

St. Wolfganger Krankenhaustage 17.-18. Juni 2026



CompuGroup
Medical

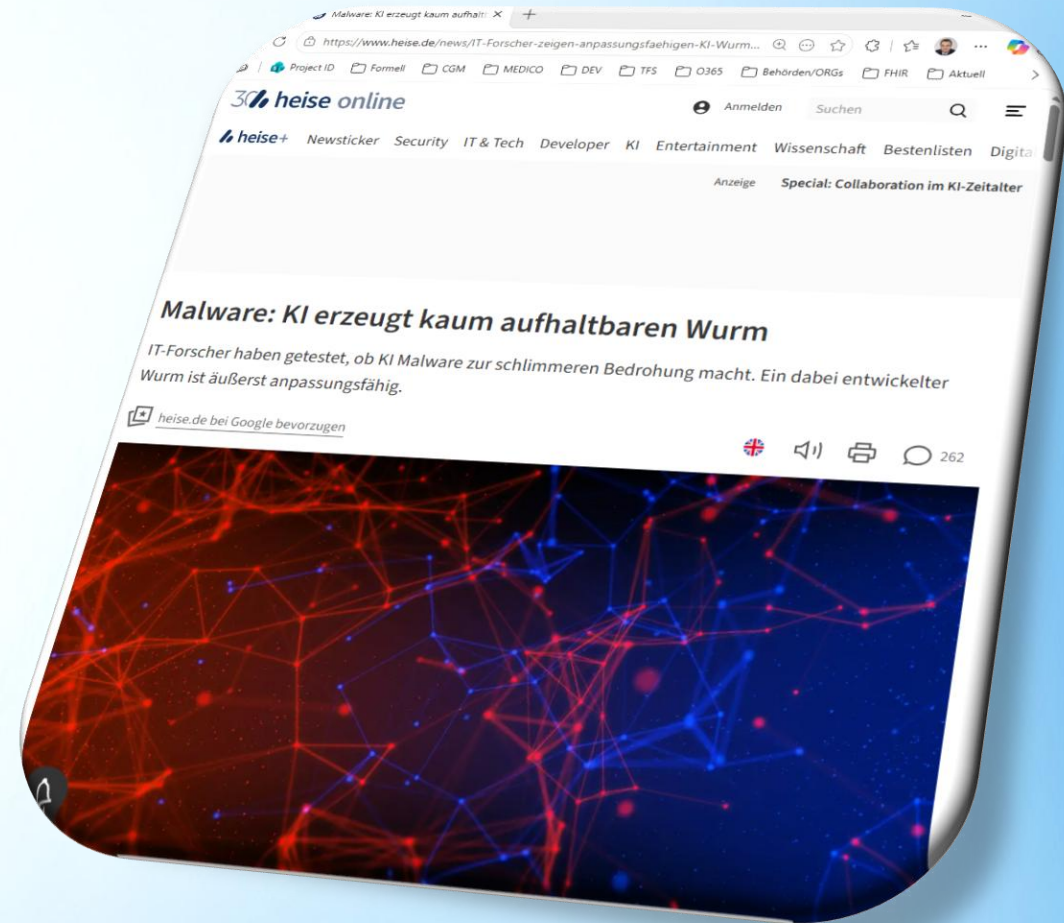
SECURITY

in CGM MEDICO 30.0

Was wir so lesen ...



Quelle.mpg.de (Max-Planck-Gesellschaft)



Quelle: Heise.de

Agenda

- 1 Szenarien
- 2 Sicherheitselement für Windows-Clients
- 3 Verschlüsselung und Zertifikate
- 4 Zentraler Linux Applikationsserver
- 5 Verschiedenes

Wir sind heute für Sie da.



Dr.med. Jörg Mehlbrech

CGM MEDICO Solution Architekt



Stephan Wimmer

Team Lead

Technical Consulting
& Infrastructure

SZENARIEN

Hauptziele von Cyber-Kriminellen

Szenarien

Hauptfokus von CGM MEDICO:
Normale Anwender auf den angedachten Wirkungskreis einzuschränken.

Anwender sollen mit User-Rechten, niemals mit Admin-Rechten arbeiten.

