

BUSINESS 24 User Manual

A modern form of Internetbanking available non-stop

BUSINESS 24 service

at www.business24.cz

BUSINESS 24 Mobile Bank

for iPhone or Android users

For service telephone support

In the Czech Republic – Support for commercial clients: 956 777 888

The following telephone number is available for calls from abroad: +420 956 777 888

TABLE OF CONTENTS

1. Characteristics of the services	3
1.1. Principles and rules governing the usage of the service	3
1.2. Technical preconditions for the usage of the service	4
1.2.1. BUSINESS 24	4
1.2.2. Mobile Bank	5
2. Service security	5
2.1. The BUSINESS 24/BUSINESS 24 – LIGHT service is secured with direct banking security features:	5
2.2. The BUSINESS 24 Mobile Bank service is secured with security features:	5
3. Logging into the service and its set-up	6
3.1. Logging into the BUSINESS 24/BUSINESS 24 – LIGHT services.....	6
3.1.1. Login via Client Certificate	6
3.1.2. Login via client number and password or login SMS message	7
3.2. Logging into the BUSINESS 24 Mobile Bank	7
3.3. Service Settings	7
3.3.1. Adding and removing of accounts and cards.....	7
4. Limits used in BUSINESS 24	8
4.1. Account limit.....	8
4.2. Co-authorisation limit	9
4.3. Mobile Bank limit	9
5. Account management by several users	9
5.1. Authorised persons	10
5.2. Joint holder rights.....	11
6. Blocking/unblocking of user access	12
7. Order processing and cancellation	13
8. Main functionalities of BUSINESS 24	14
9. Information on the functionalities of the BUSINESS 24 service	15
10. List of terms and abbreviations	15
11. Annex 1	19
12. Annex 2	19
13. Annex 3	20
14. Annex 4	22
15. Annex 5	24

1. Characteristics of the services

BUSINESS 24

BUSINESS 24 is an electronic and telephone banking which is provided to commercial and corporate clients of Česká spořitelna, a.s. (hereinafter referred to as the "Bank") on the basis of a contract associated with the client's main/primary account (hereinafter referred to as the "account owner"), which is specified in the Contract and which may be changed at a business point, if necessary.

Accounts may be serviced via the BUSINESS 24 Internetbanking by persons who have been set up as persons authorised to do so; so called users (hereinafter referred to as the "user"). Access to the service by phone allows not only for user support, but also for the execution of selected administrative operations, filing of complaints and obtaining of information on executed and non-executed transactions.

BUSINESS 24 – LIGHT

The BUSINESS 24 – LIGHT service is a simplified version of BUSINESS 24 and is intended solely for corporate clients who may use it to obtain information on passive transactions on accounts which have been assigned to the service. The list of transactions is specified under [Annex 1](#).

The BUSINESS 24 – LIGHT service is governed by the same rules, principles and technical preconditions as the BUSINESS 24 service.

Should the account owner be interested in using the BUSINESS 24 service in full scope, he/she can apply for the transfer of the BUSINESS 24 – LIGHT service to BUSINESS 24 service at a business point.

BUSINESS 24 Mobile Bank

Mobile Bank is a service which allows for a secure and comfortable management of your finances at any time and any place directly from your mobile phone or tablet with the [iOS](#) or [Android](#) operating system (iPhone, iPad, iPod touch). It is available free of charge in the Czech or English language.

The types of the serviced accounts, main features and conditions are specified under [Annex 2](#).

1.1. Principles and rules governing the usage of the service

Users log into the BUSINESS 24 service at www.business24.cz.

The service allows for an easy management of client accounts via a straightforward menu and intuitive work in the application.

A detailed description of how to use the internet banking is provided in the BUSINESS 24 Help document. It is available from the login page under the "Was your login unsuccessful?" link.

Due to higher security, all active operations require confirmation by Client Certificate.

Moreover, the service enables to avail of the telephone banker support.

Support for the BUSINESS 24 service is available on business days from 7:00 a.m. to 6:00 p.m. at 956 777 888 (+420 956 777 888 when calling from abroad). Following the welcome message and language selection (CZ, EN) the client is connected to a telephone banker.

For the provision of information about the settings of the service, accounts and transactions, the client has to be authenticated by the security details provided thereto in a sealed envelope upon opening of the service. **Contacts:**

- from a fixed line: 956 777 888
- from mobile phones: O2 726 118 128
T-Mobile 605 661 128
Vodafone 776 991 128
- from abroad: +420 956 777 888
- at e-mail address: BUSINESS 24@csas.cz

(here you can obtain replies to your questions or send you ideas concerning the BUSINESS 24 service)

The price for the administration of the BUSINESS 24 service (a monthly price for service maintenance, price for the Client Certificate, chip card and reader, for repeated sending of security details, etc.) is charged to the main/primary account of the client which is specified in the Contract on the BUSINESS 24 service. The price is charged according to a valid Pricelist.

1.2. Technical preconditions for the usage of the service

1.2.1. BUSINESS 24

The recommended equipment for the proper functionality of the **BUSINESS 24** service is a personal computer with and installed operating system and an internet browser

Supported operating system versions	Supported internet browser versions
Microsoft Windows 8.1 Microsoft Windows 10	Microsoft Edge Mozilla Firefox (latest 3 versions) *) Google Chrome (latest 3 versions) *)
OS X 10.11 (El Capitan) Mac OS 10.12 (Sierra)	Safari 6 and higher Mozilla Firefox (latest 3 versions) *) Google Chrome (latest 3 versions) *)
Linux distribution CentOS version 6 and higher Linux distribution Ubuntu version 12.10 and higher	Mozilla Firefox (latest 3 versions) *) Google Chrome (latest 3 versions) *)

*) The latest browser versions are tested for the period of three months following their release and the application is being adapted to them so that complete functionality and proper display were safeguarded.

The BUSINESS 24 Internetbanking application requires a browser capable of processing websites according to the following standards:

- HTML 4.01 (as per recommendation W3C HTML 4.01 Specification and the ISO/IEC 15445:2000 standard);
- JavaScript (as per recommendation ECMAscript-262, rev.3);
- CSS 3 (as per recommendation W3C CSS3 Values and Units);
- HTTP 1.1 (as per recommendation IETF RFC2616);
- TLS 1.1

The storage of cookies must be permitted.

We handle personal data exclusively in accordance with applicable legislation. Please read the Principles of Personal Data Processing at Česká spořitelna to find out what principles we follow when ensuring the confidentiality and security of your personal data. The principles of personal data processing can be found at <https://www.csas.cz/cs/zasady-zpracovani-osobnich-udaju>.

Usage of the cookie files and similar technologies

On its website and in Internetbanking, Česká spořitelna uses small text files – cookies, which are sent to your browser. Thanks to this, the visit to our site is easier and the content more relevant. These files are used particularly to save your settings, for example your preferred language, the monitoring of usage data and selection of proper communication. The principles of personal data protection are always strictly observed.

Please note that the Internet Explorer (IE) 11 desktop application will end support for operating systems as of June 15, 2022. Customers can upgrade to Microsoft Edge with IE mode. IE mode allows backward compatibility and will be supported until at least 2029. For users who would like to use BUSINESS 24 in IE 11 some features may not work properly or will not be available at all.

What specific cookies are used?

- Personalisation - to define the preferred language and login method;
- Authentication – to authenticate the user for the purposes of security;
- Technical – to safeguard communication with the Bank's systems and to ensure the minimum parameters necessary for the operation of the application;
- Communication – to display multimedia content;
- Statistical – to determine the usage data for individual sections of the application.

Other operating systems and internet browsers may not be fully compatible with the BUSINESS 24 service, and therefore the Bank cannot guarantee that the service will be displayed properly and that all of the offered functions will run flawlessly.

1.2.2. Mobile Bank

At present, the application is supported for tablets or smartphones with the iOS operating system and for the Android operating system.

2. Service security

2.1. The BUSINESS 24/BUSINESS 24 – LIGHT service is secured with direct banking security features:

- The client number which forms part of the User set-up protocol;
- Telebanking password which is included in the security mail consignment;
- Security ID which forms part of the security mail consignment;
- Client Certificate (so called electronic signature);
- System certificate (only for the Databanking service);
- Login SMS message

The description of individual security features is provided in [Annex 4](#)

The following phone numbers are available to clients who wish to report any loss or theft of security data:

- 956 777 888 (on working days from 7:00 a.m. to 6:00 p.m.);
- 800 207 207;
- or 956 777 956.

Other features enhancing the security of the service include the following options:

- On the part of the client, the option to:
 - Change access passwords;
 - Change limit amounts;
 - Define access to the contract only using the Client Certificate for individual joint holders;
- On the part of the Bank, the option to:
 - Record and archive any communication maintained via BUSINESS 24 (in the banking systems);
 - Actively use and combine the security features (changes of password, limits, or the use of Client Certificate where applicable),
 - Log out the client automatically if the time of validity of the site expires;
 - Take out and re-insert the chip card into the chip-card reader when logging into the BUSINESS 24 application through Client Certificate or after a longer inactivity in the BUSINESS 24 application.

