Raiffeisen Bank International

CMI Business Banking

Sicherheitshinweise

Inhalt

Raiffeisen Bank International

1 Allgemeine Sicherheitsinformationen

1.1 Schützen Sie Ihre Daten

- Gehen Sie bitte sorgfältig mit Ihren Daten um.
- Geben Sie Ihre persönlichen Zugriffs- und Autorisierungsdaten, wie Ihren Usernamen und Ihr Passwort, niemals an Dritte weiter.
- Stellen sie sicher, dass Sie niemand bei der Eingabe Ihrer persönlichen Daten beobachtet.
- Speichern Sie Ihr persönliches Passwort niemals auf Ihrem Endgerät (PC, Laptop, Handy).
- Bitte beachten Sie, dass wir Sie niemals nach ihren Logindaten oder anderen sensiblen Informationen fragen werden - unbhängig vom Kommunikationskanal (Email, SMS, Telefon,…).

1.2 Verwenden Sie ein sicheres Passwort

- Wählen Sie für Ihr persönliches Passwort keine einfachen oder leicht nachvollziehbaren Kombinationen (wie zum Beispiel Namen, Orte, Geburtsdatum).
- Halten Sie sich an die vorgegebenen Kriterien zum Erstellen Ihres persönlichen Passworts.
- Ändern Sie Ihr persönliches Passwort regelmäßig und verwenden Sie nicht das gleiche Passwort für unterschiedliche Anwendungen.

1.3 Systemsicherheit

- Verwenden Sie nur vertrauenswürdige und gewartete Endgeräte.
- Verwenden Sie einen aktuellen Virenschutz
- Verwenden Sie eine Firewall zum Schutz Ihres Endgeräts.

2 CMI Sicherheitslösung

2.1 Allgemeines

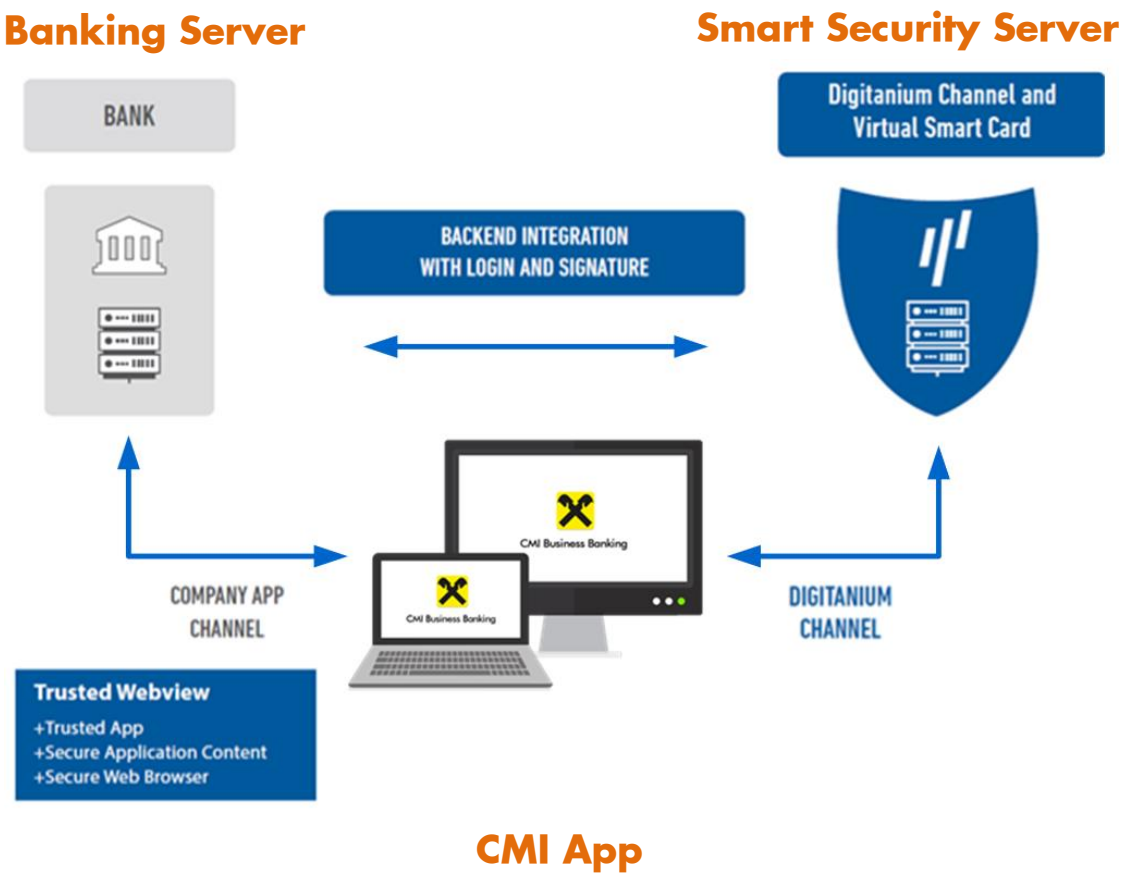
CMI nutzt eine moderne und sichere Mehr-Faktor-Authentifizierungslösung für das Corporate e-Banking. Die Lösung erfüllt modernste Sicherheitsstandards und alle Anforderungen der EU / PSD2 Vorgaben einer starken Kundenauthentifizierung.