Cyber-Kriminelle zielen auf



Lösegelderpressung bei System-Verschlüsselung



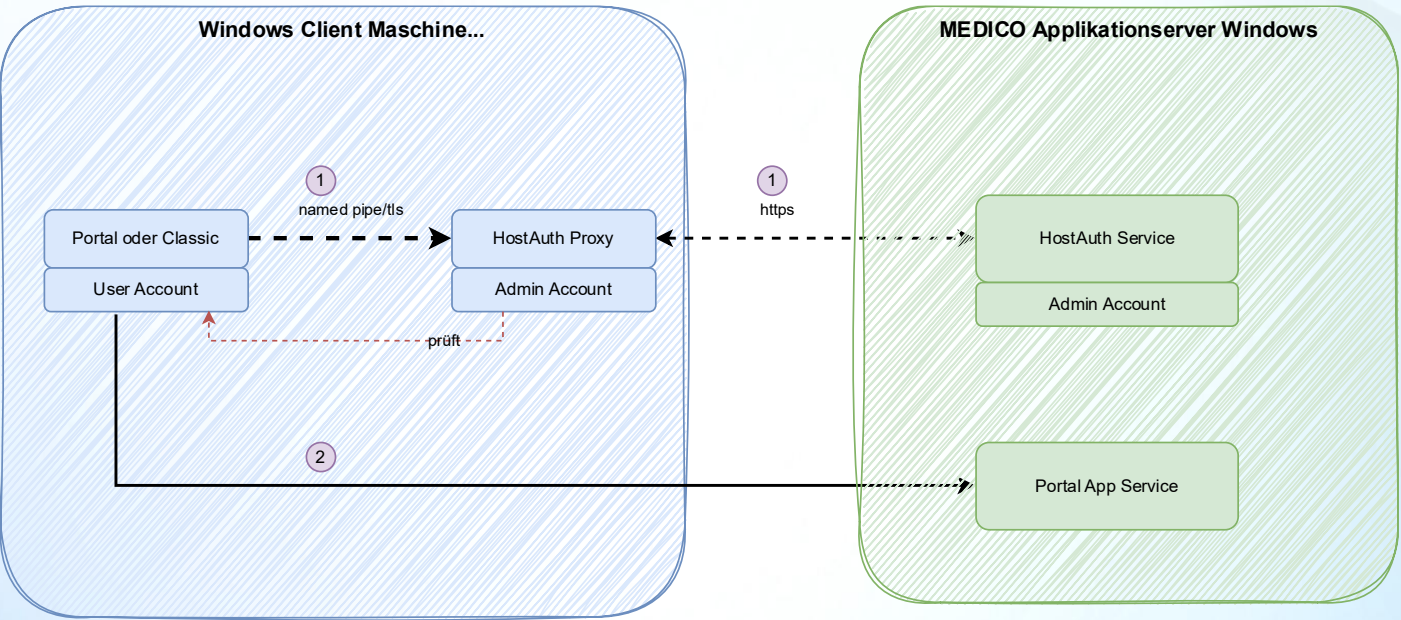
Erpressung mit entwendeten Gesundheitsdaten



SICHERHEITSELEMENT

Windows Clients und Server

Sicherheitselement



... stellt sicher, dass nur ein MEDICO Client mit MEDICO Servern kommuniziert.

Schutz vor Manipulation durch User indem HostAuth Proxy als Admin läuft.

