ČESKÁ SPOŘITELNA

BUSINESS TERMS AND CONDITIONS
for the Use of Higher Type of Security

I. DEFINITION OF COMPETENCE

1.1. Business terms and conditions for higher type of security (hereinafter referred to as the “Terms and Conditions”) regulate the rights and obligations of natural persons (hereinafter the User) and Česká spořitelna, a. s. (hereinafter referred to as the “Bank”), ensuing from the contract for security means utilisation or from contract for providing higher security type and any other contracts referring to the Terms and Conditions. Rights and duties of the User and the Bank ensuing from the contract for security means utilisation or from contract for providing higher security type are also governed by the General Business Conditions of Česká spořitelna, a.s. (hereinafter the "VOP").

1.2. The current Czech rule of law of the Czech Republic governs the Terms and Conditions.

II. DEFINITION OF TERMINOLOGY AND ABBREVIATIONS

Concepts applied in the Terms and Conditions have the meaning stipulated by the VOP, unless thereinafter stated otherwise.

KCP	-	Klientské centrum Prostějov (Prostějov Client Centre) – the Bank’s workplace which provides direct banking (including its support) and information about the Bank’s products and services, the Bank Group respectively, by telephone, SMS or e-mail messages.
Contract	-	contract for security means utilisation; or also the contract for providing higher security type.
Protocol	-	document created on the basis of Client´s interest in having higher security type established, which represents call to negotiation addressed to the Bank, and that is for the purpose of concluding Contract.
Request	-	document capturing Client´s requirement addressed to the Bank; Request is made in cases anticipated especially in the Business Terms and Conditions.
Guide	-	document User Guide for SERVIS 24/BUSINESS 24 service, which describes features and methods for utilisation of Direct Banking services that the Bank provides.

Other terminology used:

Authentication calculator	-	equipment generating codes used to authorise active transactions of SERVIS 24 Services and for verifying the Client’s identity when logging in together with the client number and password into the SERVIS 24 Internetbanking Service, thereby increasing the level of security of the SERVIS 24 Services (not designed for use in the BUSINESS 24 Service),
Certification authority	-	the institution that issues, administers and rescinds client certificates,
Chip card	-	safe storage of the client certificate, a separate microprocessor on the card in accordance with ISO 7916,
Chip card reader	-	hardware equipment necessary for the use of chip cards,
Electronic signature	-	data about the manifestation of Client´s will and about the Client in digital form generated by the Client on the basis of the use of the Client´s certificate and attached to the data message that is specifically used for unique identification of the Client,
Password for acquiring a certificate	-	single password for confirming the request for a client certificate,
client certificate	-	data message issued to for the Client by certification authority based on Protocol/Request in order to identify and verify the Client´s identity, which is stored in the chip card and which is used for authorisation of active transactions, administrative operations, for electronic signature generation or for logging in, and that ensures maximum security of the SERVIS 24 Internetbanking and BUSINESS 24 services,
Matching data	-	data for creating an electronic signature using the appropriate data for verifying the electronic signature,
Unblocking code	-	used to unblock the authentication calculator PIN,
Sponsored person	-	The User for whom under the Česká spořitelna, a.s. rate list for banking transactions the fees and prices are associated with for the opening and administration of higher type of security charged and debited by the Bank to the account whose owner agrees with this fact through the Direct Banking Services,
Certificates’ administrator	-	software, Internet application allowing the administration of the client certificate,
Rescinded certificate	-	the client certificate the force of which was terminated without the possibility of its renewal.

III. BASIC CHARACTERISTICS

3.1. By concluding the Contract the User gets the possibility to utilise the token/authentication calculator and the client certificate as the security means for Direct Banking services.

3.2. User and the Bank conclude the Contract through their actual negotiation, and that is upon User´s call to the Bank to carry out such negotiation. In particular the creation of the Protocol represents the mentioned User´s call. On the basis of this call the Bank also hands over to the User the necessary equipment for utilisation of security means (e.g. the chip card reader and the chip card) provided that the User requires such equipment is handed over to him/her.

