

Systemvoraussetzungen / Configuration système requise  
**Mobile Clients Version 20.0**

# Inhaltsverzeichnis

<b>1 Betriebsvarianten Mobile Clients .....</b>	<b>3</b>
<b>2 Systemübersicht.....</b>	<b>4</b>
2.1 CMI über Firewall .....	4
2.2 CMI mit Relay-Server .....	5
2.3 CMI AIS .....	6
<b>3 Softwarevoraussetzungen .....</b>	<b>7</b>
3.1 Applikationsserver .....	7
3.2 Web-/Publikations-/Relay-/STS-Server .....	7
3.3 PDF Tools .....	7
3.4 Client .....	8
<b>4 Authentifizierung (IAM) .....</b>	<b>9</b>
4.1 Security Token Service (STS) .....	9
4.2 Ohne Security Token Service (STS) .....	9
4.3 Mit Security Token Service (STS) .....	9
<b>5 Hardwarevoraussetzungen .....</b>	<b>10</b>
5.1 Webserver .....	10
5.2 Relay-Server .....	10
5.3 STS-Server.....	10
<b>6 Netzwerkvoraussetzungen .....</b>	<b>11</b>
<b>7 Datensicherheit.....</b>	<b>12</b>
7.1 Verschlüsselung .....	12
7.2 Zertifikate.....	12
7.3 Protokolle & Cipher Suites .....	12
<b>8 Anhang - Auszug Microsoft Product Lifecycle Suche.....</b>	<b>13</b>

# 1 Betriebsvarianten Mobile Clients

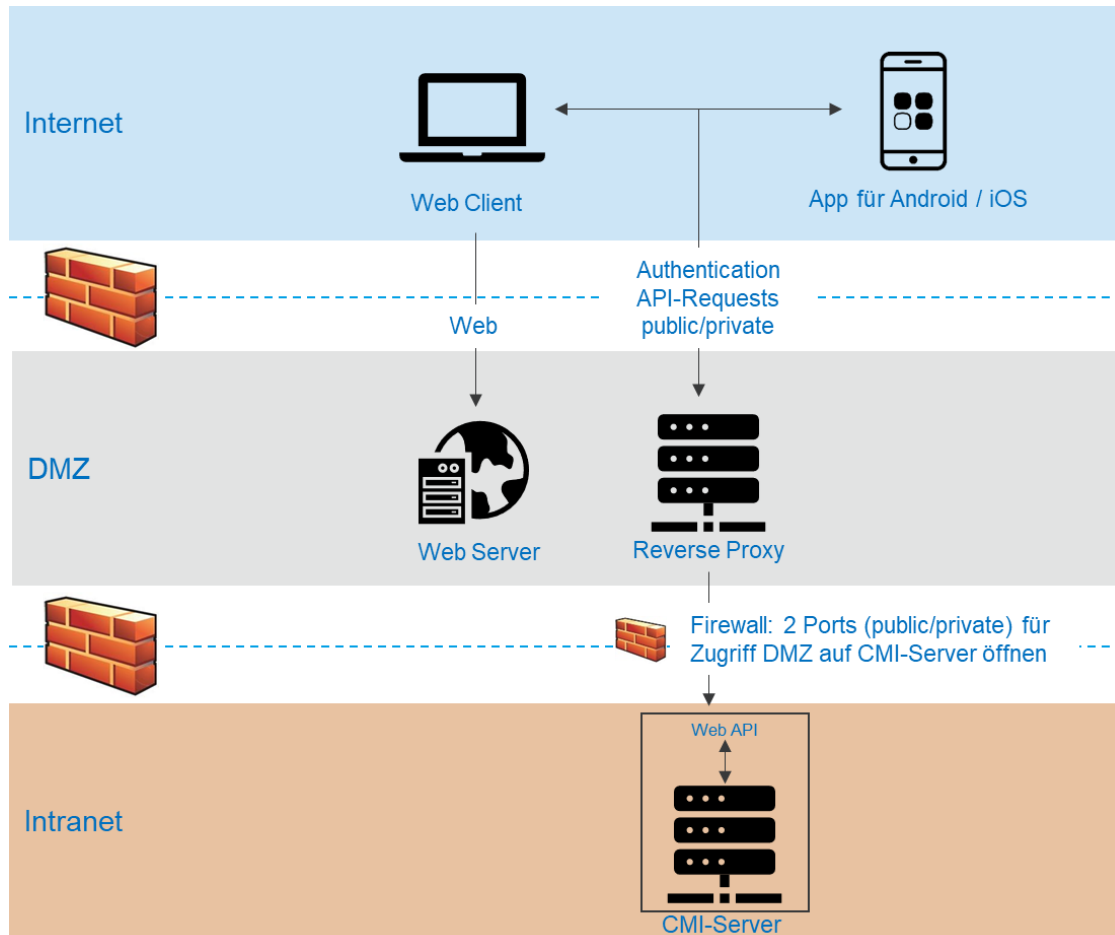
Wir empfehlen den Betrieb der Mobile Clients nicht selbst durchzuführen. Die folgenden Betriebsoptionen stehen zur Verfügung:

<b>Anbieter</b>	<b>Webclient</b>	<b>App</b>
CM Informatik AG	X	X
Talus Informatik AG	X	X
Abraxas AG	X	X

Wenn Sie über ein eigenes Rechenzentrum verfügen, kann die Installation vor Ort geprüft werden auf Basis der nachfolgenden Systemvoraussetzungen.

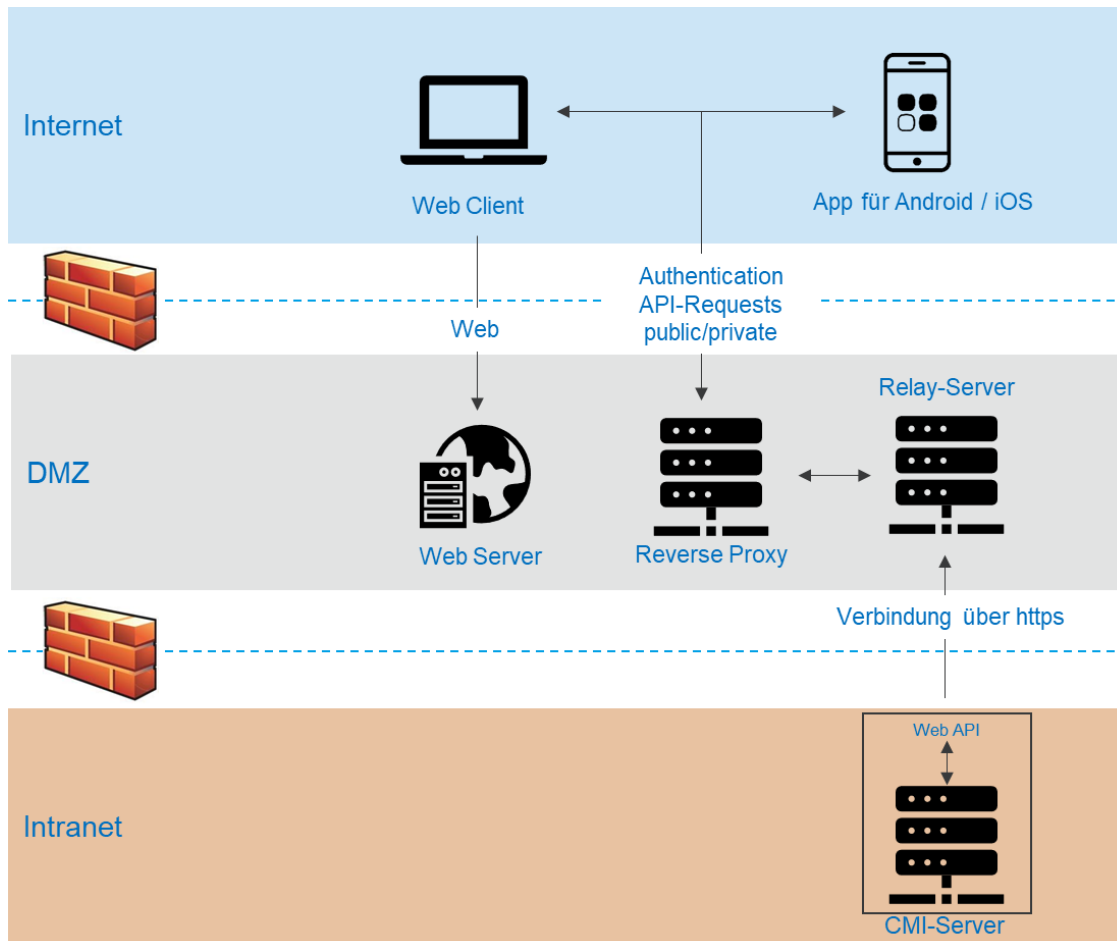
## 2 Systemübersicht

### 2.1 CMI über Firewall



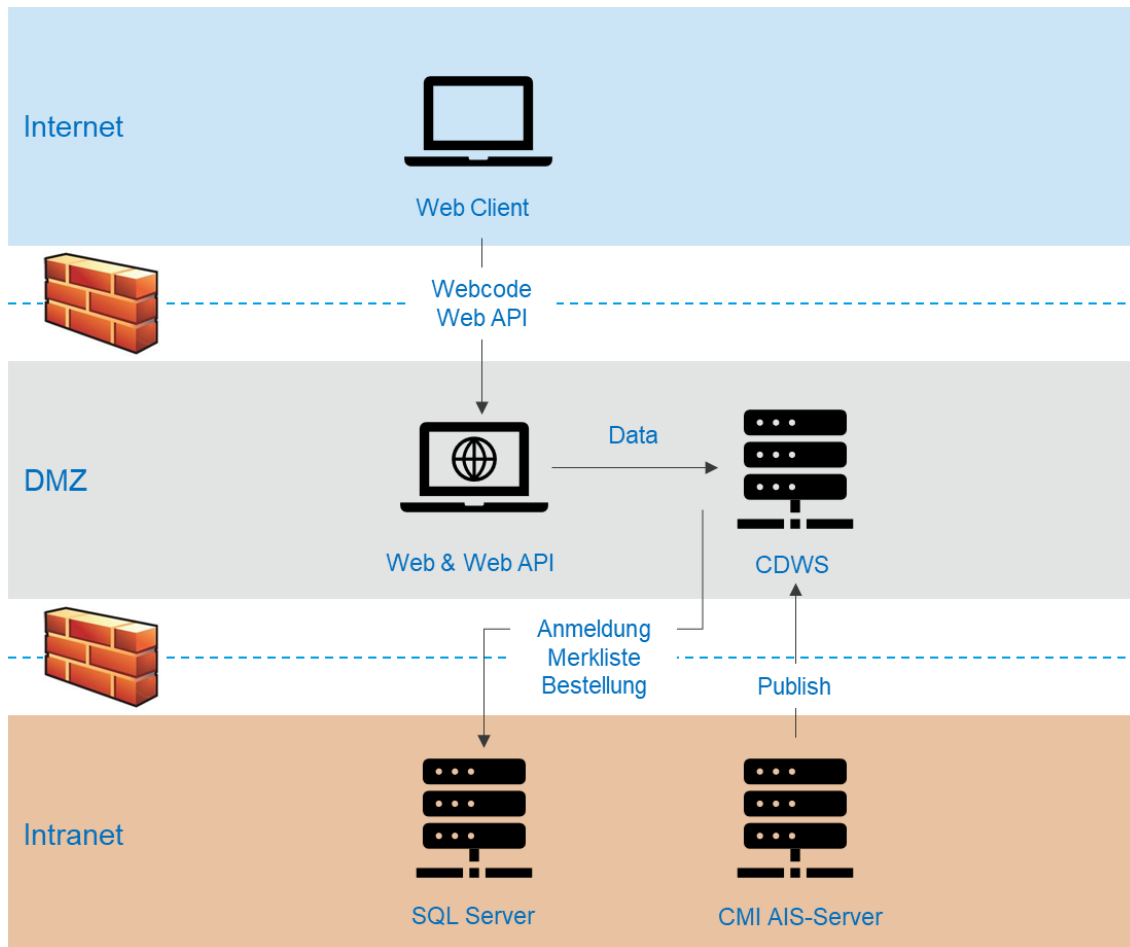
Der Zugriff aus der DMZ auf den CMI-Server wird in der Firewall über 2 Ports (public und private) geöffnet.

