Systemvoraussetzungen 22.0

Web Client/Mobile Clients

CM Informatik AG, Ringstrasse 7, CH-8603 Schwerzenbach, T +41 43 355 33 99, info@cmiag.ch, cmiag.ch

Inhaltsverzeichnis

1 Änderungsprotokoll

1.1 Änderungen zum vorherigen Release

Nachfolgend werden relevante Änderungen in den Systemvoraussetzungen im Vergleich zum vorherigen Release dargestellt.

Kapitel	Neu ab diesem Release
4.2 Sicherheitseinstellungen Office (Trust Center)	Als neues Kapitel aufgenommen
5.1 Web-/Publikations-/Relay-/STS-Server	– Windows Server 2012 nicht mehr unterstützt – Windows Server 2022 aufgenommen

1.2 Vorankündigungen für den nächsten Release (23.0)

Kapitel	Anpassung
5.1 Web-/Publikations-/Relay-/STS-Server	– Internet Information Server 10 oder höher – Windows Server 2012 R2 nicht mehr unterstützt – .Net 6.0 (zusätzlich zu .Net 4.8 Framework)
5.2 Client	– Web Client in Kombination mit IE 11 nicht unterstützt

1.3 Information zur Unterstützung von einzelnen Modulen

CMI entwickelt ihre Produkte stetig weiter und bisherige Module werden deshalb schrittweise durch die weiterentwickelten Lösungen im Web Client abgelöst. Damit Sie bereits frühzeitig über die geplanten Ablösungen informiert sind, führen wir an dieser Stelle die Module auf, die mit einem künftigen Release nicht mehr unterstützt sind. Weiterführende Informationen zur Ablösung einzelner Module werden in einer separaten Kommunikation folgen.

Modul	Nicht mehr unterstützt ab:
Dossierbrowser (Web-Lösung & App)	Ab Release 23.0
Zusammenarbeit Dritte	Ab Release 23.0
CMI Sitzungen 1.0 (Web-Lösung & App)	Ab Release 23.0
CMI Sitzungen 2.0 (Web-Lösung & App)	Ab Release 25.0

Hinweis: Ab dem Release 23.0 wird die Weiterentwicklung von CMI Sitzungen 3.0 im Web Client verfügbar sein. Wir weisen Sie schon heute darauf hin, dass wir nach dem Update auf CMI Sitzungen 3.0 keine nativen Apps (iOS, Android, Windows) mehr anbieten. Wir empfehlen bereits heute mit dem jeweiligen Web Client zu arbeiten.

