ČESKÁ SPOŘITELNA

SECURITY DATA OF MULTICASH APPLICATION

The MultiCash application (further only "MC") is installed to the Client under the closed contract documents including an appendix in which the Client is obliged to set the authorization for individual users who will handle funds deposited in accounts of the Client.

- Client = company
- User = authorized employee serving MC

Security Data

Obligatory MC Security Data

- Password Login
- Password for Communication with the Bank (communication password):
  - Password that the User uses for identification in electronic communication via MC,
  - After three wrong attempts to enter password, the password is locked,
  - Password unlock is possible only in collaboration with the authorized employee of the Bank from MultiCash Client Support.
- Password for Electronic Signature (ES password):
  - Password that is necessary for data transfer from the Client to the Bank,
  - Verifies the user's signature in sending payment Files to the Bank.
- Signature Types for Users:
  - Define the extent of individual User authorization for disposal of funds in accounts of the Client,
  - Signature type of Users is set by the Client.
- Payment File Encryption:
  - Payment File is encrypted in sending payment Files from the Client to the Bank.
- Bank Parameter Data File (BPD):
  - File contains User's data necessary for electronic access to the Bank.
- Activation of the MC service User on the part of the Bank.

Above Standard MC Security Data

- ES Limit for Payment File:
  - Defines the total amount of payment orders in the outgoing File.
  - The limit is set for one sent File. A different limit can be set for each User.
- Daily Limit:
  - Defines the total amount of sent Files,
  - This limit applies to each File irrespective of File type and account to which it is addressed,
  - The limit is set on a daily basis.
    - Authorization and approval of entered payments.
    - Client number and password for telebanking
    - All Users irrespective of signature type can obtain passive information, by telephone, on accounts connected to the MultiCash service, e.g. information on incoming and outgoing payments, current balance etc.

Each payment entered into the MultiCash service requires the Client's authorization and approval that is necessary for creating a File and its sending to the Bank.

Individual passwords are chosen by users themselves. After three failed attempts to enter password, the password is blocked. Some passwords can be restored only by the User, other passwords need to be reactivated only with the help of the Bank. Users are obliged to store security data, such as passwords, USB flash disk or diskettes, in a safe place and to prevent tits misuse, theft or loss.

Each MC service User with rights to handle funds in the Client's accounts shall have a specimen signature recorded in the Bank. At the same time the User shall be physically verified by an entrusted employee of the Bank.

Details of individual security data are described in the user manuals for MultiCash 3.2 that are the part of the MultiCash installation set.

Identification data

Users are identified by the Bank on the basis of:

- Name and surname of the User,
- Birth number or date of birth,
- User number assigned by the Bank during setting the User parameters,
- Client number and password for Telebanking. Based on this data verification the User will be provided with information,
- by telephone, on active and passive operations on current accounts connected to the MultiCash service, such as on payment status, account balance, information on payments made, etc.:
    - Client number and password are assigned at the request of the User if he/she has not been assigned identification data for Service 24 Telebanking and Business 24 Telebanking,
    - Client number and password for Service 24 Telebanking and Business 24 Telebanking are also valid for the MultiCash service,
    - Client number and password for telebanking are assigned to the User irrespective of the given signature type.

The Bank requires this data for preparation of contractual documentation including the relevant appendices and filing specimen signatures in the Bank and further in communication of the Client with the Bank.

Signature types for the MultiCash application

Signature type	Description	Right	Signature card
E	The User can sign File independently up to the set limit.	Active, Inactive	yes
A	The User can sign File together with User E, A, B, H or I up to the set limit.	Active, Inactive	yes
B	The User can sign File together with User E, A, H or I up to the set limit.	Active, Inactive	yes
		Active, Inactive	
H	The User can sign File up to the set limit as in Type A. If the limit amount is exceeded, the User can sign File only together with another User E, A, H or I according to the set limits.	Active, Inactive	yes
I	The User can sign File within the set limit independently as in Type E. If the limit amount is exceeded, the User can sign Files only together with User E, A, B, H or I.	Active, Inactive	yes
F	The User can sign File only together with User G with respect to set limits.	Active, Inactive	yes
G	The User can sign File only together with User F with respect to set limits.	Active, Inactive	yes
T	The User can sign File only to send it to the Bank for remote signature.	Active, Inactive	yes
N	The User is not allowed to sign files.	inactive	no

Clients can download from Česká spořitelna internet sites www.csas.cz/multicash the following materials:

- User Manual for MultiCash 3.2
- General Terms and Conditions
- Special Terms and Conditions for the MultiCash Direct Banking Service
- Recommended client configuration
- News in the new application version
- Technical descriptions of data formats

Contact data at ČS

- address: Česká spořitelna's Client Centre.; MultiCash service support
- phone: +420 956 711 711
- email: multicash@csas.cz;
- web: www.csas.cz/multicash