## 2.2 CMI mit Relay-Server



Der Zugriff wird vom CMI-Server zum Relay-Server über https aufgebaut.

## 2.3 CMI AIS



## 3 Softwarevoraussetzungen

Für die in den folgenden Kapiteln aufgeführten Produktversionen sind jeweils die aktuellsten Servicepacks zu verwenden.

### 3.1 Applikationsserver

#### Unterstützte Betriebssysteme

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

#### Weitere Komponenten

- .Net Framework 4.8

### 3.2 Web-/Publikations-/Relay-/STS-Server

- .Net Framework 4.8
- IIS (Internet Information Server) 7.5 oder höher
- IIS Rewrite Modul
- SSL-Zertifikate
- CMI AIS: CDWS-Service

### 3.3 PDF Tools

Mit PDF Tools können Dokumente in PDF konvertiert werden.

Unterstützte Version: 4.11

Weitere Informationen: <http://www.pdf-tools.com/>

Für die Installation von PDF-Tools wird vorausgesetzt, dass Office serverseitig installiert und lizenziert ist. PDF-Tools muss auf einem separaten Server betrieben werden. In beiden Fällen werden für PDF-Tools zwei zusätzliche Microsoft RDP-Lizenzen (Terminalserver) für Remotedesktop benötigt.

Wir gehen davon aus, dass der Kunde über die nötigen Microsoft RDP-Lizenzen bei der Installation von PDF-Tools verfügt.

Für bestimmte Funktionen wie z.B. PDF-Annotation ab Version 2.3 der Mobilien Clients wird die Option «PDF-Funktionalität Erweitert» in CMI vorausgesetzt.

### 3.4 Client

Die Lösungen sind in folgenden Ausprägungen verfügbar und setzen jeweils eine aktive Internetverbindung voraus:

Client	STS	Web (Default-Browser)	App (Public Store)
CMI Sitzungen, ab Version 2.3	O	X	iOS Android
CMI Dossier, ab Version 1.3	O	X	iOS Android
CMI Aufgaben, ab Version 1.3	O	X	-
CMI AIS Webclient, ab Version 1.2	-	X	-
CMI Schule	O	X	-
CMI Steuerbrowser	O	X	-

X verfügbar, O optional, - nicht unterstützt

#### Unterstützte Webbrowser (jeweils in der aktuellsten Version)

- Internet Explorer Version 11.0 (ohne Annotationsfunktionen)
- Microsoft Edge (Windows 10)
- Chrome (Windows, Mac OSX, iOS, Android)
- Firefox (Windows)
- Safari (Mac OSX, iOS)

Der Einsatz des Internet Explorers wird aufgrund von Performance und funktionalen Einschränkungen nicht empfohlen. CMI Steuerbrowser und CMI Schule unterstützen den Internet Explorer nicht.

Internet Explorer wird nur noch bis und mit Release 19.x aktiv unterstützt. Wir empfehlen frühzeitig auf einen der oben aufgeführten Browser umzusteigen.

#### Unterstützte App-Versionen

- iOS: letzte Version Major Release (iOS 12 Stand 01.2019)
- Android: ab Version 7.0  
Bedingt durch die Vielfalt der Hersteller, OS-Derivate und Geräteausprägungen kann nicht garantiert werden, dass sämtliche Geräte und Versionen unterstützt werden.

#### Enterprise Mobile Management / Mobile Application Management / Mobile Device Management

Bedingt durch die unterschiedlichen Ausprägungen wird die Verteilung und Verwaltung der CMI Apps und Webs mittels EMM/MAM/MDM-Systeme zum aktuellen Zeitpunkt nicht empfohlen.

Aufgrund bisheriger Erfahrungen sind massive Einschränkungen in Performance (applikatorisch wie auch bei VPN-Verbindungen) zu erwarten, welche die Verwendung der Lösung massiv einschränken, wenn nicht verhindern. Im Speziellen wird unter iOS WKWebView zwingend vorausgesetzt, welches von dem zum aktuellen Zeitpunkt bekannten EMM/MAM/MDM-Systemen nicht unterstützt wird.