Contract between the Bank and the User is concluded by means of negotiations held between the Bank and the User, and that is through utilisation of equipment that enables the User to use the security means. Contract is concluded in case when (i) to the User, who uses/intends to use the client certificate the Bank will hand over to his/her use the mailer with the password for access to the client certificate, if the password is necessary for accessing the client certificate , and will enable the User to obtain client certificate in a way described in the User Guide of SERVIS 24 Internetbanking/BUSINESS 24, whilst the User will obtain this client certificate in predictable manner; if (ii) the User, who intends to utilise the token/authentication calculator, will use the calculator to log in to a Direct Banking Service and the Bank will not reject this use of token/authentication calculator. The Contract is concluded at the moment when the relevant client certificate is downloaded by the User or at the point of the first successful login of the User to a Direct Banking Service by means of token/authentication calculator. If the User utilises both devices for higher security type then the Contract is concluded at the moment when the first of the anticipated facts/negotiations between the Bank and the User occurred.

User agrees that the Bank will enable the use of the security means before the expiry of the 14-day period for withdrawal from the contract concluded remotely in the manner described in Article 4.1.6 of the Terms and Conditions.

3.3. Token/authentication calculator as a higher security type for SERVIS 24 services can be utilised immediately after the Contract is concluded (in case the Client has been using the Direct Banking Services already); Client Certificate can be used once it was successfully issued by certification authority.

3.4. When using security means within the Direct Banking Services the unique identification and authentication of the User is ensured not only by the Client ID and the password, but also the code generated by the specific authentication calculator, or independently of the client number and password, the electronic signature generated on the basis of the use of the client certificate.

3.5. The procedure for authorising transactions and signing data messages acquired through the Direct Banking Services and logging into the Direct Banking Services with the aid of a client certificate and/or authentication calculator is described in the Guide, in the document Authentication Calculator – user instructions and in the SERVIS 24 Internetbanking/BUSINESS 24 User Manual.

3.6. When purchasing the chip card reader, the User undertakes to become acquainted with and observe the licence terms and conditions available at http://helpdesk.servis24.cz or http://helpdesk.business24.cz.

IV. IMPLEMENTING GUIDELINES FOR USING CLIENT CERTIFICATES AS PART OF DIRECT BANKING SERVICES

4.1. General Provisions

4.1.1. The certification authority issues client certificates for the needs of the Bank. The certification authority under the Contract is called the První certifikační autorita, a.s. (First Certification Authority), Praha 9, Libeň, Podvinný mlýn 2178/6, ZIP Code 190 00, IČ: 26439395 registered by the Registration Court in Prague, Section B, File 7136 (hereinafter referred to as the "I.CA"). Information about the certification authority can be obtained at the website: http://www.ica.cz, or at the e-mail addresses: oper@ica.cz and info@ica.cz.

4.1.2. The User is obliged, without undue delay once his client certificate is generated, to verify the accuracy of its contents. If the Client identifies discrepancy between the Client Certificate content and the details in the Protocol/Request, the Client is obliged to invalidate the Client Certificate and to inform the Bank about such fact immediately.

4.1.3. The client certificate shall be stored on the chip card for security of the Direct Banking Services. The Bank does not ensure support when the certificate is used outside the Direct Banking Services application.

4.1.4. The client certificate ensures:

- data integrity,
- irrecusability of liability,
- data confidentiality,
- provision of shared secrecy (keys) as part of the safe data exchange protocol,
- direct data encryption and decryption,
- direct data signature.

4.2. Force and Effect of the Client Certificate and Chip Card

4.2.1. The force of the client certificate is set at a period of one year as of the date of its issue by the certification authority while information about the period during which the certificate is in force together with the exact moment that it ceases to be in force can be obtained at any time it is used through the certificates' administrator and/or the KCP.

