Citfin – Finanční trhy, a.s.

Bucharova 1423/6b, 158 00 Prague 13
+420 234 092 011 | info@citfin.cz | citfin.eu

Technical Information

1. Introduction

1.1 This Technical Information clarifies the procedures and specifications relating to Authentication and Authorisation; administration of Payment Transactions; instructions and settlement of Exchange Trades; use of Phonebanking; use of the Client API and Citfin API services; and handling of unauthorised or incorrectly executed Payment Transactions.

Unless otherwise stated, capitalised terms have the meaning assigned in the General Terms and Conditions ("GTC").

2. Authentication and Authorisation Processes

2.1 Authentication

Authentication requires two-factor verification. In Citfin's internet banking, this includes: a knowledge factor (Client ID and PIN provided to the Client); and a possession factor (Verification Device).

When performed by a Citfin staff member, authentication is completed by verifying the Client's identity and sending a Verification Code to the Client's Verification Device.

2.2 Authorisation

When authorising Payment Transactions via internet banking, the knowledge factor (Client ID and PIN) may be reused within a session. The Client logs in using both knowledge and possession factors and then authorises transactions using the possession factor alone (Verification Device).

When performed by Citfin personnel, authorisation includes identity verification and transmission of a Verification Code to the Verification Device.

No separate authorisation is required if an Exchange Trade is concluded with the Client by the Dealing Dept. over the phone using the registered mobile number listed in the Framework Agreement.

2.3 Verification Code

The Verification Code may be obtained via one of the following Verification Devices:

a) a mobile phone registered in the Framework Agreement, to which Citfin sends a Verification Code via text message, either upon login to internet banking, use of Phonebanking, or request for information about the CPA and Client;

b) a Token provided by Citfin, which generates a Verification Code at the Client's request.

If no Verification Code is provided during Authentication or Authorisation—or if the code is incorrect—Citfin will not provide the requested Service.

2.4 Alternative Verification

If the Client is unable to use a Verification Code as part of provision of Services due to technical reasons on Citfin's side, Citfin may request Alternative Verification. This involves verifying the Client's identity using a Civil ID number or Client ID.

Clients may also initiate Alternative Verification when requesting the blocking of communication or Verification Devices.

Authentication by sending a code via text message is not performed based on a recorded telephone call with the Client using the Client's registered mobile number (during which the Client is identified via telephone).

Upon signing the Framework Agreement, Citfin will deliver the PIN and/or Token to the Client, depending on the selected Services, as follows: via Citfin's online onboarding interface; n person upon signature of the Framework Agreement; or by registered post after signed delivery of the Framework Agreement to Citfin. Citfin sends the Client ID via encrypted email after the activation of internet banking via encrypted email.

3. Administration of Outgoing Payment Transactions

3.1 Outgoing Payment Transactions are initiated based on a Payment Order that:

a) contains all mandatory fields listed in Section 3.3;

b) is submitted via Citfin internet banking, Phonebanking, or as an indirect Payment Order via the Citfin API; and

c) is verified in accordance with the GTC.

3.2 Citfin will execute an Outgoing Payment Transaction at the Client's request if:

a) sufficient funds are available in the Client's CPA to settle the transaction; and

b) the Payment Order and the funding of the CPA are received by Citfin before the cut-off time published at www.citfin.cz, on the maturity date indicated in the

Payment Order. Otherwise, the Payment Order is deemed received at the start of the next Business Day.

3.3 Mandatory Fields in Payment Orders

Mandatory elements of a valid Payment Order are published at www.citfin.cz in section Foreign payments.

Before submitting Payment Orders in foreign currencies, Clients must check any specific requirements in the current Citfin Payment Instructions, also available at www.citfin.cz.

3.4 Payment processing categories (e.g., STANDARD, URGENT) are listed on www.citfin.cz, in section Foreign payments.

3.5 Payment execution deadlines may be extended if Citfin is required to act in accordance with AML laws (AMLZ). For cross-border payments, crediting to the recipient's bank may be delayed due to public holidays in the destination country or currency jurisdiction. For payments outside the EEA, timing depends on correspondent bank processing.

