího poskytovatele platebních služeb), u nichž Klient stanoví, že mohou mít přístup k Zabezpečovacím údajům (taková třetí strana nebo poskytovatel služeb se zde označuje jako „Oprávněná třetí strana“) za účelem přístupu a využívání CitiConnect za Klienta. V případě, že se Klient rozhodne sdílet své Zabezpečovací údaje s Oprávněnou třetí stranou, Banka důrazně doporučuje, aby Klient přijal veškeré přiměřené kroky k ochraně těchto údajů před zveřejněním neoprávněným třetím stranám, a aby zajistil přijetí těchto kroků i Oprávněnou třetí stranou. Banka je oprávněna jednat na základě jakékoli Komunikace, kterou obdrží za Klienta od Oprávněné třetí strany v souladu s těmito Postupy.

## C. Integrita dat a zabezpečené Komunikace

- Klient bude předávat data a jinak vyměňovat Komunikace s Bankou za využití internetu, e-mailu a/nebo faxu, které nejsou nutně zabezpečené komunikační a doručovací systémy. Banka využívá špičkové šifrovací metody (stanovené Bankou), které pomáhají zajistit, aby informace zůstaly důvěrné a aby se během přenosu nezměnily.

- Pokud má Klient podezření nebo se dozví o technické závadě nebo jakémkoli nesprávném přístupu ke službám Banky, komunikačním kanálům nebo Metodám ověření jakoukoli osobou (ať již oprávněnou či nikoli), Klient to neprodleně oznámí Bance. V případě nesprávného přístupu nebo použití oprávněnou osobou by měl Klient okamžitě podniknout kroky k ukončení takového přístupu oprávněné osoby ke službám Banky a komunikačním kanálům .

- Pokud Klient využívá formátování souborů a šifrovací software (ať už je poskytován Bankou nebo třetí stranou) na podporu formátování a rozpoznávání klientských dat a příkazů a jedná se Citi na základě Komunikací, pak Klient použije tento software výhradně k účelu, k němuž byl nainstalován.

# VIII. Další informace o zpracování plateb

## A. Lhůty pro doručení Platebního Příkazu

**Standardní lhůty pro doručení odchozího platebního příkazu**

| Platební produkt | | Elektronické transakce | Manuální transakce (pošta,fax,doručené osobně) |
|---|---|---|---|
| Odchozí tuzemská platba | | 18:30 | 11:00 |
| Expresní odchozí tuzemská platba | | 12:00* | 9:00 |
| Zahraniční odchozí platba | | 15:00 | 11:00 |
| Odchozí platba SEPA / Odchozí platba SEPA - Hromadná | | 17:00 | - |
| Odchozí platba SEPA – Expresní / Odchozí platba SEPA – Expresní hromadná | | 13:00 | - |
| Přímé inkaso | | 18:30 | 11:00 |
| Interní platba v rámci Banky | - v domácí měně | 18:30 | 11:00 |
| | - v zahraniční měně | 15:00 | 11:00 |

Poznámka:

* Podmínkou zpracování Expresní odchozí tuzemské platby je, mimo jiné, dostatek použitelných peněžních prostředků na daném účtu Klienta, a to nejpozději do konce lhůty platné pro doručení platebního příkazu.

**Standardní lhůty pro doručení a způsob zpracování příchozího platebního příkazu**

| Platební produkt | Peněžní prostředky přijaty Bankou |
|---|---|
| Příchozí tuzemská platba | v den přijetí prostředků (D) |
| Zahraniční příchozí platba – číslo účtu zadané ve formátu IBAN | v den přijetí prostředků (D) 17:00* |
| – číslo účtu zadané v jiném formátu | v den přijetí prostředků (D) 15:00* |
| Příchozí platba SEPA | v den přijetí prostředků (D) 17:00* |
| **Připsání prostředků na účet Klienta u Banky** | **D + 0*** |

Poznámka:

"D" znamená den, kdy Banka obdrží částku převodu od poskytovatele plátce/zprostředkující banky.

* V případě zahraniční příchozí platby a příchozí platby SEPA bude částka převodu připsána na účet Klienta vedený u Banky ve stejný den, kdy Banka obdrží tuto částku, pouze tehdy, pokud Banka obdrží do 15:00, resp. 17:00 tohoto dne potvrzení o přijetí částky převodu na účet Banky (krytí platby). Obdrží-li Banka toto potvrzení později, budou peněžní prostředky připsány na účet Klienta až následující pracovní den.

| Standardní lhůty pro doručení příkazu k převodu formou vkladu a výběru hotovosti | |
|---|---|
| **Druh převodu** | **Předání příkazu Bance** |
| vklad hotovosti na účet Klienta | v provozní době pobočky (pokladny)* |
| výběr hotovosti z účtu Klienta | v provozní době pobočky (pokladny)* |
| Poznámka:<br><br>* Provozní doba poboček je uvedena na internetových stránkách Banky www.citibank.cz. | |

Výše uvedené mezní časy (cut-off times) pro doručení platebního příkazu se považují za okamžik blízko konce provozní doby Banky ve smyslu ustanovení § 158 odst. 3 Zákona o platebním styku.

