Raiffeisen Bank International

CMI Business Banking

Security Information

Content

Raiffeisen Bank International

1 General safety information

1.1 Protect your data

- Please handle your data with care.
- Never pass on your personal access and authorisation data, such as your user name and password, to third parties.
- Make sure that no one is watching you entering your personal information.
- Never store your personal password on your end device (PC, laptop, mobile phone).
- Please keep in mind, that we will never ask you about your login credentials or other seinsitive data – no matter which communication channel (Email, SMS, Telephone,...).

1.2 Use a secure password

- Do not choose simple or easily comprehensible combinations for your personal password (such as names, places, date of birth).
- Keep to the predefined criteria for creating your personal password.
- Change your personal password regularly and do not use the same password for different applications.

1.3 System security

- Use only trusted and maintained devices.
- Use up-to-date virus protection.
- Use a firewall to protect your device.

2 CMI security solution

2.1 General information

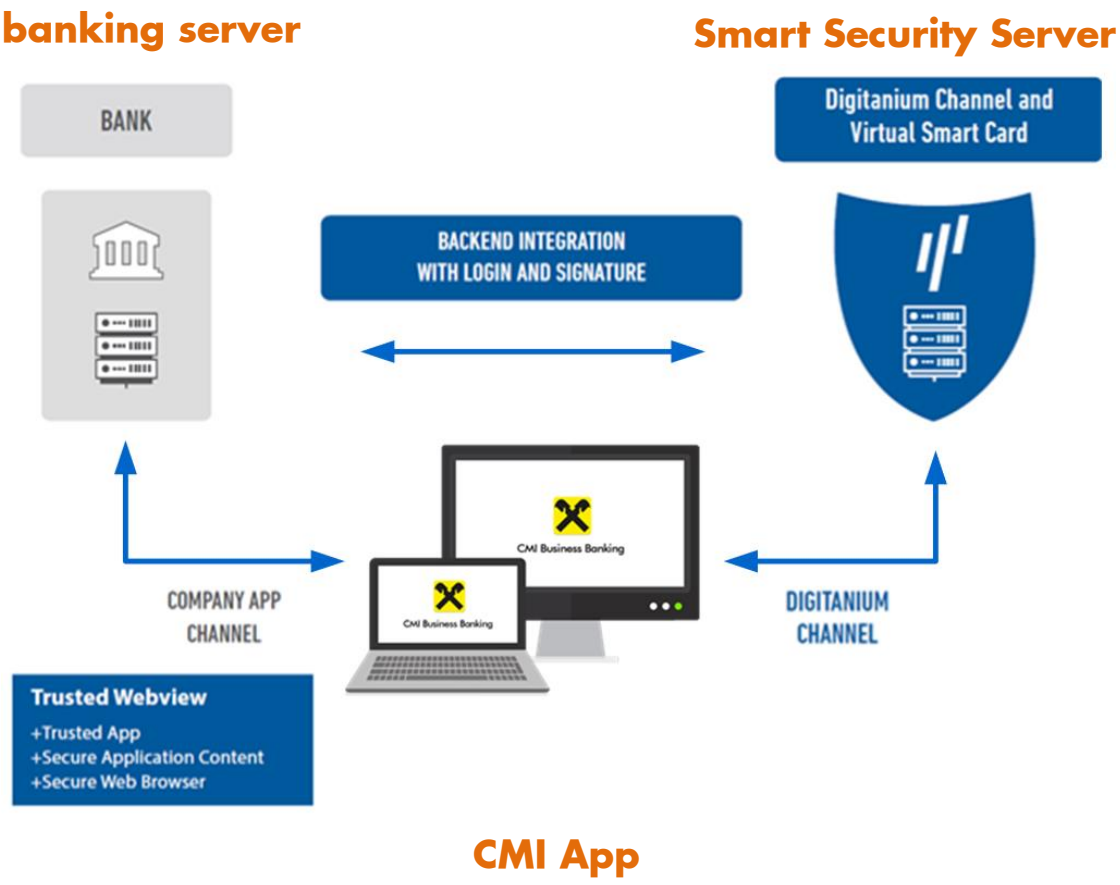
CMI uses a modern and secure multi-factor authentication solution for corporate e-banking. The solution meets the latest security standards and all EU / PSD2 requirements for strong customer authentication.