3.6 Fee Models

The applicable charge type may involve

a) **OUR** – all fees (originating, receiving, and intermediary) paid by the Payer;

b) **SHA** – the Payer covers the originating bank's fees; the Recipient covers receiving and intermediary bank charges;

c) **BEN** – all fees are borne by the Recipient, who receives the net amount.

3.7 According to legal regulations, in the case of transfers within the European Economic Area (EEA) in the currencies of EEA member states that do not involve currency exchange, the SHA bank fee type applies. If a different type of fee is specified on the Payment Order for payments within the above-mentioned currencies and countries, Citfin is entitled to change the type of bank fees to the SHA bank fee. For transfers outside EEA member states or in currencies of countries other than EEA members, the Client has the right to specify any type of bank fees. The Client acknowledges that for Payment Transactions outside the EEA, the OUR fee type may be changed by the Correspondent Foreign Bank to the SHA or BEN fee type, in which case the Payment Recipient may receive a reduced amount of funds according to the given fee type.

3.8 A Payment Order is deemed received when Citfin receives it directly from the Client, or Citfin receives it from a Third Party acting on the Client's behalf.

If Citfin and the Client have agreed that the Payment Transaction is to be executed on a future date, upon fulfilment of certain conditions, or at the end of a specific period, the agreed date or condition fulfilment constitutes the moment of receipt.

3.9 If Citfin notifies the Client of an error or inconsistency in the Payment Order, the Client may amend it by 17:00 on the next Business Day.

Notification is sent by phone or via internet banking. Citfin will inform the Client of any risks associated with executing the uncorrected Payment Order.

If the Client fails to amend the Order:

a) Citfin will not process it if the payment is inexecutable (e.g., invalid IBAN or SWIFT code) and will notify the Client; or

b) Citfin may execute the Order as-is, provided the payment is executable. The Client bears in mind that, in such as case, Citfin has no liability for any resulting loss caused by execution of the Payment Order.

4. Execution of Incoming Payment Transactions

4.1 The Client must properly and timely instruct the remitter (i.e. the originator of the incoming payment) on the following:

a) the account number which must match one of Citfin's accounts listed at www.citfin.cz;

b) recipient name must match Citfin's legal name as shown in the Framework Agreement header;

c) recipient's bank name must match the bank listed in Citfin's Separate Account directory (available at www.citfin.cz), including SWIFT code and any required correspondent bank information;

d) incoming payments to the CPA reference must include:

- identification data enabling Citfin to allocate the payment to the correct Client;
- payment-related information (e.g. invoice number) to enable Client-side identification.

5.2. Responsibility for Processing Incoming Funds

4.2 Citfin shall handle the identification of received funds on the CPA with professional diligence but is not liable for whether the incoming payment to the CPA is executed at all; or whether it is executed correctly and on time.

The client acknowledges that this payment service is provided by Citfin only from the moment the relevant amount is received in Citfin's Separate Account. Citfin is not responsible for any documents related to Incoming Payment Transactions originating from third parties, including other credit institutions. Citfin shall be guided exclusively by the notification for the Incoming Payment Transaction. Citfin is obliged to immediately inform the Client of the receipt of a properly identified Incoming Payment Transaction to the CPA, or after the Payment Transaction has been credited to Citfin's Separate Account, as well as of any differences between the Client's notification and the actual Incoming Payment Transaction

to the CPA.

4.3 If a payment received on Citfin's Separate Account cannot be reliably matched to a specific Client or instruction, Citfin will attempt to identify it with professional care to identify the Incoming Payment Transaction; equest a written declaration from the Client confirming:the identity of the remitter; the purpose of the payment; and the expected amount.

It is the decision of Citfin to decide if the Client, through their declaration on the Incoming Payment Transaction, has clearly identified the payment.

4.4 If no match is found after 15 calendar days from the crediting of funds to Citfin's Separate Account, Citfin will investigate via the banking system; and request the remitter to confirm or identify the Incoming Payment Transaction.

