Security

UC eBanking prime

Security recommendations

hilfe.hvb.de
gtb-center@unicredit.de

Inhalt

GENERAL INFORMATION ABOUT UC EBANKING PRIME

The UC eBanking prime server is installed on the customer's Intranet as a web application. What this means in practice is that, once the application has been installed, all authorized workstations across the company can access the system, wherever they are located. Communications with and data transfer to banks use the secure, web-based EBICS transfer process, which is standard throughout Germany. Login and signature is done using a standalone application (primeOTC).

CLIENT COMMUNICATION

Communication between client and server should be done using https. The certificates required for this must be provided or generated by the customer, as these require a private secret key. UniCredit provides an SSL tool including instructions for easy setup.

We explicitly recommend the use of certificates signed by a public or customer-owned trust center.

Alternatively, UC eBanking prime still supports http.

SECURE KEY STORAGE

The keys needed to log in to UC eBanking prime are stored as software keys in keybag files and are protected with a password.

It is essential to ensure that they are kept secure, stored, and protected from unauthorized access. Please also note the following additional information:

- If key files are stored on a central storage medium, other persons may have access (e.g. system administrators).
- Removable media containing key files can be accidentally left open or accidentally get stuck in the PC.
- Key files can be copied unnoticed and thus fall into unauthorized hands. Therefore, you should not store software keys on fixed data carriers (local drive, network drive), but at least on removable data carriers that must be stored securely after use. UC eBanking prime has also implemented mechanisms that ensure that only one version (original) of the key file can be used at any time. Parallel use of a second version (copy) is not possible.
- The security medium (e.g. USB stick) on which the software keys are stored must be protected against misuse and theft. This requires secure storage, e.g. by locking it up. Furthermore, we recommend that you additionally secure access to the security medium. This can be done, for example, by using a special USB stick with a numeric keypad and encryption hardware.
- Security media for storing key files should only be used for this purpose and should not be used for storing other data. Access to both the medium and the software keys stored there must be secured by a password. UC eBanking prime allows access to the keys only by entering an appropriate password. Rules for creating and changing passwords should be part of your company's internal security policy. Further information on passwords can be found later in this document.
- Use the option of changing the key. This updates the key file and an old version can no longer be used.
- After the last use, the security media should be safely disposed of or destroyed.
- UC eBanking prime offers the option of allowing software keys to be saved exclusively on external media, as well as informing the user that the media must be removed after use.

IMMEDIATE BLOCKING OF KEYS IN CASE OF SUSPECTED MISUSE OR THEFT

In the event of suspected misuse or theft, you are advised to inform your banks immediately of the misuse of the keys or the loss/theft and to have the EBICS access of your affected users blocked with UC eBanking prime.

CLEAR ASSIGNMENT OF THE SECURITY MEDIA ON WHICH THE SOFTWARE KEYS ARE STORED

Each employee who uses UC eBanking prime must be assigned his or her own security medium (e.g., USB stick), for which he or she must take care. The participant should use this medium exclusively for storing the key files for UC eBanking prime.

SECURE PASSWORD

In general, all passwords should be sufficiently long and complex. A change of passwords is mandatory if you have suspicion of any other person having knowledge of your password. No identical passwords should be used for different purposes or applications. The passwords also should not differ only by replacement of one character.

In UC eBanking prime, administrators can specify rules for the creation and validity of passwords. Furthermore, the use of previous passwords can be restricted.

As guideline for safe passwords please consult the recommendations of the German BSI: https://www.bsi-fuer-buerger.de/

To avoid password leaks no password is to be written in plain text on the computer (e.g., in a file) or on a sticky note. Instead, a free accessible tool for password handling could be used which in general also supports safe password generation.

In addition, a program for secure password entry could also be used that allows passwords to be entered bypassing the keyboard. In this way, it can be prevented that the passwords entered via the keyboard are recorded by unauthorized persons (by means of so-called keyloggers) and misused.

In UC eBanking prime the last login or log in attempt is displayed, this should always be checked.

LOGON AND AUTHORIZATION VIA OTC CLIENT

To enable secure and convenient login to UC eBanking prime, a standalone OTC client is provided with the installation. This software must be installed on every computer that uses UC eBanking prime. No admin rights are required for this.

Based on the keybag and the corresponding password (see above), the client generates a login code that is valid for 60 seconds and must be entered in the browser (comparable to a TAN). The OTC client then establishes a permanent connection to the server.

If data is available for signing, the OTC client opens and displays the data to be signed. The signature is then executed again using the above-mentioned password. Once all the necessary signatures have been provided, the payment is automatically sent to the bank.

