Security Instruction for the My HCOB Portal

Version April 2026

Hamburg Commercial Bank

CONTENTS **PAGE**

1 General information about the My HCOB Portal

Unlike a locally installed application, the My HCOB Portal is provided centrally by Hamburg Commercial Bank AG (hereinafter "HCOB") for numerous users. Access is exclusively via a web browser, in which all functions of the portal can be carried out.

If cookies are stored, it is recommended that you delete them regularly.

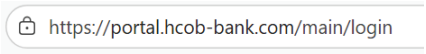
The access rights assigned for the My HCOB Portal must be reviewed regularly and adapted to changing circumstances. In particular, the access rights of former employees must be deleted, and the assigned access rights must be reviewed in the event of changes to the signing and approval rights of individual employees.

If your organisation requires a particularly high level of security, access to the My HCOB Portal should be restricted to a limited group of people.

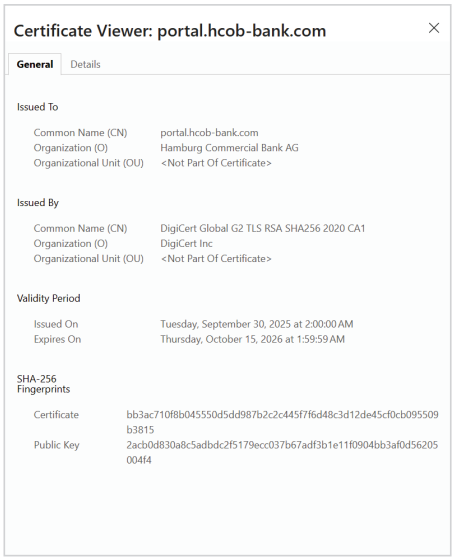
1.1 Accessing the My HCOB Portal

Data communication between the customer and HCOB takes place via an https connection encrypted using TLS. In common web browsers, such a secure connection is typically indicated by a symbol, such as a small padlock in the address bar. Before entering confidential information – particularly your password – you should always check that the displayed web address is correct and that encryption is active. Below is an example from the Edge browser.

https://portal.hcob-bank.com/main/login



The security certificate used for the portal must be issued to HCOB and signed by a trusted certification authority. To ensure that the connection has been established with the intended server, you can view the certificate yourself. To do this, double-click the padlock icon displayed in your browser's status bar.



When accessing the My HCOB Portal address, no browser warnings regarding certificate or trust issues should appear. If your browser nevertheless reports that the security certificate used is invalid or that the connection cannot be trusted, do not continue using the portal and contact our Technical Hotline immediately on +49 40 3333-23420 or by email at TechnHotline@hcob-bank.com.

The My HCOB Portal should always be accessed via a secure internet connection. Due to an increased security risk, we advise against connecting to the My HCOB Portal via open or unknown Wi-Fi networks, such as those provided in internet cafés.

1.2 Single Sign-On (SSO)

Once you have successfully logged in to the My HCOB Portal, the applications authorised for you will be immediately available without the need to log in again (single sign-on procedure).

If further authorisation is required for certain functions (e.g. when submitting electronic declarations), this is also carried out using the security medium used for logging in.

1.3 Automatic logout

For your protection, a session will be automatically terminated if there is no activity for a period of 30 minutes. You can log in to the My HCOB Portal again at any time.

2 Secure password

Passwords should always be of sufficient length and complexity to ensure effective protection. If you suspect that unauthorised persons may have gained knowledge of your password, you must change it immediately. You should also check whether access needs to be blocked. Furthermore, it is advisable never to use identical or only slightly modified passwords for different applications or accounts.

Guidance on secure password practices is provided by the recommendation of the Federal Office for Information Security (BSI), available at:

https://www.bsi-fuer-buerger.de/

When assigning passwords in the My HCOB Portal, the system automatically checks whether the specified minimum requirements are met. The minimum requirements are set by the HCOB and may change if necessary.

To avoid the risk of passwords being spied on, they must not be stored in plain text on the computer (e.g. in files) or written down by hand on notepads.

3 Computer security

3.1 Secure operating system

The operating system and all additional installed programmes – such as browsers or PDF applications – should be updated regularly. Updates should only be carried out using the official update functions provided by the respective manufacturers.

3.2 Secure browser

Use only standard web browsers and install security updates promptly via the update functions provided. Additional browser extensions should be avoided unless their use is necessary. If extensions are required, they should only be enabled for trusted websites.