4.2.2. The certificate is effective for the period that it is in force, i.e. it may be used for security of the Direct Banking Services as defined in these Terms and Conditions. The possibility of using services that the use of the certificate requires is subject to its force and effect.

4.2.3. Invalidation of client certificate, renewal or change of details in the client certificate is stipulated in details in the Guide.

4.2.4. The force of the chip card is restricted for technical reasons. The due date is displayed on the chip card in YYYY format, which means the 31st December of this year. The last time the client certificate can be saved to the chip card is on 31st December previous year to the date displayed on the chip card.

4.3. Renewal/Extension of the Force of the Client Certificate

4.3.1. The User may have the force of his client certificate extended during the period it is in force provided the following terms and conditions are fulfilled:

- there must exist effective Contract between the User and the Bank and at the same time there was no change in the identification data of the user specified in the Protocol/Request (with the exception of change of the e-mail address, which the User can perform by means of renewal/prolongation of the client certificate validity),
- The User shall fill in and mail through the certificates' administrator a request for the extension of the force of the certificate so the Bank accepts the client certificate while it is still in force.

4.3.2. Despite the fact that the renewal/extension of the force of the client certificate also means the issue of a new certificate, the existing Contract in this case continues to remain in effect and the force of the previous certificate ceases the moment the certification authority successfully issues the new client certificate.

4.3.3. User will be notified about the end of Client certificate validity at least one month before its standard validity ends, and that is to e-mail address specified in the Protocol/Request.

4.3.4. The Bank shall not permit the renewal of the client certificate if the User does not have his own account activated for the Direct Banking Services and is not a sponsored person. The Bank shall inform the User of this fact when the User submits a request for the extension of the force of the client certificate.

4.4. Issue of the Subsequent Client Certificate

4.4.1. User can ask for the issuance of the subsequent (new) Client Certificate at the Point of Sales of the Bank by means of the Request in the following instances:

- User is entitled to apply for the issuance of a new certificate in the event the Client Certificate issued on the basis of Protocol and concluded Contract, eventually based on the previous Request, ceased to be valid, i.e. the User did apply his/her right to renew the validity of the Client Certificate.
- The User is obliged to request the issue of a new certificate if there is a change to the User's identification data (name/surname/permanent address) during the force of the client certificate issued under the original identification data.
- User is entitled to apply for the issuance of a new certificate even in the event of loss/damage/renewal of the chip card, or in case the e-mail address is changed.

4.4.2. In such cases the existing valid Client Certificate is automatically invalidated by the Bank, based on the Request there is generated the new password for obtaining certificate, which can be sent by mailer or handed over directly at the Bank´s Point of Sales and the entire process of new certificate issuance has to be performed.

4.4.3. The Bank does not support the issue of the subsequent client certificate for matching data that already belonged to the issued/rescinded client certificate.

4.4.4. If the Request is created by reason of assigning/change/un-assigning of the token/authentication calculator and there exists valid Client Certificate issued on the basis of existing Contract in such case the validity of such Client Certificate will remain in force, unless the User wishes to have a new Certificate issued.

4.5. Rescission of the Client Certificate

4.5.1. The client certificate may be rescinded at the request of the User or when the Bank is authorised to rescind the client certificate for the following cases:

- The client certificate has been issued under false or falsified information, or verified and certified data is no longer in force and the Bank learns of this fact,
- The User did not pay the price for the issue of the client certificate or breached any obligation arising from the Contract or the Terms and Conditions,
- The User dies and the Bank learns of this fact,
- automatically in the event when the Contract ceases to be effective and the User utilised security through Client Certificate, or if a new (subsequent) Client Certificate is issued based on the Request,
- The issue is terminated of the client certificates for the needs of the Bank,
- If the authorised bodies decided to rescind the certificate in accordance with legal regulations.

