Sicherheitshinweise zum My HCOB Portal

Version April 2026

Hamburg Commercial Bank

INHALT **SEITE**

1 Allgemeines zum My HCOB Portal

Im Gegensatz zu einer lokal installierten Anwendung wird das My HCOB Portal zentral durch die Hamburg Commercial Bank AG (im Folgenden „HCOB“) für zahlreiche Nutzer bereitgestellt. Der Zugriff erfolgt ausschließlich über einen Webbrowser, in dem sämtliche Funktionen des Portals ausgeführt werden können.

Wenn Cookies gespeichert werden, wird empfohlen diese regelmäßig zu löschen.

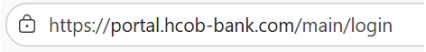
Die für das My HCOB Portal vergebenen Zugriffsrechte sind regelmäßig zu überprüfen und an veränderte Rahmenbedingungen anzupassen. Insbesondere sind die Berechtigungen ausgeschiedener Mitarbeitender zu löschen sowie die vergebenen Berechtigungen bei Änderungen von Zeichnungs- und Freigaberechten einzelner Mitarbeitender zu überprüfen.

Falls für Ihr Unternehmen ein besonders hohes Sicherheitsniveau erforderlich ist, sollte der Zugang zum My HCOB Portal nur einem eingeschränkten Personenkreis gewährt werden.

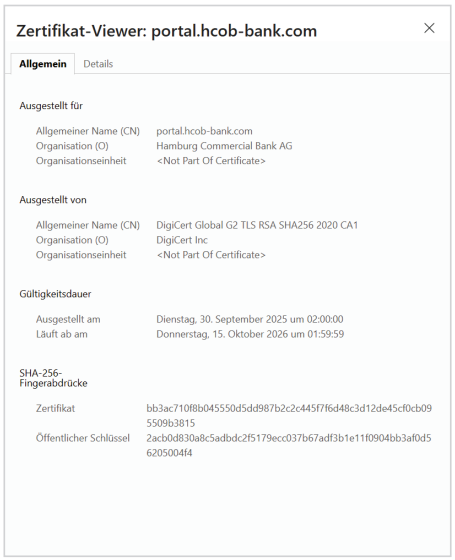
1.1 Aufruf von My HCOB Portal

Die Datenkommunikation zwischen Kunde und HCOB findet über eine per TLS verschlüsselte https-Kommunikation statt. In gängigen Webbrowsern wird eine solche gesicherte Verbindung typischerweise anhand eines Symbols angezeigt, beispielsweise einem kleinen Schloss in der Adresszeile. Bevor Sie vertrauliche Informationen – insbesondere Ihr Passwort – eingeben, sollten Sie stets überprüfen, ob die angezeigte Internetadresse korrekt ist und die Verschlüsselung aktiv besteht. Unten sehen Sie ein Beispiel aus dem Edge Browser.

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



Das für die Portalnutzung eingesetzte Sicherheitszertifikat muss auf die HCOB – ausgestellt und von einer vertrauenswürdigen Zertifizierungsstelle signiert sein. Um sicherzustellen, dass die Verbindung tatsächlich mit dem vorgesehenen Server hergestellt wurde, können Sie das verwendete Zertifikat selbst einsehen. Klicken Sie dazu in der Statusleiste Ihres Browsers doppelt auf das angezeigte Schloss-Symbol.



Beim Aufruf der My HCOB Portal-Adresse dürfen keine Warnhinweise des Browsers zu Zertifikats- oder Vertrauensproblemen erscheinen. Sollte Ihr Browser dennoch melden, dass das verwendete Sicherheitszertifikat ungültig ist oder der Verbindung nicht vertraut werden kann, nutzen Sie das Portal nicht weiter und wenden Sie sich umgehend an unsere Technische Hotline unter +49 40 3333-23420 oder per E-Mail an TechnHotline@hcob-bank.com.

Das My HCOB Portal sollte grundsätzlich über einen sicheren Internetzugang genutzt werden. Es wird aufgrund eines erhöhten Sicherheitsrisikos davon abgeraten über offene oder unbekannte WLAN-Netzwerke, wie sie beispielsweise in Internetcafés bereitgestellt werden, eine Verbindung zum My HCOB Portal aufzubauen.

1.2 Single-Sign-On (SSO)

Nach Ihrer erfolgreichen Anmeldung im My HCOB Portal stehen Ihnen die für Sie freigeschalteten Anwendungen ohne erneute Anmeldung unmittelbar zur Verfügung (Single-Sign-On-Verfahren).