AUTOMATIC LOG-OUT

If the OTC client or the browser is closed, the user is automatically logged out of UC eBanking prime. In addition, an automatic log out occurs when the inactivity time defined by the customer has expired. The user can then log in again directly.

AUTOMATIC USER LOCK

Users who have entered their password incorrectly several times in a row (the number can be configured by the customer) or who use a copy of their keybag are automatically locked. The users can then be unlocked within the software using the 4 eyes principle. One of the users must have at least the role "audit".

OPTIONAL ONE-TIME PASSWORD (OTP)

UC eBanking prime offers the possibility of optionally also using a one-time password in addition to the keybag file. For this purpose, a password generator generates a password on request (the use of a smartphone app is recommended for this purpose) which is valid only once or for a limited time (e.g. 30 seconds) and must be entered when logging in and before each payment release.

UC eBanking prime supports the standardized procedures TOTP and HOTP.

TIME-LIMITED SYSTEM ACCESS

Access to UC eBanking prime can be individually time-restricted for each user, e.g. to allow access to the system only during business hours. (e.g. Monday - Friday, 8 am - 5 pm).

PERMISSIONS WITHIN UC EBANKING PRIME

UC eBanking prime offers an extensive permission concept - you can individually set which users see which data and which permissions the users get.

ROLES

The most important roles that distinguish UC eBanking prime are:

BANKING

The user has access to the banking functions and data of the software. (e.g. payments and cash management).

ADMIN

The user may administrate banking data (e.g. authorizations, users, banks, accounts). For the administration the 4 eyes principle can be activated by the administrator of the customer.

SYSTEM

The user may make technical settings (e.g. proxy, organizations).

AUDIT

Contains all security relevant options (e.g. password settings, login).

We recommend to strictly separate technical and administrative roles.

In addition, there is a main administrator for support staff of the bank. The password of this user expires every 24 hours and can only be reset by a daily changing one-time code, which only UniCredit knows.

SECURITY OF THE COMPUTER

SECURE OPERATING SYSTEM

The operating system and other installed software e.g. PDF reader and browser must be updated regularly. The updates should be done only by means supplied by the provider e.g. Windows update or available update links within the software.

SECURE BROWSER

Only use browsers released by UniCredit (see Release Notes) and perform the security updates supplied by the provider in time. Usage of additional programs in the browser should be avoided when they are not necessary. Additional programs should only be activated for trusted websites. If the browser supports mechanisms designed for Phishing and Malware Protection these should be used.

As a guideline for security settings of several browsers please also consult: www.bsi.bund.de/ .

UPDATED VIRUS SCANNER

Usage of anti-virus software is mandatory. Also, this software must be updated regularly. In general, the anti-virus software includes permanent scans and automated updates in the background after every start of the computer. Additionally, the computer should undergo a complete testing by the anti-virus scanner at regular intervals.

Make sure the anti-virus software includes protection of your browser.

UC EBANKING PRIME UPDATES

UC eBanking prime should be updated regularly. We will inform you about regular updates and urgently required (security) patches via the integrated notification function. Please check regularly if there are messages for you here and apply the updates promptly.

COMMUNICATION BETWEEN SERVER AND BANK

Communication with the bank takes place exclusively via the server using the EBICS standard. The specification of the standard is publicly available at www.ebics.de and relies on min. TLSv1.2/TLSv1.3 as transport encryption in addition to strong 2,048 bit encryption.

Communication is always outbound via port 443 and can be routed via a proxy for security reasons. No incoming ports must be opened, and the server does not have to be in the DMZ or accessible via the Internet.

SOFTWARE DISTRIBUTION REGULATES PROGRAM INSTALLATION

Installation and maintenance of software should solely be done within a regulated process (e.g. temporary administrator access rights and documentation). Especially in case of installation of banking software by service providers other than banks the technical access rights need to be restricted and deleted directly after installation. The technical access rights must be authorized by the IT-responsible of your company. To enhance the security level authorization and installation process should be concluded in 4-eye-principle and be duly documented. Workplace and access (e.g. remote access) needed for the installation should be defined and authorized beforehand.

SINGLE SIGNATURE RIGHT

Legally it is possible to arrange a single signature right for a bank related signature. This means that only one signature can be required to release transactions.

To enhance the security level, we strongly recommend a joint signature. Therefore, you agree with the bank on two or more signatures for authorization of transactions. The 4-eye-principle is known as effective measure against assaults, as malicious or manipulated payments (e.g. after loss or theft of the key but also after social engineering attacks) can be detected and dismissed by the user with second signature.