PSD2 Compliant

Unsere technischen und organisatorischen Schutzmechanismen werden laufend aktualisiert und von unabhängigen Stellen auditiert.

Auf den folgenden Seiten wird die Basistechnologie und das Funktionsprinzip dargestellt, zusätzlich werden die wichtigsten Sicherheitsmerkmale der Lösung beschrieben.

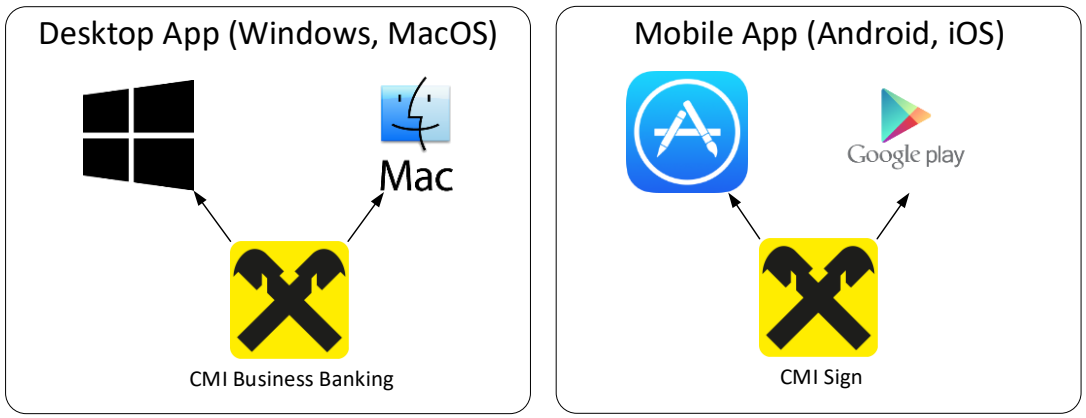
2.2 7-Layer Security



2.3 Funktionsprinzip

2.3.1 Zugriff via App

Der Kundenzugriff auf CMI@Web / FAST@Web erfolgt nicht über einen Browser oder mittels zusätzlicher Hardware, sondern über eine speziell gehärtete App, die für verschiedene Plattformen bereitgestellt wird.



- Die Desktop Apps benötigen keine Installation oder administrative Berechtigungen am Client. Die Verteilung erfolgt via Download Link vom CM Support Desk.
- Die Mobile Apps müssen über den jeweiligen Store heruntergeladen und installiert werden

Desktop App

Mobile App

App Download Seite:
https://auth.rbinternational.com/Update/
Öffnen Sie den Link bitte im Internet Explorer, da in Chrome und Firefox fälschlicherweise ein Zertifikatsfehler angezeigt wird.

2.3.2 Gerätebindung

Die App muss im Zuge des Onboardings aktiviert werden und wird dabei an das jeweilige Endgerät gebunden. Der CMI Zugriff ist daher grundsätzlich immer auf dieses Gerät beschränkt. Via Self-Service, mittels Menüpunkt „Verwaltung > Neues Gerät

Gerätebindung

hinzufügen“ können jedoch jederzeit weitere Geräte aktiviert für die Nutzung mit CMI verwendet werden.

2.3.3 Sichere App Kommunikation

1 App / 2 Kanäle

Die umfassenden Sicherheitsmechanismen der App sorgen für eine sichere Kommunikation und strikte Trennung der Kanäle für Sicherheit und Daten. Zusätzlich gibt es auf Bankseite noch ein zusätzliches Autorisierungssystem, das für eine Absicherung der Verbindung zwischen der Client App und dem e-Banking Server sorgt.