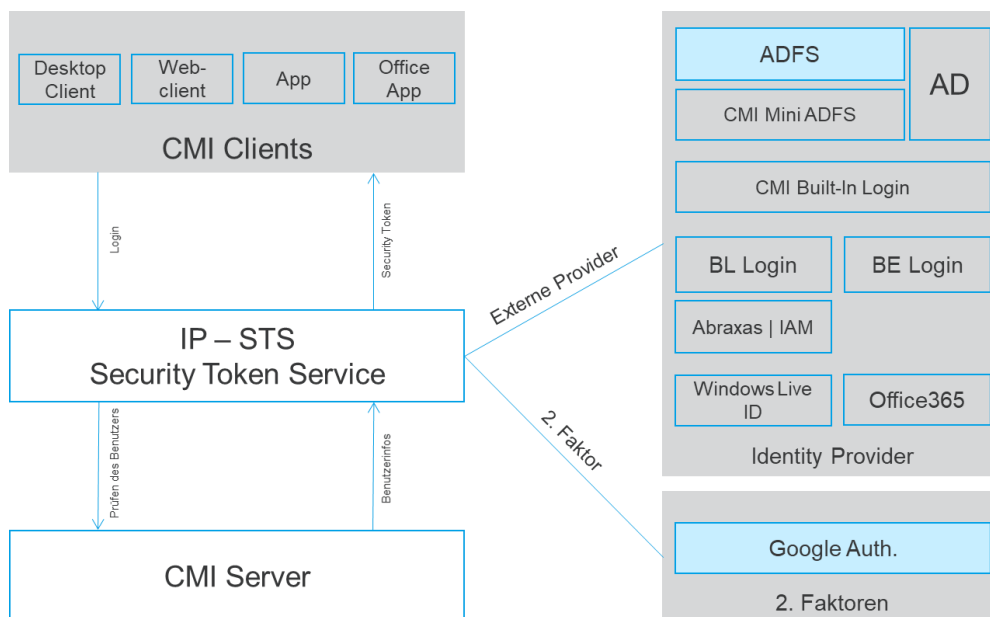
Wird aufgrund von Security-Architektur-Vorschriften trotzdem auf eine EMM/MAM/MDM-Lösung gesetzt wird dringend empfohlen ein individuelles Projekt mit kostenpflichtiger Involvierung von CMI zu starten.



## 4 Authentifizierung (IAM)

### 4.1 Security Token Service (STS)

Grundsätzlich empfiehlt die CM Informatik AG mit dem Einsatz der mobilen Clients ebenfalls den 'Security Token Service' einzusetzen. Diese CMI-Komponente erlaubt eine zentrale Authentifizierung für alle Clientvarianten, die Federation der Logins (extern, intern) wie auch die Integration von Identity Providern unserer Kunden (wie z.B. BE Login, VRSG IAM etc.). Natürlich erfüllt der STS sämtliche aktuellen Sicherheitsstandards und setzt dabei auf bekannte und etablierte Security Standards wie OAuth2, SAML 2.0, OpenID Connect und WS Fed.



### 4.2 Ohne Security Token Service (STS)

Die CMI-Applikationen unterstützen einen Login via:

- Built-In (CMI-Benutzer)
- Active Directory

### 4.3 Mit Security Token Service (STS)

Wenn die Applikationen mit einem STS betrieben werden, können werden die folgenden Varianten unterstützt:

- Built-In (CMI-Benutzer)
- Active Directory
- WS-Federation (ADFS, Office 365, Azure-AD, ...)
- OpenId Connect Authorization Code Flow
- Individuelle Umsetzungen: BE-Login, BL-Login, Abraxas-Login

Da der STS eine unabhängige und separat versionierte Komponente ist, können sich die möglichen Authentifizierungsverfahren von der obigen Auflistung unterscheiden. Für die aktuellste Liste an unterstützten Verfahren oder weiteren Themen wie Zwei-Faktor-Authentifizierung können Sie uns gerne kontaktieren.