If the browser you use has built-in protection mechanisms – such as against phishing or malware – these functions must always remain enabled.

Information on security settings for various browsers can be found at www.bsi.bund.de.

3.3 Up-to-date antivirus software

The use of up-to-date antivirus software is essential. Ensure that the programme is updated regularly. In addition, the computer should undergo a full system scan using the antivirus software at regular intervals.

Ensure that the antivirus software also monitors the web browser you use for malicious websites or downloads.

4 Two-factor authentication

With two-factor authentication, a user's identity is verified using two independent forms of proof. These can be a combination of different categories, such as a knowledge-based factor (e.g. a password), a possession-based factor (such as a mobile device or a key file), or a biometric factor (e.g. a fingerprint or facial recognition).

4.1 My HCOB Portal App

4.1.1 Authentication and authorisation using mobile devices

The My HCOB Portal App serves as a standalone security component and provides the private keys required for user authentication and for approving electronic declarations – such as for payments or administrative changes.

Access to the My HCOB Portal is only possible if the user is in possession of the authorised mobile device and authenticates themselves in the app using a password or biometric identifier (e.g. fingerprint or facial recognition). Only the combination of device and authentication method enables the use of the My HCOB Portal.

Logging in

To log in to the My HCOB Portal, the user uses their mobile device on which the My HCOB Portal App has been previously installed and set up. After opening the portal, the user is shown an access code, which can either be entered manually into the app or conveniently scanned via a QR code.
In the next step, the user sets a secure password (see notes on password security). Optionally, biometric authentication such as Face ID or Touch ID can also be enabled.

Once the code entered has been successfully verified, secure access to the My HCOB Portal is established and the user can start using the available functions.

Security
All HCOB apps detect if a device has been modified by jailbreaks, rootkits or similar modifications. In such cases, for security reasons, all data and keys stored in the app are immediately deleted.

The information stored in the My HCOB Portal App is encrypted on a device-specific basis and is therefore permanently linked to the respective mobile device. If you change devices, the app must be completely set up again; the new device is authorised via the previously used device. You can find instructions on how to do this on our website.

For security reasons, it is not possible to use the app simultaneously on multiple devices with the same personal login details.

To protect your data, the app automatically deletes all content stored within it after five consecutive failed attempts to enter your password.

The app can only be set up if a device password or biometric lock is enabled on the mobile device.

Download
Google Play Store for Android:
https://play.google.com/store/apps/details?id=de.hcob.mobiletoken

Apple App Store for iPhone:
https://apps.apple.com/de/app/hcob-portal/id6737806133

4.1.2 Authentication and authorisation using desktop version

The My HCOB Desktop App is a comprehensive security application that stores the private keys required for user authentication and for authorising electronic transactions, such as payments or administrative changes. This shifts the security-critical part of the process to a separate channel.

The My HCOB Desktop App is device-specific. Users can only access the My HCOB Portal if they have access to the relevant device and know the associated password.

Logging in
To log in to the My HCOB Portal, the user uses a desktop PC or laptop on which the My HCOB Portal Desktop App has been previously installed and set up. The latest versions of the Windows and macOS operating systems are supported. The user then logs in to the app by entering a personal password.

Security
Upon launch, the My HCOB Portal Desktop App automatically checks whether the device being used meets the necessary security requirements. If these requirements are not met, the application will not run for security reasons.

All data stored in the My HCOB Portal Desktop App is encrypted on a device-specific basis and is therefore permanently linked to the respective device. If you change devices, the app must therefore be completely set up again. As part of this process, the new device is authorised by the previously used device. You can find instructions for this on our website.

It is not possible to set up the app simultaneously on multiple devices using a user's personal login details.

To protect your data, the app is automatically reset after five consecutive failed attempts to enter the password, thereby deleting any data stored in the app.

Download
Download for Windows:
https://www.hcob-bank.com/content/uploads/apps/desktop/HCOB_Token.exe

Download for iOS:
https://www.hcob-bank.com/content/uploads/apps/desktop/HCOB_Token.dmg

5 Responsible handling of data and programmes

To ensure effective protection of sensitive information, you should implement organisational, technical and personnel-related security measures. These include, amongst other things, access control, the use of firewalls, authorisation management, and the monitoring and logging of security-related processes. Up-to-date and reliable protection against malware is essential.