2.3.4 App Login & Signatur mit Passwort

Sicheres Login & Signatur

Im Zuge der Aktivierung wird vom Kunden selbst ein Passwort vergeben, das dann sowohl beim Login wie auch für die Transaktionssignatur verwendet wird. Aufgrund zusätzlichen Sicherheitsmechanismen kann auf die Nutzung zusätzlicher Hardware verzichtet werden, ohne dadurch das Risiko zu erhöhen.

Weitere Details zu einzelnen Sicherheitsfeatures werden im nächsten Kapitel beschrieben.

2.4 Sicherheitsaspekte

Die Autorisierungslösung von CMI nutzt eine Reihe von Sicherheitsmechanismen. Einige davon werden in der folgenden Auflistung dargestellt. Aus Sicherheitsgründen können wir leider keine weiteren Details zur technischen Implementierung dieser Schutzmaßnahmen geben.

2.4.1 Sicherheitsmechanismen auf einen Blick:

- Sicherer Aktivierungsprozess
- App Gerätebindung an die Hardware
- App Integritätsprüfung
- Virtuelle Smartcard
- Sicherer, verschlüsselter Identitätsspeicher
- PKI-basierte Prozesse
- Servergestützte Sicherheitsprüfungen
- 2-Kanal Technologie / eigener Sicherheitskanal
- Multifaktor Authentifizierung für Login + Signatur
- Trusted Webview für Applikations-Inhalte
- Zertifikats Pinning
- URL Whitelisting
- Anti Debugging
- Anti Reverse Engineering
- Anti Code-Injection
- Jailbreak / Rooting / Malicious App Detection
- Static & Dynamic Manipulation Protection
- Client risk rating
- Biometrie Support: Fingerprint, Touch ID, Face ID
- Optionale Sicherheitsstufen für Signatur + Self Service

2.4.2 Sicheres „Onboarding“

Für die Aktivierung der App wird ein Aktivierungscode benötigt. Nach Abschluss des Kundenvertrags und erfolgter Teilnehmer- & Stammdatenanlage wird dem Kunden ein Erstzugangsbrief mit den Zugangsdaten (User, Aktivierungscode) per Mail zugestellt. Der Aktivierungscode ist nur einmalig gültig für 20 Tage.

Unterschriftsprüfung

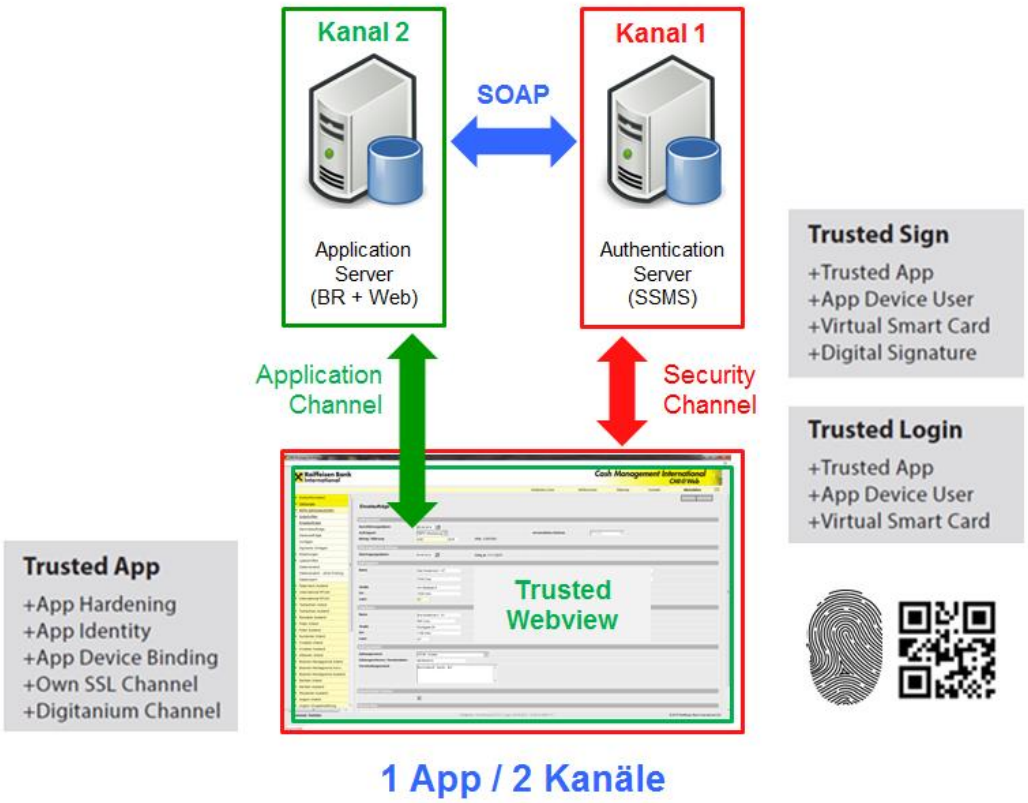
Der unterschrieben retournierte Erstzugangsbrief wird durch die Unterschriftsprobe validiert. Im Anschluss wird der Kunde am Banksystem freigeschaltet und über die Freischaltung via Mail informiert. Die Aktivierung gilt immer nur für das aktuelle Device. Um weitere Geräte zu aktivieren gibt es auf bereits aktivierten Geräten die Möglichkeit des Self-Service. Ein dabei ausgestellter Aktivierungscode ist für 5 Minuten gültig.