## B. Maximální lhůty pro provedení Zahraničních odchozích plateb v jiných měnách než CZK nebo EUR

Zahraniční odchozí platba v jiné měně než CZK nebo EUR bude na účet poskytovatele příjemce připsána vždy nejpozději druhý pracovní den po odepsání platebních prostředků z platebního účtu Klienta, tj. Banka připíše takovou Zahraniční odchozí platbu na účet poskytovatele příjemce maximálně v režimu D+2.

## D. Manuální Platební příkazy k převodu prostředků

K tomu, aby Klient mohl zadávat manuální Platební příkazy k převodu prostředků, musí Klient vyplnit a Bance doručit Globální formulář k manuální autorizací transakcí (*Global Manual Transaction Authorization*) (GMTA), který doplňuje Hlavní podmínky pro účty a služby (*Master Account and Service Terms*) (MAST) a jakékoli další podmínky vztahující se k účtům.

Klient, který neposkytl Bance formulář GMTA, rozumí a souhlasí s tím, že jím zadané manuální Platební příkazy k převodu prostředků může Banka odmítnout.

## E. Poplatek NSTP

Pokud prostřednictvím elektronického bankovnictví Klient zadává Zahraniční odchozí platbu, která je směřována do banky v členském státu EHP, **je povinen při zadávání této platby uvést BIC banky příjemce a IBAN**, a to bez ohledu na měnu platební transakce. V případě, že Platební příkaz doručený Bance nebude obsahovat tyto náležitosti, bude Klientovi účtován „Poplatek NSTP“ („Non Straight Through Processing“) ve výši dle aktuálního sazebníku Banky. Tento poplatek bude Klientovi Bankou účtován během 5-ti pracovních dní ode dne zpracování Platebního příkazu. Za tento poplatek Banka přebírá odpovědnost a uhradí veškeré náklady spojené s nutností manuálního zpracování Zahraniční odchozí platby, která byla zadána prostřednictvím elektronického bankovnictví a která neobsahuje údaje vyžadované bankami v členských státech EHP. Jedná se zejména o poplatek Banky a bank přijemců plateb za nesprávně strukturovaný platební příkaz.

K tomu, aby Klient nemusel uvedený poplatek hradit, je tedy nutné, aby Zahraniční odchozí platba, zadaná prostřednictvím elektronického bankovnictví, definovala bankovní spojení příjemce platby pomocí následujících údajů:

- BIC* (SWIFT) banky příjemce zadaný výběrem z knihovny (CitiDirect) nebo uvedený v prvním řádku pole „Banka příjemce“. Jde o samostatný řetězec znaků o maximální délce 8 nebo 11 znaků (např. CITICZPX).
- IBAN* (číslo účtu příjemce ve formátu IBAN), který je uveden samostatně, a to bez mezer a znaků před/po.

Výše zmíněné platí pro všechny Zahraniční odchozí platby, které jsou zadány prostřednictvím elektronického bankovnictví a které jsou zaslány do bank v členských státech EHP, a to bez ohledu na měnu Platební transakce a bez ohledu na indikátor poplatků SHA/BEN/OUR.

**** Informace o BIC a IBAN Klient získá od svých obchodních partnerů. Po specifikaci banky příjemce jejím BIC (SWIFT) kódem již není nutné poskytovat další informace o bance příjemce. V případě, že se nebude shodovat Klientem uvedený název banky příjemce a BIC kód, Banka jako rozhodující pro zpracování platební transakce považuje Klientem uvedený BIC kód. Stejné pravidlo platí obecně pro všechny typy platebních převodů uskutečňovaných Bankou.***

# IX. AML informační povinnost ve vztahu ke zpracování osobních údajů

Podle zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů ("**AML zákon**") je Banka povinna shromažďovat a zpracovávat osobní údaje klientů, osob jednajících jménem klienta, skutečných majitelů, členů statutárního orgánu, zástupců právnické osoby (klienta) v tomto orgánu anebo v postavení obdobném postavení člena statutárního orgánu, či jiných osob v rámci obchodního vztahu nebo provedením obchodu mimo obchodní vztah, a to za účelem zabránění zneužívání finančního systému k legalizaci výnosů z trestné činnosti a k financování terorismu a vytvoření podmínek pro odhalování takového jednání.