In addition, you should establish a regulated process for installing software and take precautions to protect the company network. To ensure that security procedures for protecting exchanged data are fully effective, appropriate precautions are also required within your technical environment. Guidance and, in particular, the latest updates on basic security can be found at http://www.bsi.bund.de/.

6 Mobile devices

New vulnerabilities are constantly being discovered on smartphones and tablets that can be exploited by attackers. To protect your device, both the operating system and installed apps should always be kept up to date. Install available updates promptly and ensure you only use official update sources. The basic security rules that apply to computers apply equally to mobile devices.

The greatest risk is the loss of the device. If lost, you should immediately change all passwords and, where possible, use a remote access function to delete the data on the device or lock the device. You should also check whether access needs to be blocked.

Do not leave your smartphone unattended whilst the My HCOB Portal is open, and ensure that no one can see what you are typing.

Apps should only be downloaded from official sources such as the Apple App Store or the Google Play Store. Check the permissions and privacy settings of each app, as well as external reviews.

You should also be cautious with links sent via text message, email or in the form of a QR code. Only open links from reliable sources.

Disable features such as internet access, Bluetooth, infrared, Wi-Fi or NFC when you are not using them.

Before selling, passing on or disposing of your smartphone, all data should be completely deleted.

Manufacturers regularly release service and security updates. Check the relevant websites for information on these.

Modifications to the operating system such as 'jailbreaks', 'custom ROMs' or 'rooting' should be avoided at all costs. They may contain hidden code that allows attackers to intercept data traffic from banking apps.

7 Software installation

The installation and maintenance of software should always be carried out in accordance with a clearly defined and controlled procedure. This may include, for example, granting administrator rights only on a temporary basis and documenting all steps taken in a traceable manner.

If the bank's software is set up by external service providers, only specifically designated technical access points should be used for the setup, and these should be deactivated immediately once the work is complete.

To further enhance security, both the authorisation and the execution of the installation should follow the dual control principle and be logged. The workstations and access routes required for this – for example, for remote maintenance software – should also be clearly defined and monitored in advance.

8 EBICS Token (key file)

8.1 Authorising payments and changes using EBICS Token (key file)

To confirm payments or administrative changes in electronic banking, users first select the transactions they wish to approve. Authorisation can then be carried out using the EBICS Token. The token is a digital key file in the format of a standard Keybag.dat file and complies with the requirements of the EBICS specification issued by the German Banking Industry Committee.

The EBICS Token is stored as a software key in a file and is additionally protected by a password. The key must be kept secure and protected against unauthorised access.

If key files are stored on central storage media, there is a risk that other people – such as administrators – may be able to access them. Care should be taken to ensure that removable media containing key files are not left lying around or forgotten in the device, as key files can be copied.

For this reason, key files should not be stored on stationary drives (local hard drives, network drives). It is recommended that they be stored exclusively on secure removable media, which should be removed immediately after use and kept safe from theft and misuse.

Security media containing key files should not be used for other purposes, such as general data storage. Access to the media and to the software keys stored on it must always be password-protected. Electronic banking itself also requires a password to access the keys.

The creation and regular updating of passwords should form part of your internal security policies.

After their last use, security media that are no longer required should be properly destroyed or securely disposed of.

8.2 Blocking keys in the event of suspected misuse or theft

If there are signs that a key has been lost, misused or copied, you should inform your bank immediately. In such a case, have the relevant access to the My HCOB Portal and electronic banking blocked immediately to prevent any potential damage.

You can change your key at any time, whereby your previous key is replaced with a new one.

9 Human factor

Attackers often attempt to exploit human behaviour in a targeted manner to gain access to confidential information (so-called 'social engineering'). Raise awareness and train your staff about these tactics to ensure that no confidential information is passed on to unauthorised third parties.

10 Support

Please contact our technical helpline immediately if you suspect that:

- Unauthorised persons have gained or may gain access to your account,
- your login details have been lost, stolen or may have been copied,
- you have been the target of a cyber attack,

or if you have general questions regarding security or the contents of this document. You can contact our representatives on:

Telephone (within Germany): 0800 3273001 – free of charge
Telephone (international): +49 40 3333 23420
Monday to Friday 8:00 am to 5:30 pm, except on public holidays and on 24 and 31 December

Hamburg Commercial Bank AG
Gerhart-Hauptmann-Platz 50
20095 Hamburg, Germany
Telefon +49 40 3333-0
Fax +49 40 3333-34001
info@hcob-bank.com