The security data are provided by the Bank to the client automatically upon opening the BUSINESS 24 service.

The Client Certificate is provided by the Bank upon the user's requirement at a business point.

The user may apply for the **Client Certificate** for BUSINESS 24 either at the time of contracting the service or any time later, but only via a business point. The validity of the Client Certificate is one year. The user can renew the Client Certificate via the BUSINESS 24 Internetbanking service.

The implementing directive for the usage of electronic certificates within the scope of direct banking services is provided in [Annex 3](#).

2.2. The BUSINESS 24 Mobile Bank service is secured with security features:

- Usage of multilayer security – the first-time login is conducted with a combination of Internetbanking security features and a password for the Mobile Bank;
- Software certificate usage;
- Automatic logout upon inactivity;
- The possibility to logout with a shake;
- Detection of a non-standard set-up of the operating system;
- Automatic blocking upon repeatedly incorrect logins (3 attempts).

Important notices

Any disclosure of the aforementioned security features may jeopardise the accounts operated via BUSINESS 24. It is advisable not to disclose the special registered-mail envelope or the individual security features to any one person and to protect them from loss or theft.

Never access the BUSINESS 24 service from unknown computers in internet cafés or other public places.

On its part, the Bank is obliged to execute any measures to safeguard the security of any and all systems and processes which provide for the operation of direct banking services to make sure it is not possible for unauthorised persons to obtain the client security data from the Bank's systems and records. The client is informed about the undertaken security measures. The Bank, however, is not responsible for the disclosure of the security data if the disclosure occurs on the part of the client or persons appointed thereby for the use of the BUSINESS 24 service.

Files in the PDF format are secured with a digital signature when sent by e-mail; the digital signature allows the client to check whether the e-mail was generated in the Bank and has not been altered by any third party.

3. Logging into the service and its set-up

3.1. Logging into the BUSINESS 24/BUSINESS 24 – LIGHT services

The user is always identified and authenticated when logging into the service. The BUSINESS 24 service requires a mandatory login via Client Certificate for all active financial transactions and administrative operations. Passive transactions (checking the balance, transaction history, etc.) and the entry of transactions for co-authorisation may be executed even after login via the client number and password, or the login SMS, where applicable.

The security set-up may be also changed to require the user to log in via Client Certificate at each time, i.e. not only when conducting active financial transactions and administrative operations, but also upon each login to the application. This set-up, however, excludes the possibility of any later login via the mobile application BUSINESS 24 Mobile Bank.

3.1.1. Login via Client Certificate

First-time login

Before first-time login via Client Certificate, it is necessary to install the essential components. The installation package is available from the csas.cz website, under the Downloads section (<https://www.csas.cz/PKIInstall>).

Upon the first-time login to the BUSINESS 24 service it is possible to activate the Client Certificate even if the client has not previously logged in using the client number and Telebanking password. It is possible to do so on the login screen of the BUSINESS 24 service through the "Certificate administrator – entry into application" option.

In this case the client only inserts the chip card into the reader connected to the computer and selects the appropriate option from the login screen. Thereafter the client will be prompted to enter the PIN for the respective chip card. This PIN is provided in the envelope together with the chip card, which the client has received after the conclusion of the Higher-type security protocol at a business point. The security ID is provided in a special registered mail consignment which the client receives by post for personal delivery after having contracted the BUSINESS 24 service.

Second and subsequent logins

To log in, the client uses the activated Client Certificate. The user inserts the chip card into the reader connected to the computer. Once the client selects the appropriate option on the login screen, he/she will be prompted to enter the PIN code for the chip card.

More details on the login via Client Certificate are provided in the Client Certificate Manual.

An authorized person always logs in to the service first, who assigns accounts and cards to the service, and also, if more users are to have access to the service, Annex 5 sets the disposition rights for other users.

3.1.2. Login via client number and password or login SMS message

First-time login

When the BUSINESS 24 application login page comes up from the internet address www.business24.cz, the client is invited to enter the client number and Telebanking password (the "Client Number" and "Password" fields). Once the data are submitted, the system is able to recognise that a first-time login is concerned and the client is invited to enter four randomly required characters from the security ID and to select his/her password for Internetbanking.

The security ID and Telebanking password are specified in a special registered-mail consignment which the client receives by post for personal delivery after having contracted the BUSINESS 24 service. The client number forms part of the User set-up protocol.

Second and subsequent logins

To log in, it is necessary to use the client number and current password for BUSINESS 24 Internetbanking, and the login SMS code.

3.2. Logging into the BUSINESS 24 Mobile Bank

First-time login

First-time login via the mobile phone or tablet is performed using the client number, one-time code and password for the Mobile Bank. The one-time code may be obtained by the client from Internetbanking, where the client number will be also displayed. The password for the Mobile Bank is generated in Internetbanking, once the user logs in via the Client Certificate, and it is necessary for the activation and subsequent logins to the BUSINESS 24 Mobile Bank application. Concurrently, when activating the BUSINESS 24 Mobile Bank, the client selects a password for the repository which serves for the confirmation of active operations.

Second and subsequent logins

To log in, the client has to use the current password for BUSINESS 24 Mobile Bank.

3.3. Service Settings

The first one to log into the service is always the authorised person, who adds accounts and cards to the service and, furthermore, if more users are to have access to the service, he/she sets up joint holder rights for the users (chapter 5.2).

3.3.1. Adding and removing of accounts and cards

The BUSINESS 24 service may be used for the management of accounts and payment cards which are assigned to it either automatically or manually (by the authorised person).

Removal of accounts and payment cards from the BUSINESS 24 service is sometimes executed also automatically, but in most cases they are removed by the authorised person.

Adding accounts and cards:

- After the first-time login, the BUSINESS 24 service will be **automatically** activated for the main/**primary account** specified in the contract for the authorised person and the **card account**, if it has been set up for the same account owner as the main/primary account. Concurrently with these accounts, all **payment cards** issued for these accounts will be automatically added to the BUSINESS 24 service.
- **Other current, savings or card accounts are added** to the service by the authorised person via the BUSINESS 24 service. Only those accounts which are identified by the contract as the client's accounts may be added. Together with the current or card account, payment cards issued for the account will be added as well.
- **A payment card holder** who is not at the same time the authorised person may add only **his/her own card**. This card will be added to this user automatically only upon first-time login to the BUSINESS 24 service.
- For corporate clients, newly provided **loans, credit lines, bank guarantees** and newly opened **deposits accounts** are **automatically** added to the BUSINESS 24 service.

- All joint holders with passive rights in respect of at least one current account of the client added to the BUSINESS 24 service will be automatically assigned with passive rights in respect of deposit accounts added in this manner.
- The rights to view loans of corporate clients are set up by the authorised person via the set-up of the activity “Loans – exchange of documentation” and thereafter the set-up of passive rights for individual loan accounts both for the authorised person itself and for other joint holders. Loans of business clients are assigned under the service by the authorised person by means of BUSINESS 24 service; thereafter, the authorised person will set up rights in respect thereof for other joint holders.

Removing an account or card:

- The main/primary account cannot be removed.
- For corporate clients, closed deposit accounts, closed loans, credit lines and cancelled bank guarantees will be **automatically** removed. It will not be possible to manually remove or add loans, credit lines, and bank guarantees from/to the BUSINESS 24 service. Nevertheless, the client will be able to manually remove or add joint-holder rights to individual joint holders.
- For business clients, only closed loans will be removed automatically.
- A payment card may be removed by its holder or by the authorised person. Upon card removal by its holder, the authorised person will still be able to display the card. If the card is removed by the authorised person, the card holder will still be able to display the card.
- A removal of a current or card account will result also in the removal of payment cards issued for the account.
- Card accounts may be removed by the authorised person. Only if the card account is cancelled, it will be removed automatically together with all cards issued for it.

4. Limits used in BUSINESS 24

Account limit	100,000,000 CZK	With the possibility of increase to 10,000,000,000 CZK, or reduction, via B24. The limit adjustment (increase/reduction) may be performed solely by the authorised person with the use of a Client Certificate.
Co-authorisation limit	not set up automatically	The co-authorisation limit is set up and may be changed only via B24 by the authorised person
Mobile Bank limit	10,000,000 CZK	May not be changed

4.1. Account limit

This is the maximum daily amount of active transactions which may be entered and submitted for processing from the given account within the scope of the BUSINESS 24 service on a business day.

It is an optional limit which may not be exceeded on the given day, not even if you the Client Certificate is used.

The limit is not affected where active transactions conducted between the accounts of a single owner assigned under BUSINESS 24, which are also assigned to the user who performs the transaction, are concerned. (For example, if two current accounts are assigned under one contract the limits are not affected by transfers of money between those accounts).