If, after 45 days, no match has been confirmed, Citfin will return the funds to the remitter.

5. Unauthorised Payment Transactions

5.1 The Client shall bear the loss from unauthorised outgoing transactions:

a) up to EUR 50, if the loss resulted from use of a lost or stolen Verification Device, or the misuse of internet banking or Phonebanking;

b) in full, if caused by:

- fraud; or intentional or grossly negligent failure to protect credentials and security devices and use them in line with the GTC (namely, they are obligated, upon receipt of the Verification Device and access to internet and Phonebanking to take all adequate measures to protect their security features;
- promptly report loss, theft, misuse, or unauthorised use of the Verification Device, online banking or Phonebanking.

5.2 The Client is not liable for unauthorised Outgoing Payment Transactions if they have not acted in a fraudulent manner and:

a) the loss occurred after the Client reported the incident;

b) Citfin failed to provide a suitable mechanism for such reporting;

c) Citfin failed to enforce strong client authentication under the PSA.

5.3 The EUR 50 liability cap does not apply if:

a) the Client could not have detected the misuse before the transaction occurred; or

b) the misuse resulted from Citfin's own actions.

5.4 If Citfin is liable, it must immediately, by the end of the following Business Day at the latest, following notification of the unauthorised Outgoing Payment Transaction:

a) restore the CPA to the state it would have been in had the transaction not occurred; or

b) refund the amount of the transaction, including all fees and lost interest, provided the steps outlined in item a) are not sufficient.

5.5 Citfin is not required to refund the Client if it has reason to suspect fraud and has reported such suspicion to the supervisory authority in writing.

6. Incorrectly Executed Payment Transactions by Citfin

6.1 If the Client notifies Citfin that they do not wish an incorrectly executed outgoing Payment Transaction to proceed, Citfin shall immediately:

a) restore the CPA to the state it would have been in had the amount not been debited; or

b) refund the amount of the transaction, the associated fee, and any lost interest—if restoration under (a) is not possible.

6.2 This applies only incorrect Outgoing Payment Transactions where the amounts have not yet credited to the recipient's provider at the time the Client informs Citfin of their intent to decline the transaction. Citfin must demonstrate such non-crediting to the Client (and, if applicable, the recipient's provider).

6.3 Citfin shall immediately ensure the full amount is credited to the recipient's provider; and either:

a) restore the Client's account as if the transaction had been properly executed; or

b) refund fees and lost interest (if account restoration as per item a) is not feasible).

If the Client provided an incorrect unique identifier (e.g., IBAN), Citfin considers the transaction to have been properly executed, but will make reasonable efforts to retrieve the funds and return them to the Client.

6.4 If the transaction was initiated indirectly (e.g., via a third-party provider), it is considered incorrectly executed if it does not match the original order submitted by the Client to that third party—even if it matches the instruction received by Citfin. In such cases, Citfin is responsible for corrective action toward the Client.

7. Execution and Settlement of Exchange Trades

7.1 Exchange Trades may be entered into on the days and during the hours listed at www.citfin.cz, in the Contacts section.

7.2 Spot and Forward Trade Instruction Requirements

Each instruction must contain the following mandatory elements:

Required Information	Spot Trades	Forward Trades
ISO code of currency being purchased	✓	✓
ISO code of currency being sold	✓	✓
Amount	✓	✓
Exchange rate	✓	See 7.3
Trade type	✓	✓
Settlement date	✓	✓
Settlement method	✓	✓

7.3 Order Instruction Requirements

Orders may be placed via the Dealing Desk and must contain:

Required Information	Orders
ISO code of purchased currency	**P**
ISO code of sold currency	**P**
Amount	**P**
Target Spot Rate (Client's desired rate)	**P**
Trade type	**P**
Order type (as offered by Citfin on its website)	**P**
Order validity (maximum 12 months) This is the period during which, upon reaching a rate equal to the agreed rate, or as close as possible to the agreed rate if it cannot be equalled (matched) due to market conditions, the Spot Trade is concluded. The validity of the Order is a maximum of 12 months from the date of submission. If the rate is not reached during the validity period, the Order expires automatically at 23:59:59 CET on the last day of validity (or the last preceding Business Day if it is not a Business Day), unless a specific expiry time is agreed	**P**

7.4 Available Currencies and Trade Methods

Spot and Forward Trades may be entered into for the currencies and via the methods listed on www.citfin.cz, in the Foreign Exchange and Futures sections.