## 5 Hardwarevoraussetzungen

### 5.1 Webserver

	<b>Mindestanforderung</b>	<b>Empfehlung</b>
Prozessor	1.8 GHz	2.4 GHz oder höher
Arbeitsspeicher	64bit: 4 GB	64bit: 8 GB

### 5.2 Relay-Server

	<b>Mindestanforderung</b>	<b>Empfehlung</b>
Prozessor	1.8 GHz	2.4 GHz oder höher
Arbeitsspeicher	64bit: 4 GB	64bit: 8 GB

### 5.3 STS-Server

	<b>Mindestanforderung</b>	<b>Empfehlung</b>
Prozessor	1.8 GHz	2.4 GHz oder höher
Arbeitsspeicher	64bit: 4 GB	64bit: 8 GB

## 6 Netzwerkvoraussetzungen

Beim Einsatz der Mobile Clients sind grundsätzlich folgende Firewalls Policies einzurichten. Die Regeln müssen immer den In und Out Traffic zulassen.

Policy Type	From	To	Port	Mobile Clients
Internal	LAN	DMZ	tcp: 443 (https)	alle
External	WWW	DMZ	tcp: 443 (https)	alle
Internal	LAN	DMZ	tcp: (5000)	CMI.CDWS.Service (CMI STAR Webclient)

Der Port für den Zugriff auf den CMI.CDWS.Service (DataService) ist als Beispiel zu verstehen. Dieser Port ist frei wählbar, beginnend ab 1024.

Weitere Konfigurationen können im Einzelfall notwendig werden in Abhängigkeit der vorhandenen Infrastruktur.

Betreiben Sie CMI oder CMI AIS in einem Rechenzentrum (RZ), so können auf Seite RZ Kosten für die Freischaltung der entsprechenden Ports, Sicherheitseinstellungen usw. entstehen. Wenden Sie sich direkt an Ihren RZ Partner.

## 7 Datensicherheit

### 7.1 Verschlüsselung

Die Verschlüsselung von Daten im Transport verhindert unter anderem die Einsicht von Dritten. Wir empfehlen daher sämtliche Verbindungen zu verschlüsseln, sofern möglich. Dazu gehören:

- Verbindung zwischen Rich Client und Applikations-Server
- Verbindung zwischen Web-Server und Applikations-Server
- Verbindung zwischen Firewall und Web-Server
- Verbindung zwischen Endbenutzern und Firewall

### 7.2 Zertifikate

Zur Verschlüsselung von Daten werden Zertifikate verwendet, die über eine bestimmte Lebensdauer verfügen. Die verwendeten Zertifikate müssen durch den Kunden gestellt und verwaltet werden.

### 7.3 Protokolle & Cipher Suites

Wir empfehlen den jeweils gültigen Sicherheitsstandards zu folgen und bspw. unsichere resp. veraltete Protokolle und Cipher Suites zu deaktivieren. Dies gilt vor allem für die Komponenten, die aus dem Internet erreichbar sind.

Als Anhaltspunkt kann auf das Dokument „SSL and TLS Deployment Best Practices“ zurückgegriffen werden:

<https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices>

## 8 Anhang - Auszug Microsoft Product Lifecycle Suche

Angaben gemäss Hersteller <http://support.microsoft.com/lifecycle> . Detaillierte Informationen zum Microsoft Mainstream Support und Extended Support entnehmen Sie der Microsoft Produkt Lifecycle Suche. Gültigkeit hat nur die Online-Version. Änderungen bleiben vorbehalten.

CMI geht davon aus, dass die Lauffähigkeit von den CMI Lösungen in Kombination mit Microsoft Client-, Server- und Office-Komponenten, welche ausserhalb des Mainstream Supports und sich derzeit noch immer breit im Einsatz befindenden, weiterhin lauffähig sind. Für eine bestmögliche Supportabdeckung wird jedoch dringend empfohlen, die CMI-Produkte mit offiziell unterstützten Microsoft Client-, Server- und Office-Komponenten zu betreiben. Bei einer Supportanfrage erhalten Sie Unterstützung im Rahmen der Möglichkeiten. Es ist jedoch nicht auszuschliessen, dass auf diese Empfehlung zurückzukommen ist.