In respect of foreign-currency accounts, the limits are set as equivalents of the amounts in CZK as per the current FX rate of the account currency at the time of posting the required transaction. Limits are converted using the non-cash/buy rate.

The limits are zeroised every day at 11:00 p.m.

Detailed description of setting up the account limit

1. In the "SETTINGS" tab, select the "Account settings" option from the left menu and then the "Set up account limit" option.
2. In the "List of account limits" screen select the account for which limits are to be set up.
3. The "Change account limit – step 1 of 2" screen will come up. If you wish to set up the limit for the maximum amount of transactions performed per day for the account, enter the required amount in the "New limit" field.
4. If you wish the confirmation of transaction acceptance to be delivered to you, complete the "By e-mail" field and select "Continue".
5. The "Change account limit – step 2 of 2" screen will come up. Check the entered details here and select "Send" + enter PIN to confirm.
6. The "Transaction acceptance confirmation" screen will be displayed.

4.2. Co-authorisation limit

This is the maximum total daily amount of active transactions which may be executed by users on the given account without the necessity of being authorised by another account joint-holder. Above-limit transactions have to be authorised (co-authorised) by other account joint holders. The co-authorisation limit is set up and may be changed only through the BUSINESS 24 service by the authorised person, for each account separately. It is an optional component of money transfers security and it cannot be exceeded, not even if the Client Certificate is used.

The limits are zeroised every day at 11:00 p.m.

Detailed description of setting up co-authorisations

1. In the "SETTINGS" tab, select the "User settings" option from the left menu and then the "Set up co-authorisation" option.
2. In the "List of co-authorisation settings" screen, select the account in respect of which co-authorisation is to be set up.
3. The "Change co-authorisation set-up – step 1 of 2" screen will come up. If co-authorisation is to be set up, select "Yes", enter the amount from which transactions are to be approved by several joint holders in the "Co-authorisation limit" field, (if each transaction is to be co-authorised by several joint holders, enter 0), and enter the number of joint holders who have to co-authorise a transaction for it to be processed in the "Number of co-authorisations" field.
4. If you wish the confirmation of transaction acceptance to be delivered to you, complete the "By e-mail" field and select the "Continue" option.
5. In the "Change co-authorisation set-up – step 2 of 2" screen, check the entered details and select "Send" + enter PIN for confirmation.
6. On the next "Transaction acceptance confirmation" screen, select the "Continue to set up co-authorisation" option and repeat steps 2-5 for all accounts in respect of which co-authorisation is to be set up.

These limits are not applicable to transactions between accounts belonging to a single client and forming part of a single "Contract on the Provision of the BUSINESS 24 Service", if, in respect of the account, you have set up co-authorisation for transfers between your own accounts.

4.3. Mobile Bank limit

It has been set up at the amount of ten million CZK per day and user. It is reflected at the moment the transaction leaves the transaction repository.

5. Account management by several users

The BUSINESS 24 service allows for the assigned bank accounts and selected functionalities without the account context to be administered by several users. For each of them, specific rights for the given account management are set up by the authorised person (e.g. only viewing of transactions). For the user to be able to administer accounts via BUSINESS 24, he/she has to be included in the specimen signatures for the account. In respect of selected functionalities without the client context, joint holders are assigned by the decision of the authorised person.

Sponsor

A specific term of the direct banking services is a sponsor. A sponsor is assigned to a user automatically upon the user's set-up, and it is the client on the initiative of which the user is being set up. The prices for standard-type security (application for the sending of a new mailer, login SMS), and higher-type security (Client Certificate renewal, ordering of a new chip card) are paid from the primary account of the sponsor.

A change or removal of a sponsor may be performed only by the authorised person via the Telebanking service or in the BUSINESS 24 application. This **cannot be done** via a branch.

Description of setting up the sponsoring

1. In the "Settings" tab, select the "User set-up" option from the left menu and thereafter the "Sponsored person administration".
2. On the "List of sponsored users" screen, select the name of the joint holder for whom you wish to set up the sponsor.
3. The "Change of user sponsoring – step 1 of 2" screen will come up. Here, set up the option "Yes" for Standard or Higher Security.
4. If you wish to have the confirmation of the transaction receipt to be delivered to you, it is necessary to complete the "By e-mail" field and to select the "Continue" option.
5. The "Change of user sponsoring – step 2 of 2" screen will be displayed. Here, check the entered data and press "Send" + enter PIN if you wish to confirm.
6. On the next screen, "Transaction receipt confirmation", select the "Continue to administer sponsored users" option and repeat steps 2-5 for all joint holders in respect of which sponsoring is to be set up.

The change and/or removal of a sponsor may be performed only by the authorised person via the Telebanking or Internetbanking service. This **cannot be done** via a branch.

5.1. Authorised persons

An authorised person is a user selected by the client and specified thereby in the contract. Each authorised person specified in the contract is automatically assigned the right to set up the following administrative operations:

Administrative operations	in respect of the account	<ul style="list-style-type: none">• add/remove an account enter• an account name• set up an account limit
	in respect of the user	<ul style="list-style-type: none">• add/remove joint holders set-up access to contract• set-up co-authorisation parameters• perform sponsored person administration
	in respect of the services	<ul style="list-style-type: none">• apply for the opening/change of a account• set-up the sending of credit advices• set-up data statements• activate/deactivate/change statement series (for business clients)• apply for cheque form issuance• apply for debit card issuance• apply for the provision of a bank reference on own person if the B24 service allows it• submit templates• display documents sent via BUSINESS 24• apply for loan drawdown• apply for the set-up of a balance regulation standing order ask a report for the auditor, a bank reference or other personal report
	in respect of the client	<ul style="list-style-type: none">• send templates / requests and be informed about the status of their processing and confirm the information needed to identify the client and the persons acting on behalf of the client• block the contract• unblock the contract

Active operations	in respect of the client	<ul style="list-style-type: none"> • electronic pledge of receivables • bank guarantees • documentary deals • approval for third party providers (TPP) • exchange of loan documentation • confirmation of treasury deals (automatically for authorised persons for the contract on the provision of the B24 service for a client with a contract with the Dealing unit) • account mode change • loans <p>The aforementioned rights are assigned by the client to specific authorised persons directly in the contract. The set-up of joint-holder rights for these activities, except for Account mode change and approval for third party providers, is not preconditioned by the inclusion of the user in the specimen signature. The right for Account mode change cannot be delegated by the authorised person.</p>
--------------------------	--------------------------	---

There may be an unlimited number of **authorised persons** for the contract. In case of **natural persons**, the client who concludes the contract is automatically assigned as the authorised person without the option to cancel this set-up. In case of **legal persons** it is entirely upon the discretion of the authorised representative to specify the authorised person. Authorised persons may act independently or jointly. In case of joint acting, it is necessary to specify the number of jointly acting persons. Unless the operation, in case of joint acting of authorised persons, is authorised by the necessary number of authorised persons within thirty days of its generation, it will be invalidated.

The authorised person specified in the specimen signature for accounts assigned under the BUSINESS 24 service, is automatically granted all [rights](#) for these accounts in respect of money management as the account owner and may perform all administrative as well as active operations, incl. those that the joint holder may not perform, i.e.

- all options for FX operations;
- set-up/change/cancellation of a balance adjustment standing order;
- set-up/change/cancellation of a deposit account;
- list of conditions for compliance with loan relationships.

5.2. Joint holder rights

The following rights (or a combination thereof) may be set up for **users – joint holders**:

- **Active transactions (A) right** – the joint holder may enter transactions associated with transfers of money from the given account or send payment instructions files for collection accounts. It can provide information on products and carry out active operations for individual activities according to authorization. The specific activities and scope of authorization are defined in the Agreement.
- **Passive transactions (P) right** – the joint holder has access to information associated with the given account (e.g. the account balance).
- **Joint co-authorisation of transactions (S) right** – the joint holder may co-authorise (authorise) transactions which have exceeded the co-authorisation limit (chapter 4.2 *Co-authorisation limit* refers) and which are stored in the repository of transactions awaiting co-authorisation. One co-authorisation of this joint holder increases the current number of co-authorisations by one.
- **Exclusive co-authorisation of transactions (E) right** - the joint holder may co-authorise (authorise) transactions which have exceeded the co-authorisation limit (chapter 4.2 *Co-authorisation limit* refers) and which are stored in the repository of transactions awaiting co-authorisation; a single co-authorisation of this joint holder substitutes all missing co-authorisations and the transaction is subsequently sent for processing.
- **Entry of transactions to the repository of transactions awaiting co-authorisation (T) right** – the joint holder may only enter transactions which are sent to the repository of transactions awaiting co-authorisation, where they await authorisation by a joint holder E or by the necessary number of joint holders S.
- **Payment card administration right (K)** – the joint holder may perform card operations (for active transactions, he/she has to have also the A right).

