

General Overview of MultiCash Classic Security

MultiCash is developed by German-based software company Omikron (www.omikron.de). The Royal Bank of Scotland N.V. bought the license for this product to use it (with all necessary localisations) and made it as its corporate electronic banking standard in the CEMEA region. The package is currently offered to all our corporate clients in the region (Austria, Germany, Netherlands, Switzerland, Spain Russia, Poland, Czech Republic, Romania, Kazakhstan and Uzbekistan) under the name MultiCash Classic.

Please find below summary and general remarks on MultiCash Classic security.

Software acceptance

The customer licences the software "MultiCash" from The Royal Bank of Scotland N.V., which has its own processes for accepting and auditing the application to comply with the bank regulations. In certain cases, e.g. Germany, there is in addition a central project management process for all private banks for which the Bank-Verlag (subsidiary of the bank association) is responsible. A check on audit compliance can be part of the responsibility of this organization, too.

Communication protocol

The highest priority in the security area, and the one affecting the banks' responsibility is the security of the connection between Customer and Bank. The communication between customer and bank is almost exclusively built on the Omikron-own communication protocol, MCFT. This protocol includes as part of an integrated package the necessary checks on authentication, validation and the integrity of the data exchanged. For this protocol, Omikron has commissioned its own external audit. A Management Summary of this audit is available upon request; please note this is not intended for general publication but may be used in case of specific inquiries.

Security features

For local security within the application, a variety of options have been included on the basis of the varying requirements of the user banks, associations and their auditors.

Users / User Groups

- User rules (Working times/Day, Pause for nr. days/Blocked)
- Functional profile (access rights per individual function)
- Data profile (Read/Write permission, Limiting of data access)

Password rules

- Validity duration
- Minimum length
- Password history

Password Administration

- Password change on first logon
- Blocking of users on three false attempts

Password storage

- Access passwords are stored encrypted
- Signature passwords are NOT stored

Other

- System log (= Audit Trail)
- Dual control for administrator functions
- Approvals scheme for payments
- Protection against manipulation of payment in the communication queue (checksums) .

All these features combined allow for the application to be easily adapted to the requirements of individual company auditors.

Appropriate steps taken by the customer must ensure the security outside the application, i.e. the embedding of the software within the general organizational environment of the corporate user.