UniCredit Bank

TECHNICAL REQUIREMENTS FOR ELECTRONIC BANKING SYSTEMS

February, 2025

UniCredit Banka Slovenija d.d.

Ameriška ulica 2
SI-1000 Ljubljana
Slovenia

Tel.: +386 1 5876 600 Fax: +386 1 5876
684 Registered with the Ljubljana District
Court under reg. no. 1/10521/00, share

capital of the company EUR 20,383,764.81, registration number 5446546000,
VAT ID number SI59622806, transaction account (IBAN) SI56 2900 0190 0030
037.

INTRODUCTION

For the smooth functioning of electronic banking systems, it is necessary to meet the minimum necessary hardware and software requirements. These requirements are described below for each system separately and apply only to the system described.

1. TECHNICAL REQUIREMENTS FOR THE E-BANK PERSONAL/CORPORATE APPLICATION

1.1. Single-User Solution – E-bank/Personal

- a personal computed running, Windows 8.1, or Windows 10, Windows 11. All Windows operating systems must be updated with the latest patches;
- Hal E-Bank software;
- a qualified digital certificate on a secure storage media issued by Halcom CA;
- a connection to a bank server (internet access or a dial-up connection); and
- a business agreement on using Hal E-Bank solutions concluded with the bank.

If your qualified digital certificate has been issued on a smart card, you also need a smart card reader (connected to your PC).

HARDWARE REQUIREMENTS:

COMPONENT	REQUIREMENT
Computer and processor	minimum: 1 GHz recommended: at least 2 GHz 32-bit processor
Memory (RAM)	minimum: 1 GB recommended: at least 2 GB
Hard Drive	minimum: 1 GB recommended: at least 2 GB of free space
Screen	minimum: 1024 x 768 pixels
Additional requirements	Internet connection. If you are using a modem connection to the Internet, the modem must support a transfer rate of at least 128 kbps, preferably 512 kbps.
	If you have a qualified digital certificate issued on a smart card, you also need a smart card reader (connected to your PC)

SOFTWARE REQUIREMENTS:

In order to install the software, you need either the appropriate installation rights or a system administrator must be present.

- Nexus Personal smart card reading software (Windows 7 SP1/8.1/10) ⊠ must be installed;
- Microsoft Internet Explorer internet browser version 11.0 or higher installed; and
- Adobe Acrobat Reader or Adobe Acrobat X version 10.0 or higher installed;

REQUIRED PARAMETER SETTINGS:

- time zone on PCs running a Hal E-Bank client or a base server must be set to GMT+1.
- Support for Slovenian regional settings must be installed (but not necessarily default) on workstations.

When connecting to a bank server through a firewall, it is necessary to open the required ports for transferring data and refresh the application to connect. IP addresses and required port numbers are listed and located at the following link: http://www.halcom.si/si/pomoc/?action=showEntry&data=203.

- The connection application does not use HTTP proxy servers, as the basic data transfer protocol is not HTTP.

The application can connect directly to the HTTPS server, but not via a proxy server. So far, we have received very few requests for the implementation of SSL tunnelling or support for SSL proxies. From a security point of view it is irrelevant whether the company allows access to a URL via an SSL proxy or allows opening external connections to a specific server and TCP port.

The only proxy servers therefore supported by the client are port forwarding or traffic redirection proxy servers, where all traffic sent to the TCP port of the proxy server is forwarded to the target e-banking server in an unchanged form.

1.2. Multi-User Solution – E-bank/Corporate

Hal E-Bank/Corporate is intended for organizations where several persons are responsible and authorized for working with electronic bank and perform payment operations on many computers that are connected to the local area network.

Hal E-Bank/Corporate program works on the client-server principle and requires a shared database, which is usually installed on a server. The database server IBM DB2 has to be installed on the server. On the workstations, where Hal E-Bank Corporate clients are installed, there has to be IBM DB2 Client Application installed and the software has to be properly configured. To perform installation on the server full control administrator rights are necessary.

Additional requirements for using a multi-user solution compared to the single-user solution. These are additional to the requirements that apply to the single-user solution!

CLIENT COMPUTERS/WORKPLACES:

Client computer requirements:

- connected to the local network via TCP/IP protocol;
- at least 2 GB of free hard disk space; and
- if dial-up access is used to connect to the Hal E-Bank server, a modem must be installed on at least one computer with the Hal E-Bank client installed. If dial-up access is used, it is possible to exchange data with the bank only on the computers that have modems installed. If the modem is installed on only one computer, all data exchange with the bank will take place via this computer.

BASE SERVER FOR THE COMMON DATABASE:

Operating system requirements vary depending on the version of the database: –
IBM DB2 ver. 11.1

- Windows 7 SP1 (Enterprise, Professional, Ultimate);
- Windows 8.1 (Enterprise, Professional, Standard);
- Windows 10 (Enterprise, Professional);
- Windows Server 2012 (Datacenter, Essentials, Standard);
- Windows Server 2012 R2 (Datacenter, Essentials, Standard);
- Windows Server 2016 (Datacenter, Essentials, Standard).

The operating system requirements for workstations are the same as for the server.

- TCP/IP protocol support.

- The disk space required to install IBM DB2 is at least 2 GB. Regarding the required disk space for the database, it is difficult to estimate the size of the database, because of its ability to receive files. Approximate calculation: 5000 transactions = 20 Mb of space + files.
- Memory (RAM) Size:
    - Windows 7 SP1/Windows 8.1/Windows 10 at least 1 GB and an additional 4 MB of RAM for each concurrent user of the Hal E-Bank network version (1.5 GB of RAM recommended)
    - Windows Server 2012/2016 at least 1.5 GB and an additional 4 MB of RAM for each concurrent user of the Hal E-Bank network version (2 GB of RAM recommended)

The recommended memory size also depends on other applications running on the server. The main requirement is for the server to have enough RAM to not use the disk as memory (swap).