The individual rights may be combined. Their specification is provided in [Annex 5 List of BUSINESS 24 operations](#). For better orientation, the individual types of joint holders are identified with the letters A, P, S, E, T, and K.

A single user may be the authorised person and a joint holder at the same time.

6. Blocking/unblocking of user access

<p>Upon request via the telephone banker</p>	<p>Following the specification of the name, surname and birth number</p> <p>Consequence: The user's access to the BUSINESS 24 service, i.e. IB and Mobile Bank, access to the third party applications is blocked.</p> <p>Unblocking: If the user blocks his/her access to the entire BUSINESS 24 service, it is possible to unblock him/her by applying for the generation of new security data which may be collected from a business point or sent to a specified mailing address for the BUSINESS 24 service.</p>
<p>By revoking the validity of the Client Certificate</p>	<p>Following login to the BUSINESS 24 service / via a business point/ via the help line at 956 777 888 (on business days from 7:00 a.m. – 6:00 p.m.)</p> <p>Consequence: Access to the BUSINESS 24 service and access to the third party applications through the Client Certificate will be blocked.</p> <p>Unblocking: Not possible; if the user wishes to continue using the Client Certificate, he/she has to apply for the issue of a new one at a business point.</p>
<p>Automatically after the entry of an incorrect detail</p>	<p>The combination of the client number and password for Telebanking or Internetbanking entered incorrectly three times in a row</p> <p>Consequence: Access to the BUSINESS 24 service will be blocked. If the client is, at the same time, also a user of the SERVIS 24 services, access to the SERVIS 24 services and access to the third party applications will be blocked as well.</p> <p>Unblocking: May be performed by the client via telephone banker or via the BUSINESS 24 service, if logged in by means of a Client Certificate (unblocking via the Change of password for Internetbanking option). If he/she is, at the same time, also a user of the SERVIS 24 services, access to the SERVIS 24 services will be unblocked as well.</p> <p>Consequence: Access to the BUSINESS 24 service will be blocked. If the client is, at the same time, also a user of the SERVIS 24 services, access to the SERVIS 24 services will be blocked as well.</p> <p>Unblocking: May be performed by the client via telephone banker or via the BUSINESS 24 service, if logged in by means of a Client Certificate (unblocking via the Change of password for Internetbanking option). If he/she is, at the same time, also a user of the SERVIS 24 services, access to the SERVIS 24 services and access to the third party applications will be unblocked as well.</p> <p>Password for Mobile Bank entered incorrectly three times in a row</p> <p>Consequence: Mobile Bank will be blocked.</p>
	<p>Unblocking: Not possible; it is necessary to perform a new registration via B24 Internetbanking.</p> <p>Incorrect PIN for chip card where the Client Certificate is stored has been entered incorrectly three times in a row</p> <p>Consequence: The chip card will be blocked.</p> <p>Unblocking: May be done by the entry of the PUK.</p> <p>An incorrect PUK for the chip card where the Client Certificate is stored has been entered seven times in a row</p> <p>Consequence: Access will be blocked.</p>

Unblocking: Not possible; it is necessary to apply for a new chip card and a new Client Certificate.

Security ID entered incorrectly three times in a row

Consequence: The user cannot execute tasks requiring the entry of the security ID such as firsttime login).

Unblocking: The security ID cannot be unblocked; the user has to apply for a new one via telephone banker or a business point.

Blocking of a client (contract)

The user or authorised person may apply for the blocking of a client via telephone support, the BUSINESS 24 service or through a business point. **Unblocking of a client (contract)**

A client may be unblocked only by the authorised person of the concerned client, via telephone support, the BUSINESS 24 service or through a business point.

7. Order processing and cancellation

Payments are processed within timelines and according to the priorities specified in the Information on Payment Services (commercial and corporate clients), which is available from the Bank's website (www.csas.cz, section Downloads/Payments/Information for clients/Information on payment services for commercial and corporate clients, or from the Erste Corporate Banking website under the Important Documents section).

General information

Orders/payments entered on weekends or holidays or on a day before a weekend or holiday after 10:00 p.m. (corporate clients) or 11:00 p.m. (business clients) will be forwarded for inter-banking clearance on the first business day following the entry date.

Orders/payments entered one day prior to a weekend or holiday before 10:00 p.m. (corporate clients) or 11:00 p.m. (business clients) with a due date of D+1 and D+2 will be executed on the first and second business day following the last non-business day, without being changed to another type of order.

In case of co-authorisation of payment transactions (except for standing payment orders, standing collection orders, direct debits, and deposit accounts) within the scope of the BUSINESS 24 service, the following shall apply: if the transaction due date expires while waiting for a signature, it is possible to update this date within thirty days of the due date by adding the remaining signature and to execute the transaction with the current due date. After the expiry of thirty days, the order is invalidated and needs to be entered again. The following applies to standing payment orders, standing collection orders, direct debits, and deposit accounts: if the transaction due date expires while waiting for a signature, the transaction is invalidated and requires re-entry.

In respect of orders entered via an order batch import with a possible retrospective due date in the batch, the order due date will be automatically updated upon the batch import to the current business day.

In case of payments (applicable to domestic payments, foreign-currency payments within the Bank, domestic payment import, and multiple domestic payments) with a due date entered for a non-business day, the due date will be changed to the next business day and the user will be informed of this change by means of a message reading "The due date has been amended to the following business day".

Furthermore, the BUSINESS 24 IB service offers a list of transaction statuses. Transactions are classified into five categories: non-executed transactions, executed and pending transactions, transactions waiting for further coauthorisation in the repository, and transactions for deletion in the repository. For corporate clients, the reason for nonexecution of the transaction is displayed for non-executed or pending transactions.

Clients may post-hoc cancel those transactions in the domestic and foreign payment system which have not been settled to date. Payments entered through third parties cannot be cancelled. A payment entered via the BUSINESS 24 service with a current due date cannot be cancelled.

SEPA: Within the scope of SEPA, it is possible to execute credit transfers and collections. The realisation is preconditioned by the counter-party bank offering the conduct of the SEPA transfer/collection service. In case of

a SEPA transfer/collection, it is possible to specify a Payment reference – as agreed with the payee. If the client (payer) does not specify any payment reference, the Bank will complete the payment reference with the value NOTPROVIDED.

SEPA collection modes: Collections of the CORE type may be conducted in respect of the payer accounts in two modes – in the Single direct debit mode, or in the General direct debit mode. The client will select one of the options which will then be applicable to all SEPA collections conducted in respect of the account.

The authorised person has to have a special authority specified in the contract. This authority cannot be delegated.

SEPA error statuses: Files in the XML format, which contain information on non-executed SEPA payments/collections. The format is consistent with the PAIN.002.001.03 version approved by the European Payments Council.

In case of any doubt regarding the posting of an entered order, the client is advised to contact the telephone support of the BUSINESS 24 service.

For all transactions, the transaction reference number will be automatically displayed in the BUSINESS 24 service for clients. This number may be used for the purposes of payment identification (e.g. in a statement) or it may facilitate handling of a potential complaint regarding a transaction entered via the BUSINESS 24 service. The BUSINESS 24 IB service allows, *inter alia*, for the sending of e-mail confirmation of a received transaction, transaction history, account detail, etc. These documents are of informative nature only. The transfer of data is conducted in a standard manner, without special security features, and for this reason the Bank cannot guarantee that it will not be seized by a third party on the way between the Bank and the client.

BUSINESS 24, moreover, offers the function of control of unintentional repetition of a domestic transaction entry. When executing a domestic payment, multiple domestic payment, or import of orders, the BUSINESS 24 service checks transactions previously entered on the same day and if it identifies an identical transaction entered by any of the joint holders in respect of the concerned account, it will display a warning. The user then may check the previously entered transactions and cancel or execute the transaction in question.

8. Main functionalities of BUSINESS 24

The **PAYMENTS** option serves for the purposes of entry or import of payment orders (domestic, multiple, foreigncurrency, within the Bank, SEPA, foreign and batch), standing orders and collections, and for the administration of payee templates. SEPA Credit Transfers and SEPA Direct Debits are executed in the full XML format prescribed by the European Payments Council. The timelines specified on the Bank's website at www.csas.cz.¹ are applicable to the processing and cancellations of orders; information about the possibility to cancel payments is provided in the annex.

The **ACCOUNTS** option allows for the display of a list of current, savings, and deposit accounts and their balances, including the export of statements, and the display of received advices. The transaction history with the details of individual transactions may be displayed. It is possible to go from the menu into the PAYMENTS option easily. Confirmation of the existence of the account, the balance of the account and the payment made, provide the Bank with information about a specific product. It is also possible to request some products and request a report for the auditor, a bank reference or another report on one's own person.