PSD2 compliant

Our technical and organisational protection mechanisms are continuously updated and audited by independent auditors.

On the following pages the basic technology and the functional principles are presented, in addition the most important safety features of the solution are described.

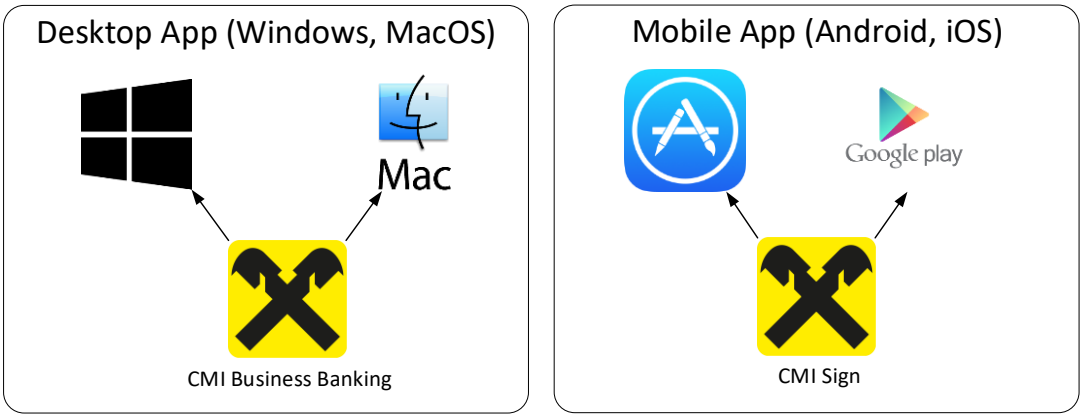
2.2 7-Layer Security



2.3 Operating principle

2.3.1 Access via App

Customer access to CMI@Web / FAST@Web is not via a browser or additional hardware, but via a specially hardened app provided for various platforms.



- The desktop apps do not require any installation or administration rights on the client. The distribution takes place via download link from the RBI CM Support Desk.
- The mobile apps must be downloaded and installed from the respective store.

Desktop App

Mobile App

App Download Page:

https://auth.rbinternational.com/Update/

2.3.2 Device binding

The app must be activated during the onboarding process and is bound to the respective device (PC, laptop, mobile device). The CMI access is therefore always limited to this device. Via the Self-Service, please use the menu item "Administration > Add new device", additional devices can be activated at any time to use CMI.

Device binding

2.3.3 Secure App Communication

The app's comprehensive security mechanisms ensure secure communication and strict separation of security channel and data channel. In addition, there is an authorization system on the bank side that secures the connection between the client app and the e-banking server.

1 App / 2 Channels

2.3.4 App Login & Signature with password

During the activation, the customer assigns a personal password, which is then used both for login and for the transaction signature. Due to additional security mechanisms, the use of additional hardware is not necessary.

Secure Login & Signature

Further details on individual security features are described in the next chapter.

2.4 Safety aspects

CMI's authorization solution uses several security mechanisms. Some of them are shown in the following list. For security reasons, we can not provide any further details on the technical implementation of these protective measures.

2.4.1 Security mechanisms at a glance:

- Secure activation process
- App device binding to the hardware
- App integrity check
- Virtuals smartcard
- Secure and encrypted identity storage
- PKI-based processes
- Server-based security checks
- 2-channel technology / separate security channel
- Multifactor authentication for login + signature
- Trusted webview for application content
- Certificate pinning
- URL whitelisting
- Anti debugging
- Anti reverse engineering
- Anti code injection
- Jailbreak / Rooting / Malicious app detection
- Static & dynamic manipulation protection
- Client risk rating
- Biometrics support: Fingerprint, Touch ID, Face ID
- Optional security levels for signature + self service