2 Betriebsvarianten Web Client/Mobile Clients

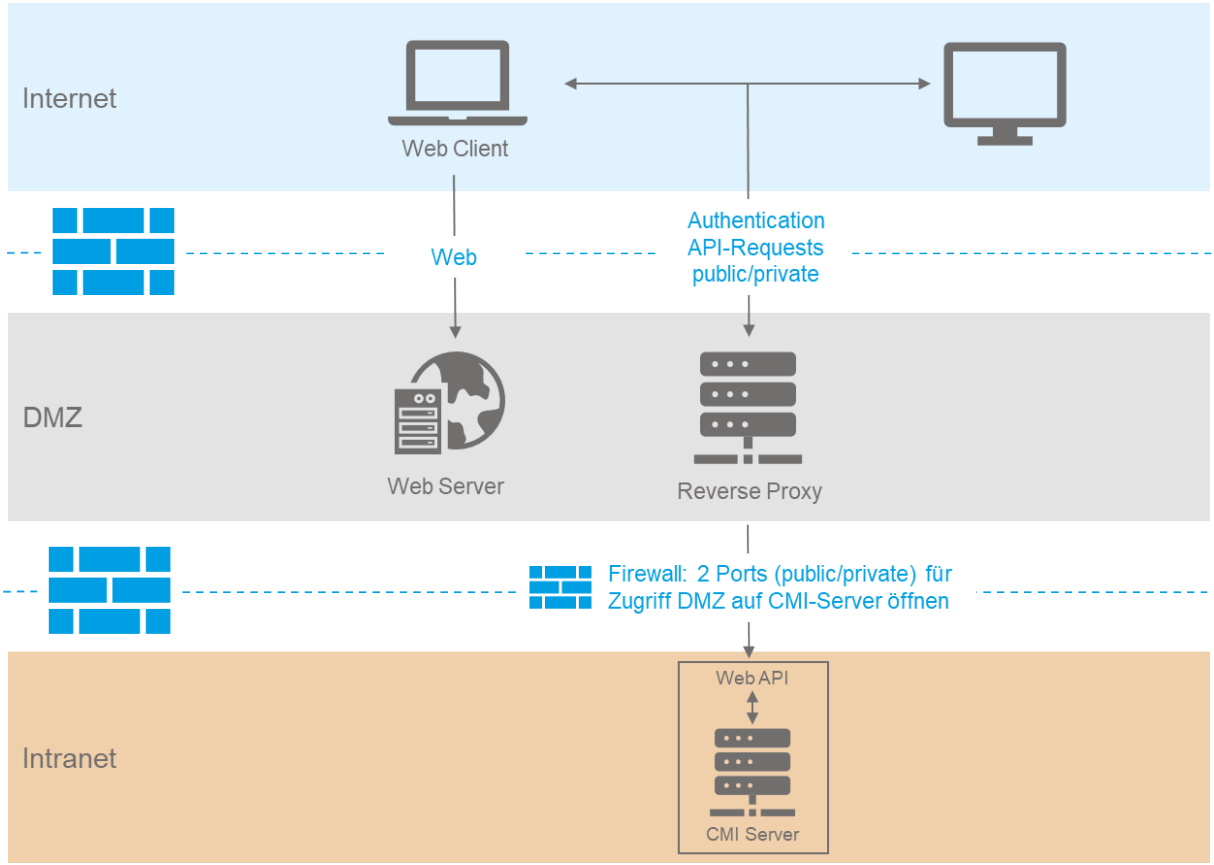
Wir empfehlen den Betrieb vom Web Client bzw. Mobile Clients nicht selbst durchzuführen. Die folgenden Betriebsoptionen stehen zur Verfügung:

Anbieter	Web Client	App
CM Informatik AG	X	X
Talus Informatik AG	X	X
Abraxas AG	X	X
OBT AG	X	X