The **CARDS** option servers for the purposes of card and card account administration, including the display of their transaction history and card operation details, card blocking and unblocking, and the ordering of new cards.

The **FINANCING** option allows for the import and submission of a list of receivables to be pledged (and to electronically conclude a collateral contract), applications for the issue of a debit card and cheque forms. The users can display a list of bank lines, products within the lines, and the utilisation of limits as well as sublimits, including their details. It is possible to display the current amount of the loan burden and the conditions of loan

¹ In case of co-authorisation of single payment transactions, the following applies: if the due date has already expired, the transaction will be invalidated after thirty days of waiting, and it will be necessary to enter it again. In respect of standing orders and collections, the transaction becomes invalid as soon as the due date expires while the transaction still awaits co-authorisation.

In case of a batch import, for payments the due date of which has already expired, the due dates are automatically amended to the current business day. Likewise, for payments entered with a due date on a non-business date, the due dates are automatically amended to the next business day.

relationships requiring performance in the current period. The menu, moreover, contains the option for the exchange of loan documentation between the client and the Bank, *including the possibility to send financial reports*.

The options for **BANK GUARANTEES and DOCUMENTARY DEALS** allow for working with issued and received bank guarantees, import and export letters of credit, and collections. The individual instruments (bank guarantees, letters of credit or collections) create so called business cases which associate individual transactions realised at the time prior to expiry of the concerned instrument. The menu also provides access to templates for individual instruments and the possibility to send an application for a consultation on a business case to a specialist in the Bank, rather than the order.

The **FX OPERATIONS** option allows the client to obtain individual foreign-exchange rates, to enter FX orders, and to perform operations on FX markets. The menu includes also access to the stored confirmations of individual deals and settlement approvals.

SETTINGS is an option intended particularly for the administration of users, accounts, and cards of the client, including the required statements. Each user administers his/her security data here. Here, the authorised person may add or remove access to activities and to set up mandatory user accesses to the BUSINESS 24 service via the Client Certificate, to carry out the administration of joint holder rights and authorisations for the service, to add or remove accounts, to set up names for accounts, to set up daily limits for payments outgoing from the account, to define rules for co-authorisation and set up the sending of data account statements.

The **CONTACTS** option allows, in addition to providing the contact for business points, also for a quick access to the menu for the exchange of documents with the Bank, to messages from the Bank, and to templates which may be downloaded.

9. Information on the functionalities of the BUSINESS 24 service

More details about the functionalities of the service are also available from the help provided on individual BUSINESS 24 screens, in video-manuals, and in the complete list of options for the system.

The list of **BUSINESS 24** operations is provided in [Annex 5](#).

The current form of the BUSINESS 24 service User Manual is available from the website of the Bank (www.csas.cz, in the Downloads section).

The bank is entitled to continuously amend and supplement this overview according to how the individual functionalities of the service are introduced, changed or terminated. The overview of operations in the BUSINESS 24 service is not a Notice in the sense of the GTC.

10. List of terms and abbreviations

- B24** – BUSINESS 24
- C** – Current (running) cycle (period) of deposit on a deposit account
- CM** – Foreign currency
- ČBA** – Czech Banking Association
- D** – Current business day (when the date of transaction entry is a business day) or the first business day after the entry of the transaction (when the transaction entry date is not a business day)
- DB** – BUSINESS 24 Databanking
- FOO** – Natural person - private individual
- FOP** – Natural person - entrepreneur
- HPÚ** – Multiple payment order
- IB** – Internetbanking
- IVR** – Automatic voice response service

- PI** – Direct debit order
- PÚ** – Payment order
- PSD 2** – Payment Service Directive II or Revised Directive on Payment Services, is a Directive of the European Parliament and of the Council on payment services in the internal market that comes into effect on 13 January 2018. The directive applies to each Member State of the EU in the form of a local law – the PSD 2 impacts thus apply to the entire European Union. In the Czech Republic, this Directive will be implemented by the new Act No. 370/2017 Coll., on Payment System
- DP** – Domestic payment
- HDP** – Multiple domestic payment
- RKC** – Regional Corporate Centre of ČS, a.s.
- MB** – Mobile Bank BUSINESS 24
- P** – A branch of ČS, a.s.
- PO** – Legal person
- PV** – Specimen signature
- SI** – Direct debit
- SEPA** – “Single Euro Payment Area” - SEPA is a uniform area for the execution of payments in EUR. SEPA includes countries of the European Economic Area (EU countries + Norway, Lichtenstein, Iceland) and Switzerland.
- TB** – Telephone banker
- TPI** – Standing direct debit order
- TPP** – Third Party Provider (within the PSD 2 a payment made through a third party)
- TPRZ** – Standing order for balance adjustment
- TPÚ** – Standing payment order
- VÚ** – Deposit account
- ÚÚ** – Loan account
- ZP** – Foreign payment

Administrative operation

An operation which results in a change to the set-up of the BUSINESS 24 service and user rights.

Accredited client

A client who has signed a contract or framework contract on dealing in financial markets with the Dealing unit and Master Agreement on the Conclusion of Foreign Exchange Spot Transactions and Depository Transactions and on the basis of the bank's business decision has been entered in the Bank system allowing to offer this client individual terms and conditions for dealing in financial markets. The client is informed of such decision of the Bank.

Active financial transaction

Transactions resulting in transfers of money.

Security ID

A number which is required particularly during first-time login to the BUSINESS 24 service and when unblocking a user. It is an eight-digit number provided in a security envelope.

Security data

Unique security features (client number, security ID, and Telebanking password), which are automatically allocated to each newly set-up user for the purposes of his/her unique identification for providing of access to direct banking services.

Security tools

Security features allocated by the Bank to the user for the purposes of his/her identification and serving for the provision of access to direct banking services for the user using enhanced security of communication with the Bank (e.g. the Client Certificate).

Security SMS

These include authorisation SMS messages (applies only to the services of SERVIS 24) and login SMS messages set up for the concerned user.

BUSINESS 24 Databanking

BUSINESS 24 Databanking is a data interface allowing the client who has activated the BUSINESS 24 service and who uses an accounting (ERP) or other system supporting Databanking, to avail of direct communication between this system and the Bank. Usage has to be permitted by the Bank.

Certification authority

An institution which issues, administers, and invalidates certificates.

Chip card

A secure repository of the certificate, an independent microprocessor on a card pursuant to ISO 7916.

Chip card reader

A hardware device necessary for the use of chip cards.

Electronic certificate

A data message issued to the client or authorised representative by the certification authority which serves for the purposes of electronic signature generation, particularly of the identification and verification of identity of the acting client or authorised representative.

Bank's financial group

Includes the Bank subsidiaries (members of the Česká spořitelna Financial Group), a company which has decisive asset share in the Bank (the Bank's parent company) and companies where the Bank's parent company has a more than a 25% asset share of the registered capital or a share in excess of 25% of voting rights. Current information on the members of the Bank's financial group is available from the Bank's website and at its business points.

Password for obtaining the certificate

A one-time password for the confirmation of the application for Client Certificate.

IVR

An automatic voice response service.

Client

An entity (natural person – private individual, natural person –entrepreneur, legal person) who concludes a contract with the Bank and who is the owner of the primary account to which the BUSINESS 24 IB service is linked.

Client Centre Prostějov

(Also KCP) A workplace of the Bank which provides, by means of phone, SMS messages or e-mail messages direct banking services (including their support) and information on products and services of the entire Bank's group.

Client Certificate

An electronic certificate issued to the user of the SERVIS 24 / BUSINESS 24 services. The user uses it for authentication into the SERVIS 24 Internetbanking / BUSINESS 24 Internetbanking services and for the authorisation of transactions entered via the SERVIS 24 / BUSINESS 24 services. It is a commercial personal certificate issued by I. Certifikační autorita.

Corporate client

A client whose contract on the maintenance of current account states that he/she is maintained in the Commercial Clients group.

Mailing address

The address to which correspondence associated with the BUSINESS 24 service is sent to the user.

Non-accredited client

A client who has not signed a contract or framework contract on dealing in financial markets with the Dealing unit and Master Agreement on the Conclusion of Foreign Exchange Spot Transactions and Depositary Transactions and has not been entered in the Bank system allowing to offer the client individual terms and conditions for dealing in financial markets.

Business day

Any day when the Bank and other banks in the Czech Republic are opened and when settlement of inter-bank deals is executed.

Business point

A branch, a regional corporate centre, or a headquarters unit (corporate clients, real estate and mortgages and municipal financing).

Passive transactions

Any information provided via the BUSINESS 24 service.

Payment card

A non-cash payment instrument. It includes all types of cards (debit card, credit card, additional credit card, charge card, prepaid card, deposit card).

Specimen signature

A power of attorney form, where the client specifies the authorised persons (the client may include himself/herself among the authorised persons), and the signature specimen of these persons or the scope of their authorisation.