4.5.2. The User is authorised to rescind his client certificate only through the certificates' administrator or through the KCP (tel. 844 111 144 or tel. 844 128 128 – The User shall state his name, surname and birth number).

4.5.3. The User is obliged to rescind the client certificate in case he suspects abuse or theft/loss of the chip card.

4.5.4. Once the Bank receives justified User´s requirement to invalidate Client Certificate the Bank will without delay revoke the Client Certificate validity and thenceforth the Client Certificate cannot be utilised for Direct Banking Services and the Certification Authority will invalidate the Certificate.

4.5.5. The rescission of the client certificate ends its irrevocable force and the certificate may no longer be used.

V. CLOSING PROVISIONS

5.1. The Contract and Terms and Conditions do not replace other contracts concluded between the User and the Bank, or some member of the Bank Group for the purpose of regulating the legal relations in connection with the provision or use of the Bank's other products or some member of the Bank Group and other business terms and conditions. In case of any inconsistency in some provisions to the Terms and Conditions valid for the Bank's accounts and other products, the Contract and Terms and Conditions prevail.

5.2. Contract concluded between the Bank and the User by means of factual negotiation under Article 4.1.7 represents Contract concluded remotely. Provided that the User is a consumer pursuant to § 52, par. 3 of Act No. 40/1964 Coll., the Civic Code (hereinafter the CivC), the Bank shall inform the Client on the following facts:

The service is provided by the Bank; the User can contact the Bank by means of the e-mail address servis24@csas.cz, or address the correspondence to address Česká spořitelna, a.s., Klientské centrum, Knihařská 10, P.O.BOX 33, 796 01 Prostějov. For telephone communication the User can use telephone number 800 207 207. The Bank recommends to the User sending his/her submissions mainly in electronic way, to the above-stated e-mail address.

The Bank is subject to supervision executed by the Czech National Bank, registered office at Na příkopě 28, Prague 1, Post Code 115 03. Information on the issuance and use of security means is stated in individual sections of the General Business Conditions, in Terms and Conditions and in the Guide. Prices of service or individual fulfilments related to the service are described in the Česká spořitelna, a.s. List of Charges for banking deals.

User has the right to withdraw from the contract concluded through remote communication means within 14 days from taking over the fulfilment without any sanction and without stating the reason for withdrawal.

Contract is concluded between the Bank and the User through their actual negotiation and in view of this the Bank only records and archives the User´s act, which with the relevant cooperation of the Bank (Article 4.1.7 of Business Terms and Conditions), results in conclusion of the Contract.

The Bank elaborated the Banking Services Code of Česká spořitelna and also adopted the Ethical Code of the Czech Banking Association. Both the documents are available at the home web page of the Bank (www.csas.cz).

5.3. The User is obliged to simultaneously follow the manuals or similar documents issued by the Bank for services connected with the use of higher type of security, which are above all the following:

- SERVIS 24 Services User Guide
- BUSINESS 24 Service User Guide,
- Authentication calculator – user instructions,
- SERVIS 24 Internetbanking User Manual
- BUSINESS 24 User Manual.

5.4. The Bank reserves the right to change or regulate these Terms and Conditions at any time with respect to the development of the legal environment and with regard to its business policy.

5.5. The Bank is obliged inform the User individually, in an appropriate manner, and at lease 1 month in advance of these changes (or modifications) and the date of their effect and simultaneously access the new (or modified) wording of the Terms and Conditions in the public premises of its business places and on the Bank's home website (www.csas.cz). If the User does not express his disapproval by the effective day of the change to the Terms and Conditions of such a change to the Terms and Conditions in writing, it is deemed that such a change is approved by the Client and is effective with regard to him as of the day the Terms and Conditions come into effect.

VI. FORCE AND EFFECT

6.1. These Terms and Conditions come into force and effect on 31 October 2009. On the same day, the Business Terms and Conditions for the Use of Higher Security Types, effective as of 18 April 2009, shall cease to have effect.