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

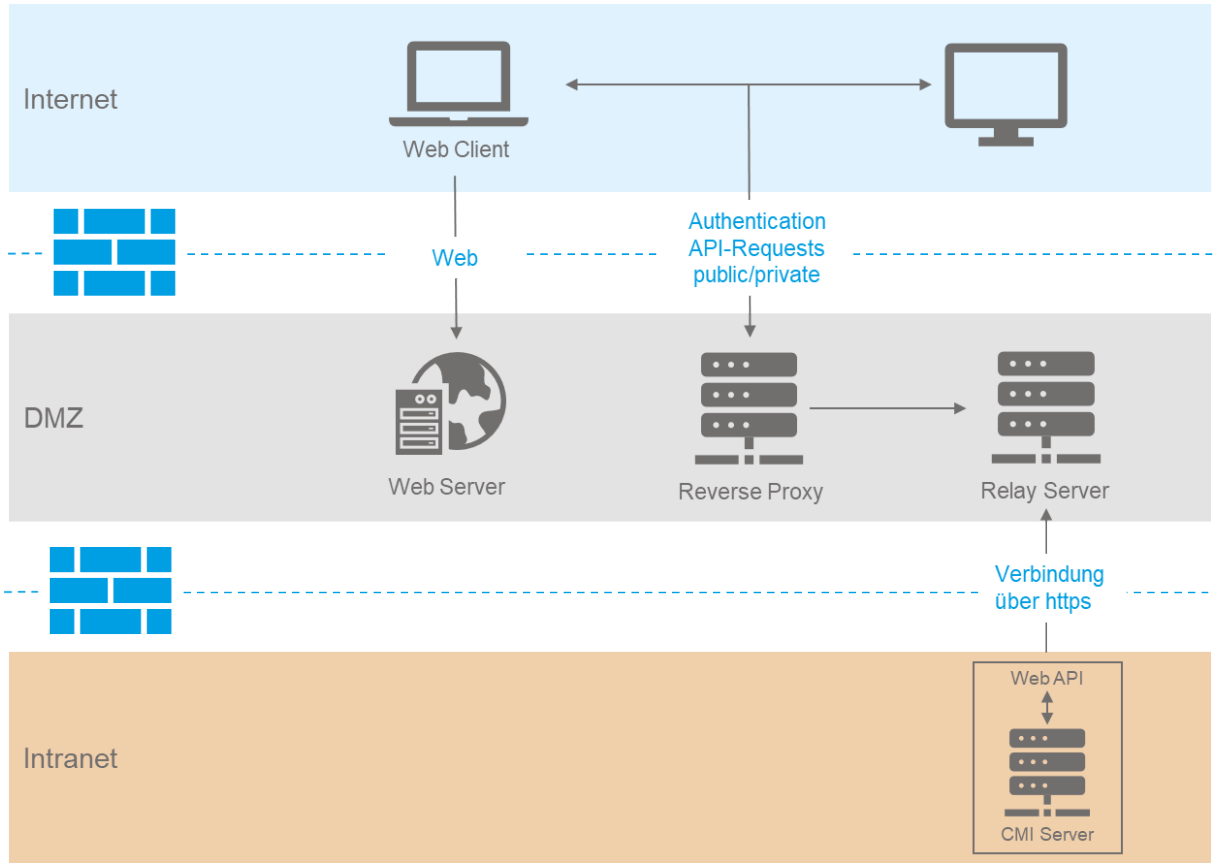
3 Systemübersicht

3.1 CMI über Reverse Proxy



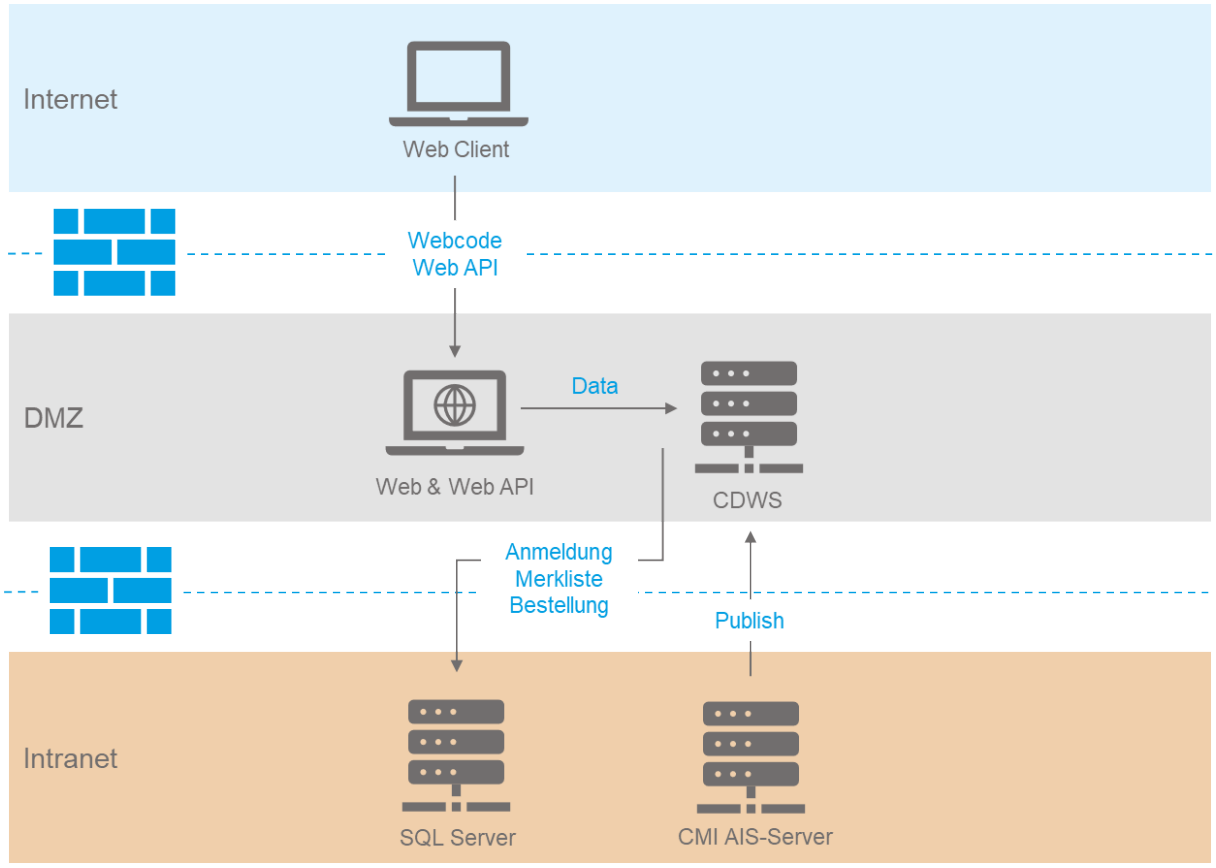
Der Zugriff aus der DMZ auf den CMI-Server wird in der Firewall über 2 Ports (public und private) geöffnet.