2.4.2 Secure „Onboarding“

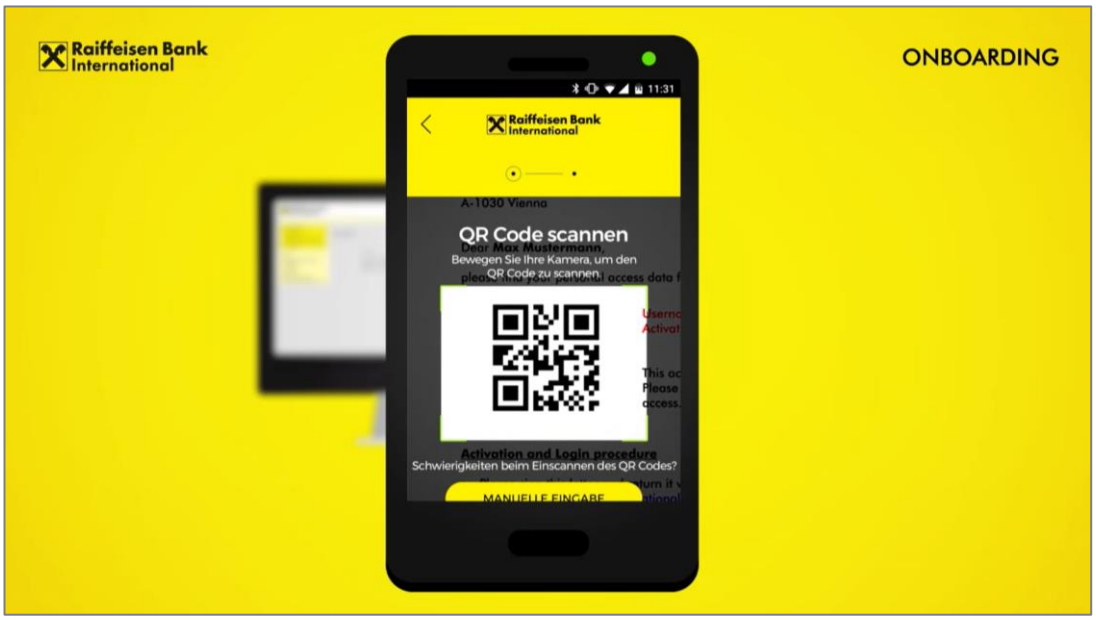
An activation code is required to activate the app. After the conclusion of the customer contract and the creation of the user and master data, a personal letter with the username will be sent to the customer via e-mail.

The letter is signed and returned to the bank by the customer and is validated with the specimen signature. The user is then activated on the banking system, informed of the activation and receiving the activation code via e-mail. The activation code is only valid once for 20 days. The activation only applies to the current device. To activate additional devices, there is the self-service option on devices that have already been activated. Such an activation code is valid for 5 minutes.