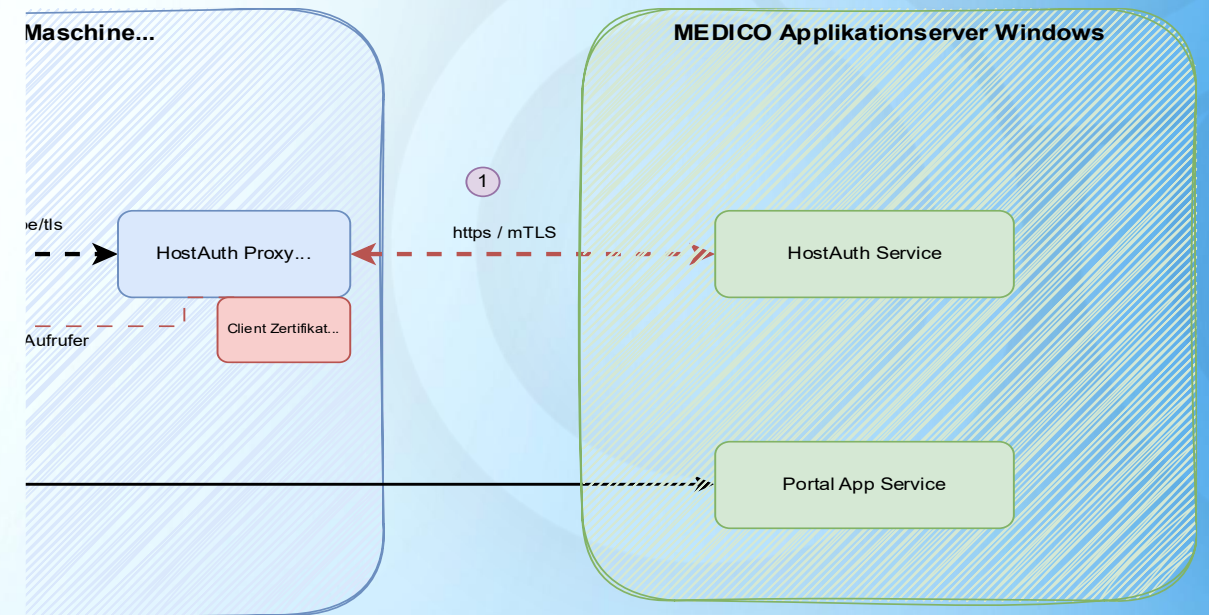
HostAuthProxy	wird als Windows Dienst automatisch von medicoreg installiert
HostAuth Service	Neuer Port 11093 auf Applikationsserver (wie Center Service - unabhängig von Manda... <small>text is not SVG - cannot display</small>

Sicherheitselement

Weiterentwicklung in 30.0: Verwendung **Client Zertifikate für Maschine** (mutmaßlich **mTLS**)
(Wird Pflicht werden)

Einrichtung via
Active Directory Client Services (ADCS)

→ Serviceauftrag an Gruppe TCI über Vertrieb



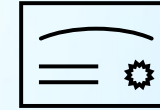
VERSCHLÜSSELUNG

Data In-Transport und Zertifikate

Transport-Verschlüsselung in MEDICO 30.0

Einheitliche Verwendung

- Einheitliche Zertifikate, mandanten-übergreifend
- TLS – short lived (~ 6 Tage, danach Austausch)
- Algorithmus („Cipher-Suite“) einstellbar
RSA und elliptic curves (RSA-4096 default)
- KEINE Speicherung im Windows Cert Store



