TECHNICAL PARAMETERS AND SPECIFICATION OF OPERATION OF ELECTRONIC BANKING SERVICES

1. APPLICATIONS

through which services are provided within the ČSOB Platform:

- **A.** web applications (ČSOB BusinessBanking App, Moja ČSOB App)
- **B.** mobile application (ČSOB SmartBanking App)
- **C.** ČSOB SmartToken App
- **D.** ČSOB API application programming interface, PSD2 (ČSOB API)

2. TECHNICAL PARAMETERS

2.1. Minimum technical specifications

1. For the ČSOB BusinessBanking App Service:

Devices	Computer, laptop, tablet, mobile phone
Operating system	MS Windows Vista/7, Mac OS X+, Android 1.x.x+, iOS, RIM, Symbian
Web browser	MS Internet Explorer 7.0 and later, Mozilla Firefox 3.0 and later, Google Chrome 4.0 and later, Safari 3.0 and later, native Android, iOS and Symbian browsers, Opera Mini / Mobile
JavaScript, Cookies	Enabled
Other	Adobe Acrobat Reader 6.0 and later

2. For the ČSOB SmartBanking App Service:

Mobile device	Mobile phone, tablet
Online sources	AppStore, Google Play and Huawei AppGallery
Operating systems	Current information on support for Android (version 9+) and iOS (version 14+) is always available in the distribution store for the relevant operating system (Google Play and Apple AppStore).

2.2. Account transaction limits

For ČSOB BusinessBanking	The limit for an Authorised Person is set by the Client or Account Holder (statutory representative), or an Authorised Person designated by them and empowered to do so under the assigned Rights Profile.
For ČSOB SmartBanking	The Bank sets no restriction on the main transaction limit for the Account Holder. The Account Holder sets this limit for an Authorised Person.

2.3. Limit for the authorisation instrument

ČSOB SmartToken App / Token DP770 for the BusinessBanking App	No limit is set by the Bank.
ČSOB SmartToken for the Moja ČSOB App	The Bank sets the limit at €34,000. The holder of the IPPID to which the token is linked may change it at a branch.
PIN for the IPPID for the ČSOB SmartBanking App	The Bank sets the limit at €50,000 per day and €150,000 per week. This limit cannot be changed.

The daily and weekly limits are the sum of the amounts of all transactions submitted to the Bank through the ELB Services, and the set limit applies to all accounts accessible to the Client. The amounts of transactions submitted through the Moja ČSOB App and the ČSOB SmartBanking App are not aggregated with each other. The daily/weekly limit for an Authentication/Authorisation Code does not apply to transactions submitted to the Bank through the Moja ČSOB App using the ČSOB SmartToken App.

2.4. Security Features

IPPID	An 8-digit number identifying a specific Authorised Person unambiguously. It is used to log in to the ČSOB BusinessBanking App and to Identify the Authorised Person when logging in to and activating the ČSOB SmartToken App and the ČSOB SmartBanking App.	A telephone application for unblocking by an Authorised Person will be rejected if the Bank processed the last unblocking application of the Client on day (D), or the preceding business day (D-1), relative to the current telephone application for unblocking.
PIN for the IPPID	A 5-digit number used to Authenticate the Authorised Person/Client.	
Password for the ČSOB SmartToken App	A 6-digit number chosen by the Client on activation of the SmartToken App and entered each time the App is used.	

2.5. Security Instruments

1. For ČSOB BusinessBanking:

Token DP770	A hardware device used for Authentication when logging in to the ČSOB BusinessBanking App and for Authorisation of payments and other active operations.	The device may be unblocked no more than three times during its entire period of use. It is then permanently blocked and a new device must be obtained in person at a Bank branch.
ČSOB SmartToken App	A mobile app usable offline and online for Authentication and Authorisation of active operations in the ČSOB BusinessBanking App. It generates an online signature or one-time offline codes for activation of the ČSOB SmartBanking App, signing transactions in ČSOB electronic banking and confirmation of 3-D Secure online card payments.	