Signature verification

Onboarding video:
https://auth.rbinternational.com/Landingpage/

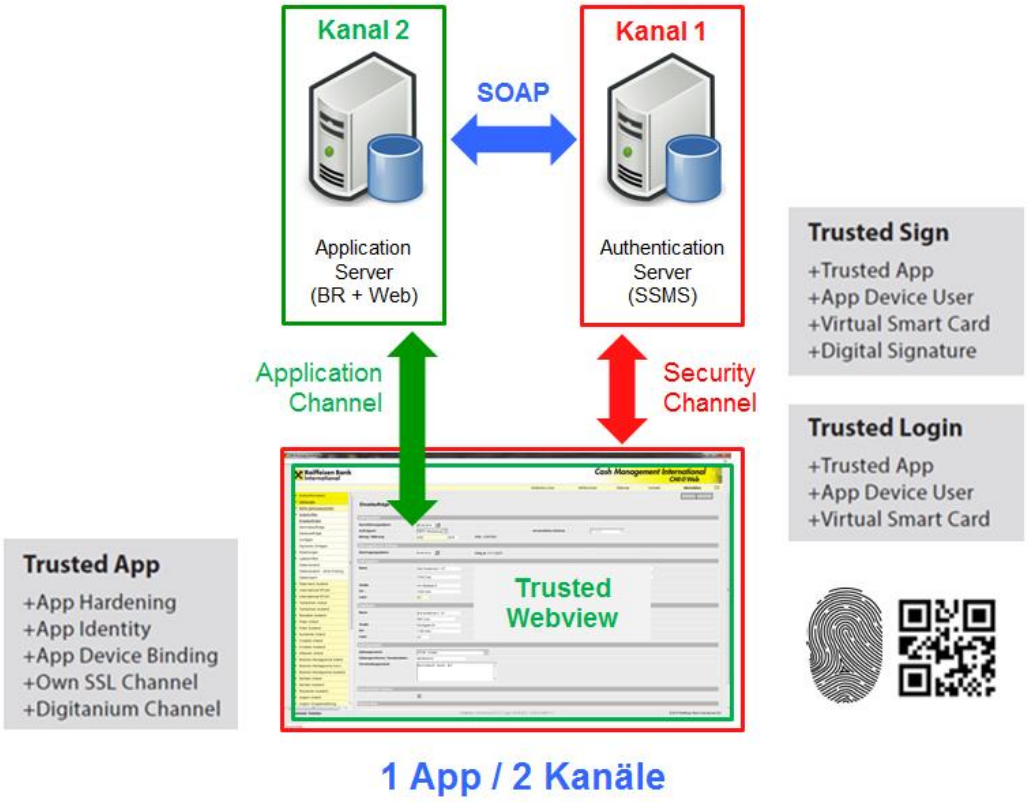
Onboarding video



2.4.3 Secure multi-factor authentication

Multi-factor authentication

The additional factors include device connectivity, secure encryption, additional server components and the separation of communication channels. Both the login and transaction signatures are secured multiple times.



Multi-channel technology

There are numerous other protective mechanisms that secure the entire process, but which cannot be fully communicated for security reasons.

2.4.3.1 Feature "Knowledge" = Password

Password

The CMI Apps are offered for download by RBI on a completely user-neutral basis; no passwords predefined by the bank are transmitted. Personalization takes place during the activation process, where the customer generates a personal password according to the specified password complexity criteria. This password is used for the login and the transaction signature and is therefore only known to the customer himself. Private/public key mechanisms are used as encryption methods.

2.4.3.2 Feature “Possession" = Device binding

Device binding

During the CMI App activation a kind of fingerprint is generated (a combination of hardware, software and user data). This results in a device binding of the app, a transfer possibility of the app without new activation to other devices is thus prevented.

2.4.3.3 Feature "Inherence”

Fingerprint and FaceID

In the CMI App settings, the fingerprint for login and transaction signature can be activated instead of the password. FaceID (face recognition) can also be used for authentication under iOS. All biometric data is managed and stored by iOS.

3 Customer requirements

3.1 Firewall settings

Firewall

For the use of CMI@Web / FAST@Web the following firewall activations on the customer side are required. Please have them set up by your local IT department:

- https://auth.rbinternational.com IP address: 217.13.188.144
- https://cmi.rbinternational.com IP address: 217.13.188.80
- https://fast.rbinternational.com IP address: 217.13.183.154

3.2 Connection tests

Connectivity tests

The connectivity can be checked using the standard browser. This only serves to check the technical accessibility, the use of CMI@Web / FAST@Web is only possible with the Desktop/Mobile Apps.

- https://auth.rbinternational.com/ssms-services/asm/rest/device
- https://cmi.rbinternational.com
- https://fast.rbinternational.com
- https://auth.rbinternational.com/Landingpage/index_en.html

The tests should be performed with Internet Explorer, as Chrome and Firefox incorrectly display a certificate error.

3.3 AST Analysis Tool

In case of errors, our analysis tool can be downloaded and used. To create the logs that are important for further analysis, start the tool and reproduce the error.

Download Link:

https://auth.rbinternational.com/Analyse/AST_Analysetool.zip

For further information please contact our Support Desk:

Phone: +43 - 1 - 33701 – 4499
Email: cashmanagementsupport@rsc.co.at
Mo - Fr: 07:00 - 18:00

3.4 Client environment

The CMI solution can be used on all current operating systems (Windows and macOS).

Special environments (Citrix, Terminal Server, VMware Virtualization,...) are excluded from support and are currently not supported, as the device binding required for security reasons may not be possible.