- Support for Slovenian regional system settings must be the default at least for the duration of the installation process. ("Regional Settings – Slovenian"; "Set as system default local") ⊠
- IBM DB2 database.

To facilitate the installation, before the arrival of the technician it is required on the server to:

- Create a folder titled "EbankFiles".
- For all future users of the multi-user version of Hal E-Bank/Corporate, it is necessary to set access to this folder (security, sharing – users must have the right to change the folder, subfolders and files).
- The client accesses the server through the TCP/IP port 50000, which means that the specified port must be open on any potential firewall and any router located between the client and the server where the database is located.

1.3. Security Mechanisms Required for the E-Bank application

To use the E-bank application safely, the user must:

- use antivirus software that is regularly updated according to the instructions of the provider/manufacturer;
- use a firewall (exceptions are ports 3600 and 3604, which must be open for smooth functioning);
- regularly update software with security patches with the latest paches and versions according to the instructions of the provider;
- carefully protect the data and elements of the authenticationfor entering the E-bank program (PIN code, certificate) and ⊠
- regularly change the password for access to the E-bank program.

2. TECHNICAL REQUIREMENTS FOR THE USE OF ONLINE BANKING

The following equipment is required for the proper functioning of Online Banking:

- username;
- token for generating passwords and PIN number;
- and internet access.

2.1.Hardware Requirements

- **Internet connection;**

2.2. Software Requirements

- Windows 7 or Higher, MacOS 10.9 or higher

-

Browser	Minimal Version
Chrome	51
Firefox	68
IE	11
Edge	13
Safari	7
Opera	24

- Adobe Acrobat Reader version 17 or higher installed;

2.3. Software Settings Requirements

- TLSv1.2 (Transport Layer Security) protocol;
- JavaScript enabled;
- the display of website pop-ups enabled www.unicreditbank.si and https://si.unicreditbanking.net;

2.4. Security Mechanism Requirements for Using the Online Banking application

To use the Online Banking application safely, the user must:

- use regularly updated antivirus software;
- use the MS Windows firewall;
- update all software with issued security patches; and
- carefully protect data and equipment for entering Online Banking (token, PIN code, username).

2.5. Security Mechanism Requirements for Using the Online Banking application

- In the Online Bank settings, activate a security question and answer that only you know.
We advise you to regularly check and change the security questions.
- Access Online Bank exclusively via the official website or via the secure link https://si.unicreditbanking.net.
- Do not allow third parties remote access to your computer.
- Follow the bank's security notices about possible fake websites.
- Regularly take care of security updates on the operating system and browser you use to use the Online Bank.
- The bank never checks your data (payment card numbers, password for the Online Bank), via e-mail or over the phone, so do not trust them to anyone, even if you are asked to do so.
- Use the option to limit the use of funds yourself by changing the transaction and daily limit in Online Bank.
- Use the option of additional notifications in Online Bank. You can activate the notifications yourself and they are carried out via e-mail.
- In case of any irregularities, notify the bank immediately at online[at]unicreditgroup.si.
- For more details on information security, we suggest you visit and review the content on the website www.varninainternetu.si and https://pazi.se/.

3. TECHNICAL REQUIREMENTS FOR USING APPLICATIONS MOBILNA BANKA GO! AND MOBILNA BANKA PRO!

The following equipment is required for the proper functioning of the application:

- Internet connection;
- Android 6.0 or higher – for users with smart devices using the Android operating system;
- iOS 13 or higher – for users of Apple smart devices;
- HarmonyOS 2.0 – for users of Huawei smart devices;

Security mechanisms when using the Mobile Bank GO! And Mobile bank PRO!

For safe use of the Mobile Bank GO! And Mobile bank PRO! we recommend:
- use of antivirus software for mobile devices,
- that the mobile device does not have the manufacturer's restrictions removed for accessing parts of the mobile system that are protected (i.e. rooting or jailbreaking)
- that you have access to the mobile device secured by a security element (PIN code, fingerprint,...)
- to install applications only from official application stores (never through web links in e-mails)
- to regularly update your mobile devices with the latest updates provided by the mobile device manufacturer
- that instead of open access points, you prefer to use a data connection (3G, 4G, 5G) or opt for a virtual private network (VPN) service

Safety recommendations when using the Mobile Bank GO! And Mobile bank PRO!

- Never store usernames and PINs on your mobile device
- The bank never checks your data (payment card numbers, password for the Online Bank), via e-mail or via phone call, so do not trust them to anyone, even if you are asked to do so.
- Do not allow third parties remote access to your mobile device, even if this is explicitly requested.
- Activate a security question and answer that only you know. We advise you to regularly check and change the security questions.
- Follow the bank's security notices about possible fake websites.
- Use the option to limit the use of funds yourself by changing the transaction and daily limit in Mobile Bank.
- In case of any irregularities, inform the bank immediately at online@unicreditgroup.si.
- For more details on information security, we suggest you visit and review the content on the website www.varninainternetu.si and https://pazi.se/.

4. USER SUPPORT

You can send additional questions to the following e-mail addresses:

- e-bank@unicreditgroup.si
- online@unicreditgroup.si

or call the electronic banking systems user help desk at +386 1 5876 600.