Primary account

An account to which the contract on the provision of the BUSINESS 24 service is related.

Protocol (also Higher-type security protocol)

A document drafted if the client is interested in obtaining the Client Certificate (a security tool) which is considered to be an invitation to act addressed to the Bank for the purposes of concluding a higher-security contract (security tool).

Login SMS

A SMS message sent by the Bank to the client's mobile phone which contains a login SMS code.

Login SMS code

A numerical code contained in the Login SMS, which serves for the purposes of authorisation of security data when the client logs into the BUSINESS 24 Internetbanking service.

Co-authorisation

Additional confirmation of active transactions or administrative operations by other joint holders as per the set-up authorisations. A co-authorisation power may include a power of joint or separate co-authorisation. The signature of the joint holder authorised to perform separate co-authorisations replaces any number of joint holder authorisations with the power of joint co-authorisation.

Direct banking services

Services provided by the Bank to the client within the scope of which the client may execute active and passive transactions and administrative operations via telephone, internet or other remote communication means.

Contract

The contract on the provision of the BUSINESS 24 service.

Contract on higher-type security

An agreement between the user and the Bank on the basis of which the user is provided with a Client Certificate. It is a contract on the usage of a security tool as referred to by the respective item of the General Business Terms and Conditions of Česká spořitelna, a.s..

Sponsor

A client of the BUSINESS 24 service to whose primary account prices as per the Česká spořitelna, a.s., Pricelist are charged for bank deals associated with user administration. Currently, a sponsor for the Client Certificate (e.g. renewal) and for e.g. repeated sending of security data is set up. In respect of a newly set-up user, the client on whose initiative the user is being set up is automatically set up as the user's sponsor. This set-up may be changed by the authorised person.

Sponsored person

The user for whom the Bank charges the fees and prices associated with the set-up and administration of security tools according to the Pricelist of Česká spořitelna, a.s. for bank deals to the account whose owner has agreed to such arrangement via direct banking services.

Certificate administrator

Software, internet application allowing for the administration of the Client Certificate.

Telephone banker

An employee of Client Centre Prostějov, who provides the predefined scope of services of the Bank's Group to **both authenticated and non-authenticated users via phone.**

User

A natural person (holder of security data) who has logged into the BUSINESS 24 service via the correct security data.

User – Authorised person (also authorised person)

A user acting on behalf of the client on the basis of authority specified in respect of him/her in the contract.

User – Joint holder (also joint holder)

A user who is authorised to handle money on the client's accounts on the basis of an authority and within the scope assigned by the user - authorised person thereto. A joint holder has to be specified in the valid specimen signature for the concerned account.

Credit line

A credit scope of a predefined amount which includes one or more loan products.

11. Annex 1

List of transactions for the BUSINESS 24 – LIGHT service

- Display of account list and details (current, loan, deposit, savings accounts)
- Display of passive operations on payment cards
- Display of bank guarantee list and details
- Display of overdraft loan list and details
- Display of credit line list and details
- Display of current loan burden of the client
- Display of account balance
- Display of transaction history
- Display of advice list
- Display of non-executed transaction list
- Display and print of text account statements and their export
- Display and print of electronic statement
- Data statement export
- MT940 statement export
- Data statement print report generation
- Contract blocking
- Contract unblocking
- Change of password
- Change of contact details
- User blocking
- Application for the sending of a chip card
- Display of bank messages by type

12. Annex 2

BUSINESS 24 Mobile Bank – types of serviced accounts, main features and conditions of provision

Types of serviced accounts

- Current accounts
- Deposit accounts
- Savings accounts

Main features

- Display of account balances
- Entry of domestic payments, SEPA payments, and foreign-currency payments within the scope of the Bank
- Entry of FX Spot/Forward deals
- Transaction co-authorisation (batch import, multiple payment, single payment, foreign-currency payment, and express payment, foreign payment, SEPA payment, collection order)
- Display and cancellation of pending and non-performed payments
- Sending of push notifications about non-executed payments and transactions for co-authorisation
- Transaction history search
- Display of FX rate table (current and individual) and use of currency calculator
- Search for Česká spořitelna ATMs and branches
- Our important contact details
- DEMO version

Conditions • Account with Česká spořitelna (see Types of serviced accounts) with a joint-holder right of the following type: A (active), P (passive), S (joint co-authorisation), E (independent co-authorisation).

- Active BUSINESS 24 Internetbanking or BUSINESS 24 LIGHT for the set-up of password for Mobile Bank.
- Contract on higher security
- Possibility to log into B24 IB also by client number and password

13. Annex 3

Implementing directive for the usage of electronic certificates in direct banking services

General provisions

A user purchasing a chip card reader undertakes to acquaint himself/herself with the licence terms and conditions available from <https://www.csas.cz/PKILicence> and to observe them.

Certificates for the Bank's purposes are issued by a certification authority. The certification authority is První certifikační autorita, a.s., Prague 9, Libeň, Podvinný mlýn 2178/6, Postal code 190 00, Company reg. no.: 26439395, incorporated under the Registry Court in Prague, Section B, item 7136 (hereinafter also referred to as I.CA). Information on the certification authority may be obtained from <http://www.ica.cz>, or from the following e-mail addresses: oper@ica.cz and info@ica.cz.

The user shall be obliged to verify the correctness of the content of the certificate after the certificate is generated without unnecessary delay. If the user identifies inconsistencies between the Client Certificate content and data in the Protocol/Application, he/she shall be obliged to invalidate the certificate and to forthwith advise the Bank to this effect. The certificate shall be stored in the chip card and it shall be intended for securing direct banking services. The Bank does not provide support for the use of the certificate outside the scope of the direct banking service applications. The certificate secures:

- Data integrity;
- Obligation to provide response;
- Confidentiality of data;
- Set-up of a shared secret (key) within the scope of the protocol for secure data exchange; • Direct encryption and decryption of data;
- Direct signing of data.

Validity and effect of electronic certificates and chip cards

The validity of electronic certificates has been set to the period of one year of the day of its issue by the certification authority.

Information on the period of validity of the Client Certificate with the specification of exact time point of certificate expiry may be obtained at any time during its use

- from the footer of BUSINESS 24 screens
- from the Settings tab, under My settings
- via certificate administrator
- from the BUSINESS 24 line (tel. 956 777 888)
- from the Regional Corporate Centre or another business point.

Throughout its validity the electronic certificate is in effect, i.e. it may be used to secure direct banking services as defined in this Manual. The possibility to use services requiring the use of an electronic certificate is linked to its validity and effect.

Client Certificate

Client Certificate invalidation, renewal or change of data therein is described in detail by this Manual.

Software certificate

It is a necessary precondition for the functioning of the BUSINESS 24 Mobile Bank service. It is issued by Česká spořitelna, a.s. The certificate is free of charge and valid for one year. No special contract is necessary for its obtaining.

Chip card

For technical reasons, the validity of the chip card is limited. The expiry date is provided on the chip card in the YYYY format, which applies to 31 December of the given year. The last valid certificate may be downloaded to the chip card no later than on 31 December of the year preceding the expiry date of the chip card.

Electronic certificate validity renewal

Client Certificate

The validity of a user's Client Certificate may be renewed throughout its effective period, providing the following conditions are met:

- An effective contract on higher-type security has been concluded by and between the user and the Bank and, concurrently, the user has not advised any change to his/her identification details specified in the protocol/application;
- The user completes and submits an application for renewal of validity via the certificate administrator in a manner allowing the Bank to receive it before the Client Certificate expires.

Although the renewal of the Client Certificate also means the issue of a new one, the current contract on higher type of security will remain in effect in this case and once the certification authority successfully issues the Client Certificate, the previous certificate will be automatically invalidated.

The Bank shall advise the client of the expiry of the Client Certificate at least one month before the end of its standard validity, through the BUSINESS 24 screen and, concurrently, by an e-mail message sent to the e-mail address specified in the protocol/application.

The Bank shall decline Client Certificate renewal if the user does not have his/her own account activated for direct banking services and he/she is not a sponsored person. The user will be advised of this fact by the Bank when submitting the application for Client Certificate prolongation.

System certificate

The renewal of the system certificate validity via direct banking services is not supported by the Bank. The client may apply for the issue of a new system certificate.

Software certificate

Software certificates are renewed automatically. If the client enters an active transaction within the period of 30-90 days prior to the expiry date, an application for a new certificate will be generated. When entering another active transaction, the certificate will be withdrawn. If the client does not enter any active transaction within the timeline of 30-90 days prior to the expiry date, but only within 0-30 days, he/she will be invited to enter a password for the safe repository immediately after login, and an application for certificate withdrawal will be generated. Until the withdrawal is successfully completed, the client will not be able to work with the application. Should the certificate expire, the client has to deactivate his/her device in IB and to generate a one-time code and password for the Mobile Bank again. **Electronic certificate issue**

Client Certificate

In the following cases the user may/must apply for the issue of a subsequent (new) Client Certificate at a business point by submitting the application:

- The Client Certificate issued on the basis of the protocol and concluded contract on higher type of security or a previous application has expired, i.e. the user has not availed of the right to renew the Client Certificate
- If a change to the user identification details occurs (name/surname/address of permanent residence), even during the time of validity of the Client Certificate issued on the basis of the original identification details
- Loss/damage/exchange of the chip card or change of e-mail address

The Bank does not support the issuance of a subsequent Client Certificate for data which applied to a previously issued/invalidated Client Certificate.