3.2 CMI mit Relay-Server



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

3.3 CMI AIS


Internet
Web Client
Webcode
Web API
DMZ
Data
Web & Web API
CDWS
Anmeldung
Merkliste
Bestellung
Publish
Intranet
SQL Server
CMI AIS-Server

4 Allgemeines

4.1 Internetverbindung (Bandbreite)

Für ein zuverlässiges und flüssiges Arbeiten wird eine stabile und performante Internetverbindung vorausgesetzt. Die dafür benötigte Brandbreite hängt individuell pro Kunde von den eingesetzten Modulen, der Grösse der Dateien und Dokumente sowie der Anzahl aktiver Benutzenden ab. Zudem ist die Verfügbarkeit und Performance von der Erreichbarkeit des CMI Backends innerhalb der Umgebung des Kunden abhängig.

4.2 Sicherheitseinstellungen Office (Trust Center)

Im Trust Center von Office muss die Domain des Web Clients als vertrauenswürdig eingetragen werden, damit eine uneingeschränkte Nutzung möglich ist. Diese Einstellung kann zentral für die gesamte Organisation als Ausnahme in den Gruppenrichtlinien hinterlegt werden. Wird beispielsweise die URL https://cmi.gemeinde.ch/webclient verwendet, so muss die Domain cmi.gemeinde.ch freigeschaltet werden.

- Möglicherweise müssen administrative Templates (ADMX/ADML) für Office auf dem Domain Controller installiert werden: https://www.microsoft.com/en-us/download/details.aspx?id=49030
- Die folgende Ressource hilft, um eine Gruppenrichtlinie zu erstellen: https://admx.help/?Category=Office2016&Policy=office16.Office.Microsoft.Policies.Windows::L_AuthenticationFBABehavior

5 Softwarevoraussetzungen

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

5.1 Applikationsserver

Unterstützte Betriebssysteme

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Weitere Komponenten

- .Net Framework 4.8

5.2 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
- CMI Dossier/Webdav: .Net Core Hosting Bundle 3.1

5.3 Client

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

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

- Microsoft Edge Chromium (Windows 10)
- Chrome (Windows, Mac OSX, iOS, Android)
- Safari (Mac OSX, iOS)

Hinweis: Der Einsatz des Internet Explorers wird aufgrund von Performance und funktionalen Einschränkungen nicht empfohlen. Der Internet Explorer wird nicht mehr aktiv unterstützt. Wir empfehlen auf einen der weiteren oben aufgeführten Browser umzusteigen.

Unterstützte App-Versionen

- iOS: letzte Version Major Release (iOS 12 Stand 01.2019)
- Android: ab Version 8.0

Bedingt durch die Vielfalt der Hersteller, OS-Derivate und Geräteausprägungen kann nicht garantiert werden, dass sämtliche Geräte und Versionen unterstützt werden.

Wichtig: Die Mobile Apps unterstützen keine Pre-Authentication.

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.