TECHNICAL PARAMETERS AND SPECIFICATION OF OPERATION OF ELECTRONIC BANKING SERVICES

2. Identification and verification of the identity (Authentication) of the Authorised Person and Authorisation of orders use two factors as follows:

Access to the ČSOB BusinessBanking App		
Identification	Authentication	
Identification Number	1st factor	PIN for the IPPID
	2nd factor	Code generated by Token DP770
		Confirmation in the ČSOB SmartToken App
	Five unsuccessful attempts block the IPPID in all electronic banking services.	
Initial login to the ČSOB BusinessBanking App – Authentication		
PIN for the IPPID	Setting the PIN for the IPPID	
Identification	Authentication	
Instructions – Token DP770		
Authentication	Authorisation	
PIN for Token DP770	Scanning QR codes + confirmation with an Authorisation Code	
Blocking Token DP770	Five incorrect authorisation code entries block payment authentication / authorisation.	
Instructions – SmartToken App (active access)		
Authentication	Authorisation	
PIN for the SmartToken App	Offline version: Reading graphic codes scanned by SmartToken + confirmation with an authorisation code Online version: Confirmation in the SmartToken App	
Instructions – SmartToken App (passive access) – no authorisation available		

3. An Authorised Person Authorises an Instruction using Token DP770 or the SmartToken App in accordance with the Signature Rules. An Instruction entered will not be executed unless Authorised by the Authorised Person using Token DP770 or the SmartToken App.

Access to the ČSOB SmartBanking App		
App activation	Authorisation	
Identification Number	1st factor	PIN for the IPPID
	2nd factor	SmartToken App
Sign-in		
1st factor	Mobile device certified through the activation process	
2nd factor	PIN for the IPPID / Biometrics	
Instructions – PIN for the IPPID / Biometrics		
Authentication		
IPPID PIN / Biometrics	Five incorrect PIN entries block the IPPID Identification Number for all Services.	

The Bank blocks the Client's Identification Number (IPPID), preventing access to ELB Services, if the Client:

a) enters an incorrect PIN five consecutive times during Authentication; or
b) enters an incorrect Activation Code five consecutive times when activating ČSOB SmartBanking; or
c) enters one of the Secure Contacts incorrectly five consecutive times when regenerating the PIN.

The Bank will block the Client's authorisation element if the Client enters an incorrect code generated by the relevant device five consecutive times during Authentication or Authorisation, or enters an incorrect PIN five consecutive times when using the ČSOB SmartToken App. The Client may request unblocking of access or of the Authentication/Authorisation Code in person at a branch or by telephone, subject to Authentication.

2.6. Tokens for the ČSOB BusinessBanking App

	ČSOB SmartToken App	Token DP770
Available from	Google Play, App Store	Assigned at a branch to a specific Authorised Person
Available for operating systems	Android and iOS	Hardware device assigned at a branch

2.7. Security Features

1. For the ČSOB BusinessBanking App:

PIN for Token DP770	A 4- to 8-digit number chosen by the Authorised Person when first switching on the device.
Password for the SmartToken App	A 5-digit number chosen by the Authorised Person after first switching on the Token and entered each time the Token is used.
PIN for the IPPID	A 5-digit number automatically generated by the Bank system or created by the Authorised Person. In combination with the IPPID and a code from Token DP770 or confirmation of the transaction using SmartToken, it enables two-factor Authentication of the Authorised Person.
Authentication/Authorisation Code	A one-time numeric code with a limited validity period, generated using Token DP770 or SmartToken, for Authentication and Authorisation of active operations in selected services.

For the ČSOB BusinessBanking App, either the SmartToken App or Token DP770 may be used for one IPPID.

If an Authorised Person forgets their Security Features:

a) PIN (for the IPPID) - they may set a new PIN through the Service login page. This PIN will subsequently also apply to other Electronic Banking services to which the Authorised Person logs in using the IPPID Identification Number for which the PIN was changed, or using that PIN;

b) PIN (for Token DP770) - they must contact the Contact Centre by telephone.

2. For the ČSOB SmartBanking App:

Activation Code	An online signature in ČSOB SmartToken or an 8-digit one-time code with a limited validity period, used to confirm the activation process for the SmartBanking App. The Client obtains the Activation Code during activation in the ČSOB SmartToken App.
ČSOB SmartToken App	The ČSOB SmartToken App is used to activate the ČSOB SmartBanking App. With internet access, activation takes place automatically. Without internet access, the ČSOB SmartToken App displays the one-time Activation Code of the Client.
PIN for the IPPID	A 5-digit number used to Authenticate the Authorised Person.

3. For security reasons, the Bank may deactivate an active Security Instrument - the ČSOB SmartToken App - if the Client has not used it for more than six months. The Client may reactivate the ČSOB SmartToken App at any time after such deactivation.

4. The Bank may allow the Client (on mobile devices supporting the Bank's biometric functionality in the ČSOB SmartBanking App) to replace the PIN with another Security Feature (e.g. biometric data). The PIN may be changed solely through the Client's own action, in the self-service area available before logging in to the ČSOB BusinessBanking App, or in the ČSOB SmartBanking App. A successful PIN change requires the Client to have provided the Bank with Secure Contacts: a) a mobile telephone number and b) an email address.