Falls für bestimmte Funktionen eine weitergehende Autorisierung notwendig ist (z. B. bei der Abgabe elektronischer Erklärungen), erfolgt diese ebenfalls mit dem für die Anmeldung genutzten Sicherheitsmedium.

1.3 Automatisches Abmelden

Zu Ihrem Schutz wird eine Sitzung automatisch beendet, wenn über einen Zeitraum von 30 Minuten keine Aktivität erfolgt. Sie können sich jederzeit erneut im My HCOB Portal anmelden.

2 Sicheres Passwort

Passwörter sollten grundsätzlich eine ausreichende Länge und Komplexität aufweisen, um einen wirksamen Schutz zu gewährleisten. Wenn der Verdacht besteht, dass Unbefugte Kenntnis von Ihrem Passwort erlangt haben könnten, ist ein sofortiger Passwortwechsel zwingend erforderlich. Zudem sollte geprüft werden, ob eine Sperrung des Zugangs erforderlich ist. Darüber hinaus empfiehlt es sich, für unterschiedliche Anwendungen oder Zugänge niemals identische oder lediglich minimal abgeänderte Passwörter zu verwenden.

Eine Orientierung zu sicheren Passwortpraktiken bietet die Empfehlung des Bundesamts für Sicherheit in der Informationstechnik (BSI), abrufbar unter:

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

Bei der Vergabe von Passwörtern im My HCOB Portal, wird automatisch geprüft, ob bei der Vergabe die vorgegebenen Mindestanforderungen erfüllt sind. Die Mindestanforderungen werden durch die HCOB vorgegeben und können sich, wenn erforderlich, ändern.

Um das Risiko des Ausspähens zu vermeiden, dürfen Passwörter weder im Klartext auf dem Computer (z. B. in Dateien) noch handschriftlich auf Notizzetteln abgelegt werden.

3 Sicherheit des Rechners

3.1 Sicheres Betriebssystem

Das Betriebssystem sowie alle zusätzlich installierten Programme – beispielsweise Browser oder PDF-Anwendungen – sollten regelmäßig auf den neuesten Stand gebracht werden. Die Aktualisierung sollte ausschließlich über die offiziellen Updatefunktionen der jeweiligen Hersteller erfolgen.

3.2 Sicherer Browser

Verwenden Sie ausschließlich marktübliche Webbrowser und installieren Sie Sicherheitsupdates zeitnah über die bereitgestellten Updatefunktionen. Auf zusätzliche Browser-Erweiterungen sollte verzichtet werden, sofern deren Einsatz nicht zwingend erforderlich ist. Falls Erweiterungen benötigt werden, sollten diese nur für vertrauenswürdige Webseiten aktiviert werden.

Sofern der von Ihnen eingesetzte Browser über integrierte Schutzmechanismen – etwa gegen Phishing oder Schadsoftware – verfügt, sollten diese Funktionen unbedingt aktiviert bleiben.

Hinweise zu Sicherheitseinstellungen verschiedener Browser finden sich unter www.bsi.bund.de.

3.3 Aktueller Virenscanner

Der Einsatz einer aktuellen Antiviren-Software ist zwingend erforderlich. Achten Sie darauf, dass das Programm regelmäßig aktualisiert wird. Zusätzlich sollte der Computer in regelmäßigen Abständen einer vollständigen Systemprüfung durch die Antivirensoftware unterzogen werden.

Stellen Sie sicher, dass die Antivirensoftware auch den genutzten Webbrowser in Bezug auf schädliche Webseiten oder Downloads überwacht.

4 Zwei-Faktor-Authentifizierung

Bei der Zwei-Faktor-Authentifizierung wird die Identität eines Nutzers durch zwei voneinander unabhängige Nachweise bestätigt. Dabei können verschiedene Kategorien kombiniert werden, etwa ein Wissenselement (z. B. ein Passwort), ein Besitzmerkmal (wie ein mobiles Gerät oder eine Schlüsseldatei) oder ein biometrisches Kennzeichen (z. B. Fingerabdruck oder Gesichtserkennung).

4.1 My HCOB Portal App

4.1.1 Authentifizierung und Autorisierung mit mobilen Endgeräten

Die My HCOB Portal App dient als eigenständige Sicherheitskomponente und stellt die privaten Schlüssel bereit, die für die Benutzerauthentifizierung sowie für die Freigabe elektronischer Erklärungen – etwa für Zahlungen oder administrative Änderungen – benötigt werden.