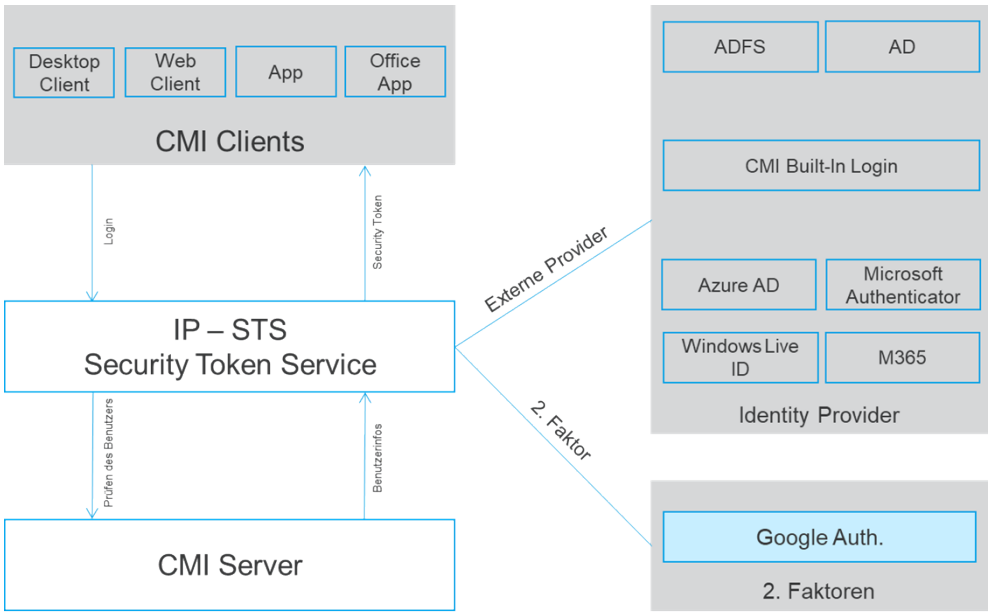
Aufgrund bisheriger Erfahrungen sind massive Einschränkungen in Performance (applikatorisch wie auch bei VPN-Verbindungen) zu erwarten, welche die Verwendung der Lösung massiv einschränken, wenn nicht verhindern. Im Speziellen wird unter iOS WKWebView zwingend vorausgesetzt, welches von dem zum aktuellen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

6 Authentifizierung (IAM)

6.1 CMI Security Token Service (STS)

Grundsätzlich empfiehlt die CM Informatik AG mit dem Einsatz der mobilen Clients ebenfalls den ‘CMI 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. Azure AD, ADFS). Natürlich erfüllt CMI STS sämtliche aktuellen Sicherheitsstandards und setzt dabei auf bekannte und etablierte Security Standards wie OpenID Connect und WS Federation.



6.2 Ohne CMI Security Token Service (STS)

Die CMI-Applikationen unterstützen einen Login via:
- Built-In (CMI-Benutzer_in)
- Active Directory

6.3 Mit CMI Security Token Service (STS)

Wenn die Applikationen mit einem STS betrieben werden, werden die folgenden Varianten unterstützt:
- Built-In (CMI-Benutzer_in) mit optionalem 2. Faktor via TOTP
- WS-Federation (ADFS)
- OpenId Connect Authorization Code Flow (Office 365, Azure AD)

Mit dem Release 22.0 ist CMI STS 2.x sowie CMI STS 3.0 kompatibel.

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

7 Hardwarevoraussetzungen

7.1 Web-/Publikations-/Relay-/STS-Server

	Mindestanforderung	Empfehlung
Prozessor	1.8 GHz	2.4 GHz oder höher
Arbeitsspeicher	64bit: 4 GB	64bit: 8 GB

Hinweis: Für CMI AIS Web Client sollten mindestens 8 GB (pro Mandant) vorhanden sein. Empfohlen werden 16 GB (pro Mandant).

8 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)
Internal	DMZ	LAN	tcp: (Owin public/private)	alle

Der Port für den Zugriff auf den CMI.CDWS.Service (DataService) ist als Beispiel zu verstehen. Diese Ports sind 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.

9 Datensicherheit

9.1 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 Endbenutzenden und Firewall

9.2 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.

9.3 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

10 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.