2.8. Factors for authentication of login, transactions or Instructions

1. For the ČSOB BusinessBanking App:

1st factor	Static numeric code PIN for the Identification Number
2nd factor	A one-time numeric code with a limited validity period generated by the Token DP770 hardware authorisation device or the ČSOB SmartToken App software authorisation device, or confirmation of the transaction/Instruction in the ČSOB SmartToken App itself.

2. For the ČSOB SmartBanking App:

1st factor	Mobile device certified through the activation process
2nd factor	PIN for the IPPID / Biometrics

3. An Authorised Person may request unblocking of Security Instruments by telephone through the Contact Centre after Authentication for the purpose of unblocking the Security Instruments.

4. For reasons relating to the security of the Services provided, the Bank may require the Client to change the PIN within time limits set by the Bank.

2.9. Accepted file formats for the ČSOB BusinessBanking App

Data may be exported to:	Format: *.CSV, *.XLS	The Bank may change the format of exported data.

3. SPECIFICATION OF OPERATION OF ELECTRONIC BANKING SERVICES

3.1. ČSOB BusinessBanking App

1. Provides Clients with internet access to selected Bank products and services. Its use is equivalent to written communication. It is provided in Slovak and English; the Authorised Person sets the language when logging in to the App.

2. The Bank enables the following Instructions in the ČSOB BusinessBanking App:

a) an Authorised Person's instruction to execute a payment operation under the relevant Current Account Maintenance Terms and Conditions, or use Bank products and services in the current offer on the Bank's Website, including concluding, establishing, modifying or cancelling (terminating) a product and service and an Account Agreement/Product Agreement on behalf of the Client/Account Holder, or performing the necessary related acts on behalf of the Client/Account Holder;

b) an instruction by an Authorised Person to change data or define new payment card data and parameters in accordance with the current terms and conditions for that payment card published on the Bank's Website;

c) an instruction by an Authorised Person to change selected parameters of a deposit account agreement or a current account agreement (e.g. changing the language setting for statements available for viewing) in accordance with the current terms and conditions for that account published on the Bank's Website;

d) an instruction to change selected parameters of accounts of the Client/Account Holder made available by the Client/Account Holder to the Authorised Person for disposal of funds (e.g. changing the language setting, the frequency of statements available for viewing, or the frequency) in accordance with the current terms and conditions for that account published on the Bank's Website.

3. The Bank also provides the following through the ČSOB BusinessBanking App:

a) the ability for Clients to communicate with the Bank in real time (online);

b) the ability to sign payment orders jointly by two persons;

c) the ability to process data statements in the Client's information system (accounting);

d) the ability to manage individual Rights Profiles, Signature Rules and Signature Roles through an Authorised Person with the Administrator Rights Profile designated by the Client;

e) the ability for the Administrator to designate Authorised Persons who may purchase products and services on behalf of the Client within the Service;

f) the ability for the Administrator to create additional Administrators;

g) the ability for the Administrator to designate Authorised Persons who may inspect the Client's Documents, including personal data of an Authorised Person;

h) the ability to configure automatic delivery of information, which the Authorised Person may select after logging in to the ČSOB BusinessBanking App;

i) the ability to send account statements electronically to an Authorised Person's email address, subject to the Authorised Person configuring electronic account statement delivery after logging in to the ČSOB BusinessBanking App. A password must be entered to encrypt the electronic statement. Statements attached to email messages are encrypted and the Client must define the password through the Service themselves;

j) unilateral changes to output information on Instructions (Bank receipt confirmations for payment orders, Info messages) via selected Services (or a branch), using contact details specified by the Client;

k) delivery of SMS messages to a (mobile) telephone number and email messages to an email address. These messages are neither electronically signed nor encrypted;

l) making an account statement available to an Authorised Person;

m) configuration of account statement delivery to an email address through an Authorised Person, who must set/enter a password to encrypt the account statement for such delivery;

n) configuration of the frequency, form and language of account statements;

o) the ability for an Authorised Person to check the account balance and account history.

4. Further information on the ČSOB BusinessBanking App:

a) Files for download will be available to the Client in the ČSOB BusinessBanking App for a period determined by the Bank (specified in the App's help section).

b) To revoke, i.e. cancel, a payment order, Authorisation using Token DP770 or the SmartToken App by any one Authorised Person is sufficient, even if the payment order was originally signed by two Authorised Persons.

c) Transactions are posted individually, showing the relevant details, e.g. data identifying the operation, the payee and the amount debited to the account in the account currency.