Der Zugriff auf das My HCOB Portal ist nur möglich, wenn sich der Nutzer im Besitz des autorisierten mobilen Endgeräts befindet und sich per Passwort oder biometrischem Merkmal (z. B. Fingerabdruck oder Gesichtserkennung) in der App authentifiziert. Erst die Kombination aus Gerät und Authentifizierungsmerkmal ermöglicht die Nutzung des My HCOB Portals.

Anmelden
Für die Anmeldung am My HCOB Portal nutzt der Anwender sein mobiles Endgerät, auf dem die My HCOB Portal App zuvor installiert und eingerichtet wurde. Nach dem Aufruf des Portals wird dem Nutzer ein Zugangscode angezeigt, der entweder manuell in der App eingegeben oder bequem per QR Code gescannt werden kann.

Im nächsten Schritt legt der Nutzer ein sicheres Passwort fest (siehe Hinweise zur Passwortsicherheit). Optional kann zusätzlich eine biometrische Authentifizierung wie Face ID oder Touch ID aktiviert werden.

Sobald der eingegebene Code erfolgreich geprüft wurde, ist der sichere Zugang zum My HCOB Portal hergestellt und der Nutzer kann mit den bereitgestellten Funktionen arbeiten.

Sicherheit
Alle Apps der HCOB erkennen, wenn ein Gerät durch Jailbreaks, Rootkit oder ähnliche Modifikationen verändert wurde. In solchen Fällen werden aus Sicherheitsgründen sämtliche in der App gespeicherten Daten und Schlüssel sofort gelöscht.

Die in der My HCOB Portal App abgelegten Informationen sind gerätespezifisch verschlüsselt und dadurch fest an das jeweilige mobile Endgerät gebunden. Bei einem Gerätewechsel muss die App vollständig neu eingerichtet werden; das neue Gerät wird dabei über das zuvor verwendete Gerät autorisiert. Eine entsprechende Anleitung finden Sie auf unserer Homepage.

Eine parallele Nutzung der App mit denselben persönlichen Zugangsdaten auf mehreren Endgeräten ist aus Sicherheitsgründen nicht möglich.

Zum Schutz der Daten löscht die App nach fünf aufeinanderfolgenden Fehlversuchen bei der Passworteingabe automatisch alle in der App gespeicherten Inhalte.

Die App kann nur eingerichtet werden, wenn auf dem mobilen Endgerät ein Gerätepasswort oder eine biometrische Sperre aktiviert ist.

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

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

4.1.2 Authentifizierung und Autorisierung mit der Desktop-Version

Die My HCOB Desktop App ist eine vollständige Sicherheitsanwendung, die die erforderlichen privaten Schlüssel für die Benutzerauthentifizierung und für die Autorisierung von elektronischen Erklärungen, wie Zahlungen oder administrativen Modifikationen bereithält. Dadurch wird der sicherheitskritische Teil des Prozesses auf einen separaten Kanal ausgelagert.

Die My HCOB Desktop App ist gerätegebunden. Nur wenn der Nutzer Zugriff auf das entsprechende Gerät hat und das zugehörige Passwort kennt, kann er das My HCOB Portal nutzen.

Anmelden
Für die Anmeldung am My HCOB Portal nutzt der Anwender einen Desktop PC oder Laptop, auf dem zuvor die My HCOB Portal Desktop App installiert und eingerichtet wurde. Unterstützt werden die jeweils aktuellen Versionen der Betriebssysteme Windows und macOS. Der Login in die App erfolgt anschließend durch die Eingabe eines persönlichen Passworts.

Sicherheit
Die My HCOB Portal Desktop App überprüft beim Start automatisch, ob das verwendete Gerät den erforderlichen Sicherheitsanforderungen erfüllt. Sind diese Voraussetzungen nicht gegeben, wird die Anwendung aus Sicherheitsgründen nicht ausgeführt.

Alle in der My HCOB Portal Desktop App gespeicherten Daten sind gerätespezifisch verschlüsselt und damit fest an das jeweilige Endgerät gebunden. Bei einem Gerätewechsel muss die App daher vollständig neu eingerichtet werden. Das neue Gerät wird im Zuge dessen durch das vorher genutzte Gerät autorisiert. Eine Anleitung hierzu finden Sie auf unserer Homepage.