7.5 Trade Limits

Instructions must comply with the limits specified in Articles 7.6 and 7.7 of the GTC.

7.6 Maximum Limits for Online Spot Trades

- Maximum single trade volume: CZK 15,000,000 or foreign currency equivalent (unless otherwise specified);
- Maximum daily cumulative limit: CZK 250,000,000 or foreign currency equivalent.

If the Client exceeds the daily limit, Citfin may cancel the Spot Trades exceeding the limit(s); and execute mirror (offsetting) transactions under the same terms.

Confirmation will be sent immediately to the Client. The Client agrees to cover all related costs and acknowledges their obligation not to exceed the stated limits.

7.7 Minimum Limits for Orders and Forward Trades

Minimum transaction sizes are listed at www.citfin.cz, in the Currency Order and Futures sections.

7.8 Handling of CPA Balance After Termination

If the Framework Agreement is terminated and the Client does not instruct Citfin on how to dispose of the CPA balance, the Client must submit such instructions prior to the date of terminating the CPA: via internet banking; in hardcopy form with a notarised signature; or via the Client's data box.

If no such instruction is received from the Client, Citfin shall: transfer the remaining balance on the CPA to internal records ("auxiliary register"); and ,convert foreign currency balances held on the CPA into CZK at Citfin's current rate on the final day of the notice period.

8. Citfin Internet Banking

8.1 If the Parties agree in the Framework Agreement, communication between Citfin and the Client may be conducted electronically via Citfin's internet banking. The Client may designate any number of Authorised Persons. For each, specific access rights and payment limits can be configured:

a) Administrator / Full Active Rights – may initiate outgoing Payment Transactions from the CPA;

b) Active with dual-signature restriction (Variant 1) – transactions from the CPA must be authorised by the Client (if a natural person) or the statutory body (if a legal person);

c) Active with dual-signature restriction (Variant 2) – transactions from the CPA must be authorised by another Authorised Person with active rights;

d) Passive Right – allows view-only access to CPA balances and transaction history.

8.2 The internet banking service is secured by a GlobalSign certificate issued for www.bankservis.cz, which encrypts all communication between Citfin and the Client.

The Client is not permitted to conduct operations on the www.bankservis.cz server unless encrypted by this

certificate.

Citfin reserves the right to refuse the execution of operations or provision of information if they are not authenticated in accordance with the GTC.

8.3 To use internet banking, the Client must have the following:

a) a computer with internet access, and access via www.bankservis.cz;

b) a registered mobile phone number active on a Czech mobile network (foreign numbers must be pre-approved); or

c) a Token provided by Citfin for receiving Verification Codes;

d) a Registered Email used to activate or restore internet banking access.

8.4 The Client may use the service 24/7. Citfin may temporarily limit access for maintenance. Citfin may use internet banking to eliver the Client notices; and provide transaction reports in accordance with the PSA.

In the event of system outage for the internet banking and all other communications resources per the GTC and the Account Agreement, communications between Citfin and the Client will continue via www.citfin.cz.

9. Online Trading via Citfin Internet Banking

9.1 The Online Trading feature allows Clients to conclude Spot Trades at real-time Spot Rates directly via internet banking. Authorised Persons with the following access rights may trade. They include

a) Administrator;

b) Active;

c) Active with Client dual-signature restriction;

d) Active with any dual-signature restriction.

The ful description of permissions is in Article 8.1.