3.2. ČSOB SmartBanking App

1. A mobile app that the Client may install on their own device (e.g. smartphone, tablet) from the official digital distribution platforms Google Play, App Store or Huawei AppGallery, gaining access to the part of the Platform where ČSOB offers services of ČSOB Group Members, SmartSlužby+, Kate - proactive personalised services with additional added value - and Personalised Services - personalised partner services.

2. Activation of the ČSOB SmartBanking App requires:

a) the Identification Number;

b) the PIN (for the Identification Number);

c) confirmation of activation in the ČSOB SmartToken App.

3. The ČSOB SmartBanking App may be deactivated:

a) using the App's "Settings" function; or

b) upon a telephone request to the Helpline; or

c) by uninstalling the App from the mobile device.

4. Each subsequent act by the Client contains the Identification Number (IPPID) and is Authorised with its PIN. The IPPID is stored in encrypted form in the ČSOB SmartBanking App and need not be re-entered.

3.3. ČSOB API (PSD2)

1. Provides access to payment initiation services (PIS - Payment Initiation Service), account information services (AIS - Account Information Service), and services confirming the availability of funds in a payment account for a card-based payment operation (CPIIS - Card-based Payment Instrument Issuer Service) under the Act on Payment Services. It enables execution of payment orders of the Authorised Person - user - from the Account Holder's Payment Account which were not entered in the Bank's information system, and provides the Authorised Person with access to the Account Holder's accounts and selected information.

2. The use of the ČSOB API (PSD2) Service is described in the ČSOB API (PSD2) Terms and Conditions published on the Bank's Website.

3. Use is subject to:

a) an 8-digit Identification Number allocated to an Authorised Person with ČSOB BusinessBanking App access;

b) the Authorised Person granting consent to an Authorised Third Party and completing strong Authentication in the ELB Services environment. An Authorised Third Party means a third party that has requested the Bank to allow it to intermediate this service, is listed in the register of the relevant national authority, holds a qualified certificate under the ČSOB API (PSD2) Terms and Conditions, and has been permitted by the Bank to intermediate these API (PSD2) Services.

3.4. Kate

1. The virtual assistant service is a proactive personalised service with additional added value. As part of such services, after the Client gives specific consent (depending on its scope), the Bank carries out automated analysis of the Client's personal data, uses it to assess the Client's personal situation and needs, and then provides personal assistance and additional support relating to services provided by ČSOB or Partner Services.

2. The Client may use it after Authentication within the SB service (i.e. only within the SB app on a supported mobile device) and additional services accessible through the SB service. It assists the Client with products and services of companies in the ČSOB financial group and with Partner Services, depending on the digital environment, the specific version of Kate (which the Client may choose to activate) and the Client's personal situation.

3. It provides services in the following areas:

a) Providing information, e.g. on products and services, expiry of a payment card, or insufficient funds in the Account for scheduled payments.

b) Improving the Client's convenience and customer experience, e.g. the Client may use the voice service to submit requests to Kate; Kate may also notify the Client of important matters such as the forthcoming expiry of the Client's identity card.

c) Identifying and eliminating potential risks, e.g. offering the Client the option of taking out travel insurance in connection with payment for an airline ticket.

d) Suggestions for optimising the Client's management of funds; e.g. suggesting the purchase of a prepaid public transport pass if this is more advantageous for the Client than buying single tickets.

4. Communicating with Kate:

Communication may begin after launching the service by clicking the relevant Kate icon in the SB app.

5. Ways to communicate with Kate:

a) through chat; or

b) through voice conversation provided via Google Services by Google LLC. By starting voice communication, the Client agrees to the Google Services terms of use, available in full at https://cloud.google.com/terms/aup.

6. Kate's functions:

If voice conversation is selected, communication may take place by voice or by a combination of voice and chat.

The ongoing communication may be displayed so that its content can be checked.

Voice communication requires the microphone on the mobile device to be switched on. ČSOB records voice communication with Kate; recording of the Client's speech stops automatically when voice communication ends or when the microphone is switched off during communication. The Client may end voice communication at any time by clicking the relevant icon or switching off the microphone.

For voice communication, the Client should find an environment without significant noise, speak clearly and follow the conversation on the screen.

There is no legal entitlement to voice conversation. The voice communication function may be unavailable for technical reasons or unsupported in certain situations (e.g. for security reasons).

ČSOB is not liable for the availability of the voice communication function or for its interruption, termination or complete unavailability for technical reasons.

7. Ending communication:

The Client may end communication at any time.

Kate may also end communication (particularly if the Client does not continue the conversation for a certain period, or for technical reasons). The end of communication will be displayed on the mobile device screen.