Software certificate

The certificate is issued upon the first-time login to the application, when the client is invited to create a password for the certificate (secured repository). The application for the certificate is generated and the certificate

downloaded to the mobile device. In case of unsuccessful download the client may continue to work with the application without the possibility to submit active transactions. The certificate will be downloaded upon next login.

Electronic certificate invalidation

Client Certificate

The Client Certificate may be invalidated upon request of the user or in cases when the Bank is entitled to invalidate the Client Certificate:

- The Client Certificate has been issued on the basis of untrue or falsified data or the validated and certified data are no longer valid and the Bank learns about this fact
- The user failed to pay the price for the issue of the Client Certificate or has breached any obligation implied by the contract on higher type of security
- The user has died and the Bank learns about this fact
- Automatically, when the contract on higher type of security expires and the user has been using security via Client Certificate or if a subsequent (new) Client Certificate has been issued upon application submission
- Automatically, when the client has advised a change of data to the Client Certificate and has not applied for a subsequent (new) Client Certificate within the established timeline
- The issuance of Client Certificates for the purposes of the Bank has been terminated
- If concerned authorities have decided about the invalidation in compliance with effective legal regulations

The user shall be entitled to invalidate his/her Client Certificate only via certificate administrator or via the BUSINESS 24 line (tel.: 956 777 888 – the user will provide his/her name, surname and birth number).

The user shall be obliged to invalidate the Client Certificate if he/she suspects that it has been abused or if his/her chip card is lost or stolen.

After the Bank receives the client's justified application for Client Certificate invalidation, it shall forthwith revoke the validity of the Client Certificate and since that moment it will not be possible to use the Client Certificate for the purposes of electronic and telephone banking services and the Certificate shall be invalidated by the certification authority.

The invalidation of the Client Certificate irrevocably terminates its validity and it is no longer possible to use the Certificate.

Software certificate

A separate invalidation of the certificate is not possible. To invalidate the certificate, the BUSINESS 24 Mobile Bank service has to be deactivated.

14. Annex 4

User identification and authentication

The precondition for the execution of active as well as passive transactions in respect of the account is the user's identification by means of the security features. General information on the services provided by the Bank's financial group is accessible without authentication.

The following security features are used to authenticate the user:

Client number

A ten-digit number which is specific in the User set-up protocol. The User set-up protocol is given to each user when the service is contracted. The client number serves for the purposes of the client's authentication upon login. It is possible to apply for a change of the client number through a business point.

If the user logs into the BUSINESS 24 service by Client Certificate, the appropriate client number will be displayed in the Settings menu.

Telebanking password

A six-digit number which the user has received at a business point of the Bank or via registered mail consignment for personal delivery and which serves for the purposes of client's authentication when communicating with the telephone banker and for the first-time login to the BUSINESS 24 service. In cases of lost or forgotten password, it is possible to set up a new password via the BUSINESS 24 service if the client has logged in via the Client Certificate. When talking to the telephone banker the user can apply for the generation of a new password for

Telebanking. For it to be sent, it is necessary to provide the required positions from the security ID. The client may request the generation of new security data also at a business point of the Bank.

BUSINESS 24 Internetbanking access password

The password is a generated combination of numerals and letters of at least 8 and no more than 30 characters (distinguishing between upper and lower case and without the use of diacritical symbols) which should contain at least two letters and at the same time at least two numerals. The user sets up his/her password when logging into the BUSINESS 24 service for the first time, when the current password for Telebanking is used. It is possible to change this password at any time following an authenticated login to the BUSINESS 24 service. In case of forgotten password for the BUSINESS 24 service, it is possible to call the telephone banker and ask him/her (after an authenticated login) to set up this password to a password identical to the Telebanking password. When the user logs in again to the BUSINESS 24 service he/she will define a new password for the service. If the user has logged in via Client Certificate, it is possible to set up a new password in place of a lost or forgotten one via the BUSINESS 24 service.

Mobile Bank password

The first-time login is conducted with the client number, one-time code, and password for the Mobile Bank. The onetime code may be obtained via Internetbanking, where the client number will be also displayed. The password is a combination of letters without diacritical symbols, numerals, and some other symbols created by the client. The password for Mobile Bank is generated in Internetbanking after the user logs in via Client Certificate and it is necessary for the activation and subsequent logins to the BUSINESS 24 Mobile Bank application. The password must contain at least 6 and no more than 20 characters. The password distinguishes between the upper and lower case. It must not be a simple numerical sequence. If the Caps Lock key is activated, the screen will display a brief warning.

Biometrics login

You can also log in to your account in the BUSINESS 24 mobile application using biometrics. It is assumed that your mobile phone must allow this method to log in to applications.

Security ID

An eight-digit number of which only four characters selected randomly by the system are always entered. The user can have only one valid security ID. Corporate clients can ask for repeated generation of the security ID at a business point. Both corporate and business clients may apply for a new security ID via the telephone banker. The new security ID will be sent via registered mail consignment for personal delivery to the client's mailing address or issued at a business point.

Client Certificate

It is necessary for the authorisation of all entered active financial transactions and administrative operations. It is stored in a chip card and access to it is protected by a four-digit PIN code. To obtain the Client Certificate, it is necessary to sign the Higher-type security protocol at any business point.

Login SMS

An optional enhancement of security (client number and password) for the BUSINESS 24 service. A login SMS message is required upon each login. The set-up of login SMS messages is performed via the BUSINESS 24 service if the client has set up a mobile phone number for the sending of security SMS messages or upon login to the service via Client Certificate. The set-up may be requested at any business point.

Electronic signature

You can use an electronic signature to sign documents. Contact your bank consultant to send the documents for BUSINESS 24 internet banking electronic signature. It is simple, secure and more efficient. Instructions for signing the document can be found on the website: <https://www.csas.cz/en/navod-elektronicky-podpis-b24>

15. Annex 5

Overview of operations in the Business 24 service

The overview specifies individual operations by the user rights and the communication channels through which the operations may be executed. Some of the operations associated with account administration do not need to be necessarily conducted directly at the business point, but they can be executed by phone through the BUSINESS 24 support lines (chapter 8 *BUSINESS 24 support refers*) or via the internet.

User/joint holder administration	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Application for additional sending of new security data (security ID and Telebanking password)							TB
Application for the generation of a new password for the obtaining of the certificate and the sending of the PKI mailer							TB
Certificate renewal or change							IB, RKC, P
Unblocking of password for BUSINESS 24 Internetbanking							TB, IB ⁵
Contract blocking					✓		TB, RKC, P, IB
Contract unblocking					✓		TB, RKC, P, IB

User/joint holder administration	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Login SMS							IB
User blocking							TB
User unblocking							TB
Application for the sending of a chip card						Available only if chip card expires	IB, TB
Certificate collection							IB
Use of certificate						P, T only if the obligation to login via Client Certificate has been set up for them	IB
Revocation of (own) certificate validity							IB, TB
User access to service					<input checked="" type="checkbox"/>		IB
Login via client number and password						Unless the obligation to log in via higher security has been set up for the joint holder	IB, TB
Setting up of access to data					<input checked="" type="checkbox"/>		IB
Setting up of bank message sending							IB
User administration					<input checked="" type="checkbox"/>		IB

User/joint holder administration	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
User administration – set-up of authorisation for activities					<input checked="" type="checkbox"/> 6		IB
Sponsored persons administration					<input checked="" type="checkbox"/>		IB, TB
Change of password							IB
Change of Telebanking password						A joint holder without higher security conducts the change only via a voice automaton	IB
Change of contact details							IB May be changed only by an authorised user, both through the BUSINESS 24 service, via telephone support, as well as at any business point. A change of mailing address is effective immediately.
Change of PIN for chip card							IB
User/joint holder administration	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels

Unblocking of PIN for chip card						May be unblocked using PUK either on the login screen or immediately after the blocking	IB
Mobile Bank set-up	✓	✓	✓			Mandatory login via Client Certificate	IB

Account administration	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Adding an account for management							IB
Removing an account from management							IB
Setting up account limit							IB
Setting up co-authorisation limit							IB
Setting up co-authorisation							IB
Setting up co-authorisation between own accounts (under a single Identification Number)							IB
Setting up the sending of the current FX rate table							IB
Account name entry						AP has to have a special authorisation stipulated in the contract	IB