V rámci plnění povinností Banky podle AML zákona jsou obvykle shromažďovány a zpracovávány následující osobní údaje:

1) všechna jména a příjmení,
2) rodné číslo, a nebylo-li přiděleno, datum narození,
3) místo narození,
4) pohlaví,
5) trvalý nebo jiný pobyt a státní občanství;
6) jde-li o podnikající fyzickou osobu, též její obchodní firma, odlišující dodatek nebo další označení, místo podnikání a identifikační číslo osoby.

Odůvodňuje-li to hodnocení rizik podle AML zákona, mohou být kromě osobních údajů uvedených výše shromažďovány a zpracovávány i další údaje k identifikaci fyzické osoby, jakými jsou zejména číslo telefonu, adresa pro doručování elektronické pošty, údaje o zaměstnání nebo zaměstnavateli apod.

Osobní údaje jsou shromažďovány a zpracovávány po dobu obchodního vztahu s příslušným klientem a dále nejméně 10 let od konce roku, ve kterém byl takový obchodní vztah ukončen.

Banka může předat získané osobní údaje třetím osobám, které využívá k plnění svých povinností podle AML zákona, přičemž osobní údaje mohou být v takovém případě předány do jurisdikcí jiných států, které přísnou ochranu dat nebo zákony na ochranu osobních dat nemají. Seznam zpracovatelů osobních údajů pro účely plnění povinností Banky podle AML zákona je uveden na internetových stránkách Banky (www.citibank.cz).

Poskytnutí příslušných osobních údajů je dobrovolné, avšak jejich neposkytnutí pro účely plnění povinností Banky podle AML zákona bude zpravidla znamenat, že Banka nebude moci poskytnout příslušné služby nebo uzavřít příslušný obchod, popřípadě bude nucena existující smluvní vztahy s Klientem ukončit.

Subjekt osobních údajů má právo na přístup ke svým osobním údajům shromažďovaným Bankou a práva uvedená v § 21 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

# X. Reklamace služeb a stížnosti

Reklamace služeb a stížnosti Klienta Banka vyřizuje dle platného Reklamačního řádu Banky pro právnické osoby a podnikající fyzické osoby (dále jen „**Reklamační řád**“), který Banka uveřejňuje na svých internetových stránkách (www.citibank.cz) a který je k nahlédnutí v sídle odštěpného závodu Banky v České republice – Citibank Europe plc, organizační složka a v každé pobočce Banky v České republice.

# XI. Závěr

Děkujeme, že jste si vybrali Citi Treasury and Trade Solutions (TTS) k řešení Vašich potřeb týkajících se cash managementu. Neváhejte, prosíme, kontaktovat Vašeho Citi bankéře s jakýmikoli dodatečnými dotazy, které máte ohledně TTS služeb.

Tato Uživatelská příručka vstupuje v platnost a nabývá účinnosti 13. ledna 2018.

# XII. Definice

V této Uživatelské příručce mají níže uvedené termíny následující význam:

"**Členský stát**" znamená členský stát Evropské unie nebo jiný smluvní stát Dohody o Evropském hospodářském prostoru;

"**EHP**" znamená Evropský hospodářský prostor;

"**Platební příkaz**" znamená pokyn poskytovateli Platební služby, jímž plátce nebo příjemce žádá o provedení Platební transakce;

"**Platební služba**" znamená platební službu ve smyslu Zákona o platebním styku;

"**Platební transakce**" znamená vložení peněžních prostředků na Platební účet, výběr peněžních prostředků z Platebního účtu nebo převod peněžních prostředků, je-li tato transakce prováděna v rámci Platební služby;

"**Platební účet**" znamená účet, který slouží k provádění Platebních transakcí;

"**SEPA prostor**" znamená prostor tvořený státy účastnícími se projektu Evropské unie nazývaného SEPA (Single Euro Payments Area – jednotná oblast pro platby v eurech);

"**Transakce EHP**" znamená platební transakci, která (i) v případě odchozích platebních transakcí Klienta, kde Banka vystupuje jako poskytovatel plátce, je poskytovatelem příjemce poskytnuta v Členském státě nebo (ii) v případě příchozích platebních transakcí Klienta, kde Banka vystupuje jako poskytovatel příjemce, je poskytovatelem plátce poskytnuta v Členském státě;

"**Zákon o platebním styku**" znamená zákon č. 370/2017 Sb., o platebním styku, v platném znění.