Online Trading is available on days and times listed at www.citfin.cz. Citfin reserves the right, in exceptional cases, to suspend Online Trading, i.e., during data service outages or system failures.

10. Phonebanking

10.1 Phonebanking enables communication between Citfin and the Client. To use the service, the Client must have:

a) a mobile phone active on a Czech mobile network (foreign numbers must be pre-approved); or

b) a Token for receipt of Authorisation Codes provided by Citfin.

10.2 Phonebanking is available via specific phone lines published on www.citfin.cz. To issue Payment Orders per the terms in the GTC, the Client provides required data by phone. During the call, the Client identifies themselves using their Client ID received when concluding the Framework Agreement and a Verification Code also received per the GTC.

The Code authorises a Citfin staff member to act as a "shadow user" and process the Client's Payment Order in the system.

Furthermore, during the telephone call, the Client shall provide the details necessary to execute the Payment Transaction or Payment Order for entry into the system. Immediately thereafter, the Client shall be sent a Verification Code in accordance with the GTC, which the Client shall communicate to the Citfin employee, thereby enabling them to execute the Payment Transaction.

10.3 In the event that the Client requests a Payment Transaction in favour of a person whose details are not yet entered in the system, i.e., it is the first Payment Transaction in favour of this person, it is recommended to deliver the payment title, i.e., the relevant invoice, to Citfin in advance as a scanned copy attached to an email. By communicating the Verification Code to a Citfin employee, the Client agrees to the parameters of the Payment Order, i.e., confirms its correctness.

The Client may use the Phonebanking services on the days and at the times listed on www.citfin.cz, in the Contact section. Citfin reserves the right, in exceptional cases, particularly in cases of external circumstances or force majeure, not to provide Phonebanking services for a certain necessary period of time.

11. Citfin API

11.1 The Citfin API allows automated access to the CPA through a data interface that connects Citfin's system with third-party applications.

11.2 Access requires an amendment to the Framework Agreement granting Citfin API access. Access can only be granted to a user as defined in Article 8.1. of this document.

11.3 All authentications and authorisations are performed using a Token.

11.4 Permissions for specific Citfin API services are authorised by a code generated via Token (mobile token).

Authorisations via token are valid for 90 days and may be withdrawn by the Client at any time. The Client is entitled to refuse authorisation of an instruction to use the Citfin API Service or subsequently revoke permission to use any Citfin API Service by means of an authorised instruction.

11.5 Indirect Payment Orders may only be executed if:

a) they are properly authorised; and

b) all required conditions and data submission are met.

In such a case, Citfin is obliged to accept the indirectly given Payment Order and execute the requested Payment Transaction. Citfin shall immediately notify the Third Party that it has accepted the indirectly given Payment Order and

will execute the Payment Transaction in accordance with the relevant indirectly given Payment Order. An indirectly given Payment Order cannot be revoked after Citfin sends information about the acceptance of this Payment Order to the Third Party.

11.6 Citfin may refuse an API order if:

a) it suspects unauthorised or fraudulent use of the Verification Device or other Client security components;

b) the order was placed by an unauthorised third party;

c) the third party failed to verify its identity; or

d) rejection is required or permitted by law.

11.7 Citfin shall inform the Client of the rejection and the grounds therefor: via internet banking if possible; otherwise, without undue delay. This does not apply if doing so would compromise payment system security.

Citfin must also inform the CNB of the rejection without delay. Citfin will also inform the Client in the aforementioned way in cases of repeated incorrect authorisation attempts. Citfin may permanently block the Citfin API service and notify the Client.

12. Client API

12.1 The Client API is a one-way data interface allowing access to information on all movements in the Client's CPA.

12.2 It is available to any Authorised Person with active or passive internet banking rights. Access is granted upon identity verification via text message (SMS).

12.3 Upon activation, a Token is issued and sent to the Authorised Person in a password-protected ZIP file via email.

12.4 All API authentications and authorisations are carried out using the Token assigned to the Authorised Person.

13. Validity of this Technical Information

13.1 This Technical Information are valid as of December 01, 2025.