SEPA – SEPA collection execution regimen						For more details please refer to chapter 7.	IB
--	--	--	--	--	--	---	----

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Entry of a single FX deal (Spot, Forward, Swap) ^C						AP + JH ⁴	IB, MB
Entry of a block FX deal (Spot, Forward, Swap) ^C						AP + JH ⁴	IB
Entry of an FX order						AP + JH ⁴	IB
List of open deals						authorisation for at least one account	
List of FX operations display	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	AP + JH ⁴	IB

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Entry of a direct debit order	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>			IB, DB ¹
Entry of a transaction for co-authorisation (domestic payment [^] , multiple domestic payment [^] foreign payment/SEPA [^] , payment from FX, import of domestic payment/direct debit [^] , foreign payment/SEPA [^])	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>			IB

Entry of a payment from the account in a foreign currency							IB, DB, MB
Entry of a payment from the account in CZK ¹							IB, DB, MB
Cancellation of transaction with a future due date or of a transaction deferred due to lack of coverage of the account balance ³							IB, MB

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Entry of a foreign payment (ZP)				<input checked="" type="checkbox"/>		The payment order may be entered with priorities as follows: Normal, Express	IB, RKC, P, DB
SEPA entry ¹						The order may be entered with priorities as follows: Normal, Express.	IB, RKC, P, DB, MB
SEPA payment import							IB, DB
SEPA errors						Information on non-executed SEPA payments/collections	IB, DB, MB
SEPA direct debit / Blacklisted payees						As per the setup SEPA collection mode.	IB

Pending SEPA collections						Prior to the collection due date, the client-payer may decline any collection (regardless of the type of collection or	IB
--------------------------	--	--	--	--	--	--	----

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
						selected collection execution mode).	
SEPA collection order	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>			IB
Import of SEPA collection orders	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		XML format	IB, DB
SEPA B2B direct debit	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		Set-up of SEPA direct debits for collection type B2B.	IB
Direct debit display							IB
Direct debit detail							IB
Setting up a direct debit ¹							IB, RKC, P
Change of direct debit ¹							IB
Cancellation of direct debit ¹							IB
Display of a direct debit							IB

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
standing order							
Direct debit standing order detail							IB
Setting up a direct debit standing order ¹							IB, RKC, P
Change of direct debit standing order ¹							IB
Cancellation of direct debit standing order ¹							IB
Display of standing order for balance adjustment						7	IB
Standing order for balance adjustment detail							IB
Setting up a standing order for balance adjustment						AP has to be also joint holder "A" for the given client's account. 7	IB, RKC, P

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Change of a standing order for balance adjustment						AP has to be also joint holder "A" for the given client's account. 7	IB
Cancellation of a standing order for balance adjustment						AP has to be also joint holder "A" for the given client's account. 7	IB
Display of a standing payment order							IB
Standing payment order detail							IB
Setting up a standing payment order ¹							IB, RKC, P
Change of a standing payment order ¹							IB
Cancellation of a standing payment order ¹							IB
Entry of a multiple domestic payment from a CZK account ¹							IB

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Above-limit withdrawal advice ¹							IB
Export of data statements in the ABO or CSV formats for several accounts							IB

Export of MT940 statements							IB
Export of data statements in the xml format							IB, DB
Export of XML statements						Option to download the statement in the XML format defined by ČBA.	IB, DB
Multiple deletion of orders from a batch ¹							IB
Import of a domestic payment/direct debit batch (ABO format or MC format)							IB
Import of a domestic payment/direct debit batch from several accounts of the payer simultaneously							IB

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
¹							
Import of a foreign payment/ SEPA batch ¹							IB
Display of a text account statement and its export							IB
Display of an electronic account statement and its export							IB
Display of the account balance							IB, DB, MB

Activate/deactivate/change statement series							IB
Payee templates (setup, change, cancellation, use and export thereof)							IB
Template download							IB
Payee template import				–			IB
Application for the setup/change of a current account					–		IB, RKC, P

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Account management with passive access ¹							IB
Display of transactions for co-authorisation							IB, MB
Setting up the sending of credit advices							IB
Setting up the sending of text statements – Activation / Deactivation / Change ²							IB, MB
Display of the list of advices							IB, MB
Transaction coauthorisation							IB
Entry of a transaction for co-authorisation (domestic payment, multiple domestic payment, foreign payment, SEPA, batch import)							IB

Display of the transaction history							IB, DB, MB
Display of the list of							IB, MB
Current account transactions entered via B24	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Confirmation of acceptance of transaction for processing							IB, MB
List of files sent for collection account							IB
Sending of files (payments/direct debits) to the collection accounts ¹							IB
Display of the list of pending transactions							IB

Deposit and savings accounts	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Display of the deposit account							IB
Display of the savings account						7	IB
Deposit account detail							IB
Savings account detail						7	IB
Opening of a deposit account						For corporate clients only. AP has to be also joint holder "A" for the client's current account ³	IB, RKC, P

Change of a deposit account						AP with P rights for the specific deposit account ³	IB, RKC, P
Termination of a deposit account						AP with P rights for the specific deposit account ³	IB, RKC, P

Payment cards and card accounts	Joint holder K	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Payment card detail							Payment card holder: his/her own payment card only. Via TB also without authentication after the provision of certain personal data, only for private payment cards.	IB, TB

Payment cards and card accounts	Joint holder K	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Card account detail								IB, TB
Card account transaction history								IB, TB

Card account limit change							For business clients only. Via TB Authorised person for all/ Payment card holder: his/her own payment card only, if mentioned on the specimen signature. The functionality does not apply to deposit cards.	IB, TB
Change of payment card parameters and purchase of insurance							Insurance may be purchased only by natural persons entrepreneurs and legal persons	IB
Display and change of password for card								IB
Payment card blocking								IB
Replacement card ordering								IB
Payment card unblocking								IB
Display of a list of blocked payment cards								IB
Display of temporarily active cards								IB

Financing	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Import of list of receivables to be pledged ⁶						7	IB
List of receivables to be pledged ⁶						7	IB
Application for loan drawdown						Available only if at least one active loan account assigned under B24 exists ³	IB, RKC, P
Application for provision of a						7	IB, RKC, P

Financing	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
bank reference about own person							
Application for the issue of a debit card							IB, RKC, P
Application for the issue of cheque forms							IB, RKC, P
Display of the list of bank guarantees ⁶						7	IB
Display of the list of overdraft loans							IB
Display of the list of products within a credit line						7	IB
Display of the list of credit lines						7	IB

Loans						7	IB
List of loans						7	IB
Application for loan drawdown ⁶						7	IB
Exchange of documentation ⁶						7	IB
List of documents ⁶						7	IB

Financing	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Free application ⁶						7	IB
File submission ⁶						7	IB
List of conditions of loan relationships to be fulfilled						7	IB
List of issued guarantees/letters of intent ⁶						7	IB
Issued guarantees ⁶						7	IB
Advised guarantees ⁶						7	IB
New transaction/bank guarantee ⁶						7	IB
Data update ⁶						7	IB
List of orders submitted prior to 28 April 2014 ⁶						7	IB
Export letters of credit ⁶						7	IB
Import letters of credit ⁶						7	IB

Export collections ⁶						7	IB
Import collections ⁶						7	IB
New transaction ⁶						7	IB
Data update ⁶						7	IB
List of applications sent prior to 28 April 2014 ⁶						7	IB

PAYMENT 24	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Display of shopping basket detail						Available only if an active account for PAYMENT 24 assigned under B24 exists	IB, DB

Information	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
List of financing products							IB
Display of the summary list of accounts							
Display of the list of accounts							IB, DB, MB
Display of the account detail							IB
Information on current loan burden of the client							IB

Display of the current FX rates table							IB, MB
Display of the setting of the BUSINESS 24 service							IB
Display of the current bank messages							IB
Display of messages to be handled							IB
Settings wizard						Login via Client Certificate	IB

Exchange of documents	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Send templates							IB
Application for certificate							IB
Display of the list of documents sent via B24 IB							IB

Exchange of documents	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Bank report for the auditor	x	x			x		IB
Overview of company financial health	x	x			x		IB

- 1 Transactions entered by type T joint holder require co-authorisation.
- 2 For business clients only.
- 3 For corporate clients only.
- 4 A user with the account owner profile (AP + JH), who works in the context of an accredited client.
- 5 Only in cases of login through the Client Certificate.

- 6. These authorisations for activities are set up by a selected authorised person. A special authorisation of the AP is stipulated by the contract.
- 7. This functionality is available only for corporate clients.

- ^ Within thirty days after the expiry of the due date, it is possible to update the transaction entry date by adding the remaining signature and to execute the transaction with the current date.
- B Transactions for this purpose are: payment orders, batch import.
- C Sending to so called administrative operations repository does not apply to the operations.