RESPONSIBLE HANDLING OF DATA AND SOFTWARE

Measures must be taken for information security on organizational, technical, and personal level. These measures need to include protection of access to premises and data, installation of firewalls, active management of access rights as well as monitoring and logging. Protection from malware today is essential. Furthermore, a regulated process to install software and provisions to protect the corporate network are to be implemented.

Also, in your technical environment precautionary measures need to be taken to support the included security policies for data exchange. Information and recent notes can be found at http://www.bsi.bund.de/.

SECURE INTERFACES BETWEEN UC EBANKING PRIME AND YOUR ERP SYSTEM

UC eBanking prime offers the option to define folders that are polled regularly (usually between 3 and 5 minutes) and import all payment files contained therein. In addition, retrieved data from bank (e.g. account statements) can be placed in defined folders for further processing.

AUTHORIZATIONS FOR INTERFACES

Only users who need to create files and store them in the UC eBanking prime interfaces or retrieve the statements stored there may be authorized. In general, we recommend that only the host systems (server UC eBanking prime and server ERP system) can access the interfaces. For this purpose, we recommend defining an ADS user who is authorized to access the folder and who is stored as a context with the UC eBanking prime Tomcat service for this purpose.

HASH VALUES

UC eBanking prime can display the hash values in SHA256 or MD5 format when displaying the payment transaction files. This allows the user to check whether the hash value from the ERP system corresponds to the one calculated by UC eBanking prime. This effectively prevents manipulation of payment files from ERP systems.

For this purpose, the ERP system must transmit this information to the user, e.g. by printing it on supporting documents. Successful use of this function requires that the hash is generated in both systems using the identical method.

We recommend the use of a SHA256 hash value.

ENCRYPTION

UC eBanking prime can import files encrypted with AES256 via the automatic interfaces.

AES/ECB/PKCS5Padding encryption with a 256Bit key is used. The key is based on the SHA256 hash of a password defined by the customer ("PreSharedKey"). This is defined once and is not changed continuously. The password is stored in UC eBanking prime and can only be changed with admin rights.

We recommend always combining encryption with the display of the file hash value (see above).

CERTIFICATION

UC eBanking prime is audited annually by TÜV Trust IT. We will be happy to provide you with the test certificate for the current version on request.

HUMAN FACTOR

Social Engineering means an assailant is taking advantage of human characteristics to gather confidential information. In the imagination of many people internet criminals are technical masterminds programming complex codes to hack computer networks. This often is not reality. Next to classical “hacking”, meaning invading a computer by technical means such as a computer virus, there are easier ways for criminals to gain valuable information.

Why not just ask nicely?

Hard to believe but the method of “social engineering” is very promising especially in companies with above-average IT security. Assailants take advantage of human traits such as good faith, helpfulness, pride, conflict avoidance or respect for authorities to gain information using psychological tricks. A social engineering attack usually starts by gathering general information of the company which is targeted to be assailed or spied on.

Social engineering for internet criminals is a popular method to unauthorizedly gain insight on sensitive information: it is for free and overcomes even the best IT security barriers.

An organizational chart or telephone list are enough for an experienced assailant. The assailant calls the company with the knowledge of hierarchical structures. He is faking an identity to slowly give out important information using skilled questioning and psychological tricks. Often the offender takes up the role of a person of trust or authority. He collects information pieces that make him seem trustworthy in other places.

Very frequently social engineers have it in for passwords and access to banking data. The assailant fakes a problem, e.g. a hacker attack that requires immediate action to for example log-in to the banking software. The assailant presents himself sure and authoritative and imposes stress on his victim, which is chosen by psychological aspects and many times readily gives out access data.

Social engineers pretend being someone else and fake an identity. Therefore, never give out information you are not entitled to. This includes work and company organization, responsibilities, personal information of colleagues or even user data. Only give out as much information as really needed and question the requests of a caller.

Careless decisions regarding security are often taken to be polite or in situations of stress. When in doubt: security comes first, courtesy later. A process should be in place that it is not to your disadvantage to reassure with your superiors even if it means an important customer or manager may have to wait.

Never keep written notes and correspondence in plain sight on your desks but protect information from third parties. Always store sensitive data encrypted on your computer. Even from apparently unimportant information crucial conclusions can be drawn in combination with other facts. Avoid talking about business matters in public places such as trains or restaurants.

Further information and recent examples on the topic of Social Engineering can be found on our website for this purpose: http://www.hvb.de/ceo-fraud

SUPPORT

At having the suspicion of:

- Someone having unauthorized access to your account
- Having lost access credentials by accident, theft, or unauthorized copy
- Being victim of a CyberCrime Attack

Or questions regarding data safety in general or to this brochure please contact our Helpdesk at:

gtb-center@unicredit.de