Eine gleichzeitige Einrichtung der App mit den persönlichen Zugangsdaten eines Nutzers auf mehreren Geräten ist nicht möglich.

Zum Schutz Ihrer Daten wird die App nach fünf aufeinanderfolgenden Fehlversuchen bei der Passworteingabe automatisch zurückgesetzt und löscht dabei in der App gespeichert Daten.

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

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

5 Verantwortungsbewusster Umgang mit Daten und Programmen

Für einen wirksamen Schutz sensibler Informationen sollten Sie organisatorische, technische und personelle Sicherheitsmaßnahmen treffen. Dazu zählen unter anderem ein Zugangs- und Zugriffsschutz, der Einsatz von Firewalls, ein Berechtigungsmanagement sowie die Überwachung und Protokollierung von sicherheitsrelevanten Vorgängen. Ein aktueller und zuverlässiger Schutz vor Schadsoftware ist dabei unverzichtbar.

Darüber hinaus sollten Sie einen geregelten Prozess zur Installation von Software und Vorkehrungen zum Schutz des Unternehmensnetzwerkes treffen. Damit die Sicherheitsverfahren zum Schutz der ausgetauschten Daten Ihre volle Wirkung entfalten können, sind auch in Ihrer technischen Umgebung entsprechende Vorkehrungen erforderlich. Hinweise und insbesondere aktuelle Meldungen zur Basissicherheit finden sich unter http://www.bsi.bund.de/.

6 Mobile Endgeräte

Auf Smartphones und Tablets werden fortlaufend neue Schwachstellen entdeckt, die von Angreifern ausgenutzt werden können. Um Ihr Gerät zu schützen, sollten sowohl das Betriebssystem als auch installierte Apps stets aktuell gehalten werden. Installieren Sie verfügbare Updates zeitnah und achten Sie darauf, nur offizielle Aktualisierungsquellen zu nutzen. Die grundlegenden Sicherheitsregeln, die für Computer gelten, treffen gleichermaßen auf mobile Endgeräte zu.

Das größte Risiko stellt der Verlust des Endgeräts dar. Bei Verlust sollten Sie unverzüglich alle Passwörter ändern und, sofern möglich, über eine Fernzugriffsfunktion die Daten auf dem Gerät löschen oder das Gerät sperren. Zudem sollte geprüft werden, ob eine Sperrung des Zugangs erforderlich ist.

Lassen Sie Ihr Smartphone nicht unbeaufsichtigt, wenn das My HCOB Portal geöffnet ist, und achten Sie darauf, dass niemand Ihre Eingaben mitverfolgen kann.

Apps sollten ausschließlich aus offiziellen Quellen wie dem Apple App Store oder dem Google Play Store heruntergeladen werden. Prüfen Sie die Berechtigungen und Datenschutzeinstellungen jeder App sowie externe Bewertungen.

Seien Sie zudem vorsichtig mit Links, die per SMS, E-Mail oder in Form eines QR Codes bereitgestellt werden. Öffnen Sie ausschließlich Links aus verlässlichen Quellen.

Deaktivieren Sie Funktionen wie Internetzugang, Bluetooth, Infrarot, WLAN oder NFC, wenn Sie diese nicht nutzen.

Vor dem Verkauf, der Weitergabe oder Entsorgung Ihres Smartphones sollten sämtliche Daten vollständig gelöscht werden.

Hersteller veröffentlichen regelmäßig Service und Sicherheitsupdates. Informieren Sie sich dazu auf den entsprechenden Webseiten.

Modifikationen des Betriebssystems wie „Jailbreaks“, „Custom ROMs“ oder „Rooting“ sollten unbedingt vermieden werden. Sie können versteckten Code enthalten, der Angreifern ermöglicht, Datenverkehr von Banking Apps auszulesen.

7 Sofwareinstallation

Die Installation sowie die Pflege von Software sollte stets in einem klar definierten und kontrollierten Verfahren erfolgen. Dazu kann beispielsweise gehören, Administratorrechte nur vorübergehend zu vergeben und alle durchgeführten Schritte nachvollziehbar zu dokumentieren.

Wird Software der Bank durch externe Dienstleister eingerichtet, sollten für die Einrichtung ausschließlich speziell vorgesehene technische Zugänge genutzt werden, die nach Abschluss der Arbeiten unverzüglich wieder deaktiviert werden.