8. Overview of basic functions (i.e. categories in which Kate provides services):

Available on the Bank's Website in the section concerning Kate.

ČSOB may change the scope of Kate's functions (particularly as the Kate service develops) by updating the scope of services on the Bank's Website.

If adding or changing a function would constitute an amendment to an existing agreement between the Client and the Bank (e.g. an agreement concerning the Client's payment account or payment card), the Client may use that function only after the relevant agreement has been amended in accordance with the applicable legal regulations, or on the basis of the Client's express consent given through Kate. If Kate offers the Client a selected product or service (including ČSOB products or services), the offer may in selected cases (particularly depending on the development stage of the Kate service) be accepted directly through Kate.

Kate may also provide the Client with the assistance or help needed to accept the offer (e.g. by redirecting the Client to the product or service provider's website or to the relevant ČSOB employee).

9. General rules of use:

Assistance is fully automated and may therefore result in decisions being made without

human involvement. Information on automated decision-making and on personal data processing related to Kate services is provided in the Personal Data Protection Memorandum, available on the Bank's Website at https://www.csob.sk/pravne-informacie.

10. Liability for damage:

The Bank draws attention to the fact that it is not liable to the Client for damage resulting from improper use by the Client, malfunction of the mobile device through which the Client uses Kate, breach of security measures protecting the mobile device, the SB app and its digital environment, or use of Kate by a third party (other than the Client).

The Bank does not guarantee continuous availability, particularly for technical reasons, scheduled downtime or system maintenance.

11. Options for the Client's use of the services:

Available in two versions:

a) a basic version; and

b) a proactive version, intended only for Clients over 18 years of age with full legal capacity.

Persons under 18 may use Kate services only to a limited extent; the Bank determines and may change the scope of these services.

Basic version: communication is always initiated by the Client. The Client may ask Kate for help and support when using the SB app.

Proactive version: communication is initiated by the Client or Kate. Proactive Kate is activated automatically for the Client within SB. The Client may switch from the proactive to the basic version and vice versa at any time in the SB app settings. The proactive version also includes all functions of the basic version. It is a fully fledged digital assistant that contacts the Client on its own initiative with proposed solutions and provides comprehensive personalised assistance and support in view of the Client's personal situation and needs. Based on a deeper analysis of the Client's personal data and behaviour, it can address more complex situations and provide more complex assistance, as well as create and propose offers of ČSOB products and services and Partner Services tailored and prepared for the Client. The Client may submit a question or request concerning, in particular, ČSOB products and services or Partner Services available through SB. Kate can communicate proactively with the Client and contact the Client independently to address requests based on the Client's personal situation and assessed needs.

If resolving the Client's request requires activation of proactive Kate, fulfilment of specific conditions, specific consent, a specific act or conclusion of a separate agreement, the Client will be informed during communication with Kate.

When Kate actively contacts the Client, it always checks whether the Client is interested in help or assistance concerning the subject of the contact. If the Client declines Kate's offer of help or assistance, Kate will not provide it; the scope of Kate services provided to the Client is therefore always subject to the Client's decision. Kate actively contacts the Client through a notification - a push notification - whenever relevant in view of the Client's personal situation and the analysis of their needs. For proactive Kate to function properly, notifications/alerts must therefore be enabled on the mobile device. With this setting, Kate may also contact the Client when the Client is not currently using the SmartBanking App.

12. Processing of the Client's personal data when using Kate:

When Kate is used, the Client's personal data are processed appropriately and proportionately to prepare a response to the Client's request. Use of the proactive version involves a deeper analysis of the Client's personal data and behaviour. If the Client does not submit any request through Kate, ČSOB does not process the Client's personal data. Kate also does not process the Client's personal data falling within special categories of personal data under the applicable personal data protection legislation.

4. ELECTRONIC BANKING SERVICES SUPPORT

Helpline	+421 2 5966 8844 from within or outside the Slovak Republic
Operating hours	24 hours a day, 7 days a week
Website	www.csob.sk/kontakty
Standard activities performed by the Helpline	• Information on the entry / modification / cancellation of Client instructions • Blocking/unblocking Security Features and Security Instruments • Receiving and resolving a problem of the Client and communicating the outcome • Communication with Clients by email and via the ČSOB SmartBanking App • App deactivation

Capitalised terms in this document have the meanings given in the Terms and Conditions for the Provision of ČSOB Electronic Banking Services and the Terms and Conditions for the Provision of ČSOB Electronic Banking Services for Entrepreneurs, unless this document provides otherwise.

Attachments:

1. Overview of Functionalities, Rights Profiles, and Signature Rules in the ČSOB BusinessBanking App