Onboarding Video

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

2.4.3 Sichere Mehr-Faktor-Authentifizierung

Die zusätzlichen Faktoren sind unter anderem durch die Gerätebindung, sichere Verschlüsselung, zusätzliche Serverkomponenten sowie die Trennung der Kommunikationskanäle gegeben. Sowohl das Login wie auch Transaktionssignaturen sind mehrfach abgesichert.



Es existieren zahlreiche weitere Schutzmechanismen, die den Gesamtprozess absichern, welche jedoch aus Sicherheitsgründen nicht zur Gänze kommuniziert werden können.

2.4.3.1 Merkmal „Wissen" = Passwort

Die CMI Apps werden von RBI völlig userneutral zum Download angeboten, es werden keine bankseitig vordefinierten Passwörter übermittelt. Die Personalisierung erfolgt im Zuge des Aktivierungsprozesses, wo vom Kunden selbst ein Passwort gemäß den vorgegebenen Komplexitätskriterien erzeugt wird. Dieses Passwort wird für den späteren Login und die Transaktionssignatur verwendet und ist somit nur dem Kunden selbst bekannt. Als Verschlüsselungsverfahren kommen Private-/Public-Key Mechanismen zum Einsatz.

2.4.3.2 Merkmal „Besitz“ = Gerätebindung

Gerätebindung

Im Zuge der App Aktivierung wird eine Art Fingerprint erzeugt (eine Kombination aus Hardware, Software und Userdaten). Damit ergibt sich eine Gerätebindung der App, eine Übertragungsmöglichkeit der App ohne neue Aktivierung auf andere Umgebungen wird damit verhindert.

2.4.3.3 Merkmal „Biometrie“

Fingerprint und FaceID

In den App-Einstellungen kann anstelle des Passwortes auch der Fingerabdruck für Login und Transaktionssignatur aktiviert werden. Unter iOS kann auch FaceID (Gesichtserkennung) zur Authentifizierung genutzt werden. Alle biometrischen Daten werden von iOS verwaltet und gespeichert.

3 Kundenanforderungen

3.1 Firewall Freischaltungen

Firewall

Für die Nutzung von CMI@Web / FAST@Web werden folgende Firewall Freischaltungen auf Kundenseite benötigt. Bitte diese von der lokalen IT einrichten zu lassen:

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

3.2 Verbindungstests

Connectivity Tests

Anschließend kann die Konnektivität über den Standard Browser überprüft werden. Dies dient lediglich zur Überprüfung der techn. Erreichbarkeit, die Nutzung von CMI@Web / FAST@Web ist nur mit den Desktop/Mobile Apps möglich.

- 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

Die Tests sollten mit dem Internet Explorer durchgeführt werden, da bei Chrome und Firefox fälschlicherweise ein Zertifikatsfehler angezeigt.

3.3 AST Analyse Tool

Im Falle von Fehlern kann unser Analyse Tool heruntergeladen und genutzt werden. Zum Erstellen der für die weitere Analyse wichtigen Logs starten Sie das Tool und reproduzieren den Fehler.

Download Link:

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

Für weitere Informationen wenden Sie sich bitte an unseren Support Desk:

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

3.4 Client Umgebung

Die CMI Lösung ist grundsätzlich auf allen aktuellen Betriebssystemen einsetzbar. Spezielle Umgebungen (Citrix, Terminal Server, VMware Virtualisierung,…) sind vom Support ausgenommen und werden aktuell nicht unterstützt, da die aus Sicherheitsgründen nötige Gerätebindung dort ggfs. ein Problem darstellt.