Um die Sicherheit zusätzlich zu erhöhen, sollte sowohl die Genehmigung als auch die Durchführung der Installation nach dem Vier Augen Prinzip erfolgen und protokolliert werden. Auch die dafür benötigten Arbeitsplätze und Zugangswege – beispielsweise für Fernwartungssoftware – sollten im Vorfeld eindeutig festgelegt und überwacht werden.

8 EBICS Token (Schlüsseldatei)

8.1 Zahlungen und Änderungen mit EBICS Token (Schlüsseldatei) autorisieren

Um Zahlungen oder administrative Änderungen im Electronic Banking zu bestätigen, wählen Nutzer zunächst die gewünschten Vorgänge aus, die sie freigeben möchten. Die Autorisierung kann anschließend über den EBICS Token erfolgen. Der Token ist eine digitale Schlüsseldatei im Format einer klassischen Keybag.dat Datei und folgt den Vorgaben der EBICS Spezifikation der Deutschen Kreditwirtschaft.

Der EBICS Token wird als Softwareschlüssel in einer Datei gespeichert und zusätzlich durch ein Passwort geschützt. Der Schlüssel muss sicher aufbewahrt und vor unbefugtem Zugriff geschützt werden.

Werden Schlüsseldateien auf zentralen Speichermedien abgelegt, besteht die Möglichkeit, dass andere Personen – beispielsweise Administratoren – darauf zugreifen können. Es sollte darauf geachtet werden, dass Wechseldatenträger, die Schlüsseldateien enthalten, nicht offen liegen gelassen oder im Gerät vergessen werden, weil Schlüsseldateien kopiert werden können.

Aus diesem Grund sollten Schlüsseldateien nicht auf stationären Laufwerken (lokale Festplatten, Netzlaufwerke) gespeichert werden. Empfehlenswert ist die Aufbewahrung ausschließlich auf sicheren Wechseldatenträgern, die nach Gebrauch unmittelbar entnommen und geschützt vor Diebstahl und missbräuchliche Nutzung verwahrt werden.

Sicherheitsmedien, die Schlüsseldateien enthalten, sollten nicht für andere Zwecke, wie die allgemeine Datenspeicherung, genutzt werden. Der Zugriff auf das Medium sowie auf die darauf abgelegten Softwareschlüssel muss stets durch ein Passwort abgesichert sein. Auch das Electronic Banking selbst erfordert für den Zugriff auf die Schlüssel eine Passwortabfrage.
Die Erstellung und regelmäßige Aktualisierung von Passwörtern sollte Teil Ihrer internen Sicherheitsrichtlinien sein.

Nach der letzten Nutzung sollten Sicherheitsmedien, die nicht mehr benötigt werden, fachgerecht vernichtet oder sicher entsorgt werden.

8.2 Sperrung von Schlüsseln bei Verdacht auf Missbrauch oder Diebstahl

Sollten Anzeichen dafür bestehen, dass ein Schlüssel verloren gegangen ist oder missbraucht oder kopiert wurde, sollten Sie unverzüglich Ihre Bank informieren. Lassen Sie in einem solchen Fall die betroffenen Zugänge zum My HCOB Portal sowie zum Electronic Banking umgehend sperren, um möglichen Schaden zu verhindern.

Sie können jederzeit einen Schlüsselwechsel durchzuführen, durch den Ihr bisheriger Schlüssel durch einen neuen ersetzt wird.

9 Faktor Mensch

Häufig versuchen Angreifer menschliche Verhaltensweisen gezielt ausnutzen, um an vertrauliche Informationen zu gelangen (sog. „Social Engineering“). Sensibilisieren und schulen Sie Ihr Personal für diese Vorgehensweisen, damit keine vertraulichen Informationen an unbefugte Dritte weitergegeben werden.

10 Support

Bitte wenden Sie sich umgehend an unsere Technische Hotline, wenn Sie den Verdacht haben, dass:

- Unbefugte Zugriff auf Ihr Konto erhalten haben oder erhalten könnten,
- Ihre Zugangsdaten verloren gegangen, entwendet oder möglicherweise kopiert wurden,
- Sie Ziel eines Cyberangriffs geworden sind,

oder wenn Sie allgemeine Fragen zur Sicherheit oder zu den Inhalten dieses Dokuments haben.

Unsere Ansprechpartner erreichen Sie unter:
Telefon (Inland): 0800 3273001 – kostenfrei
Telefon (Ausland): +49 40 3333 23420
Montag bis Freitag 8:00 Uhr bis 17:30 Uhr, außer an gesetzlichen Feiertagen sowie dem 24. und 31.12.

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