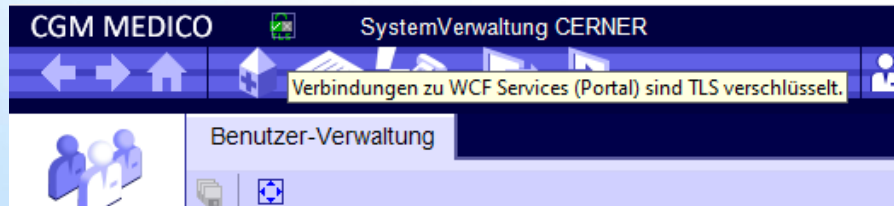
Alle Zertifikate ändern sich mit 30.0

Touch: ausgenommen

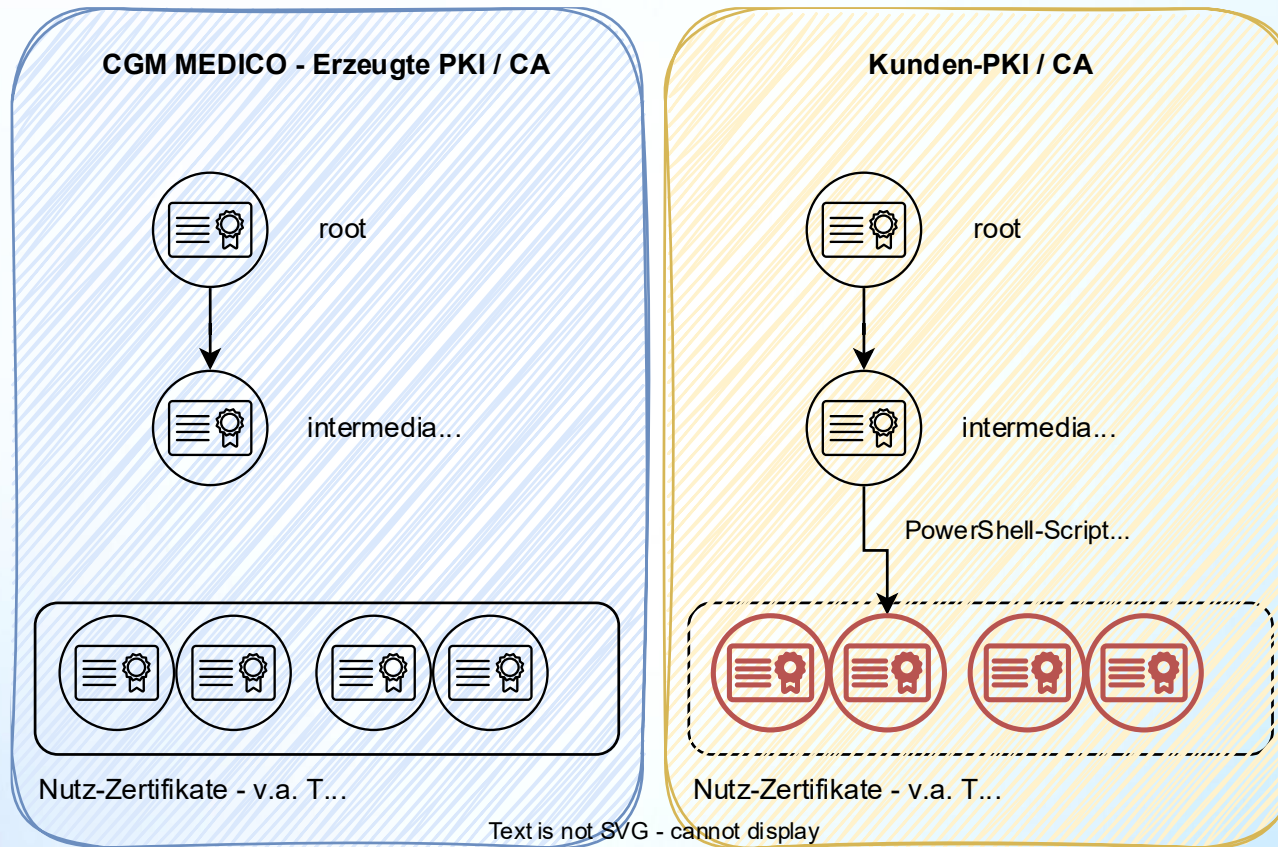
Transport-Verschlüsselung in MEDICO 30.0

Verwendung in

- *Classic („DNET“)* – kam mit 29.01
nicht clusterfähig
- Zwischen Portal und Portal App Service
- HTTPS Services
 - Center Service
 - Auth Service
 - FHIR ISIK / Partner
 - Browser Service
 - WebData Service
 - HostAuth Service (Ab 30.0)



Transport-Verschlüsselung in MEDICO 30.0

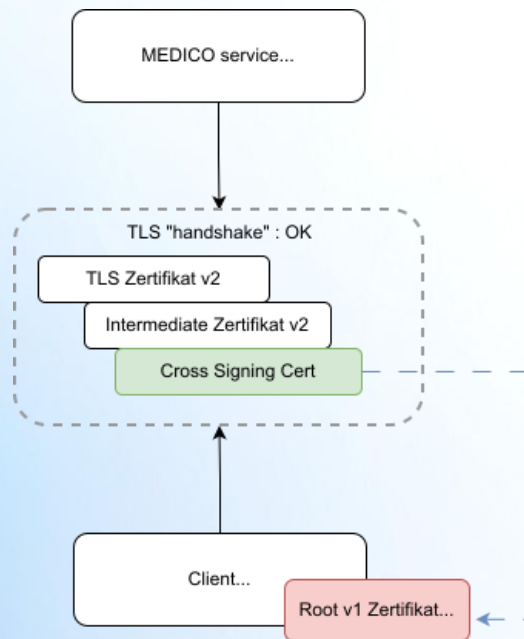


PowerShell Script Einrichtung
→ Serviceauftrag an Gruppe TCI über Vertrieb

Verschlüsselung in MEDICO 30.0

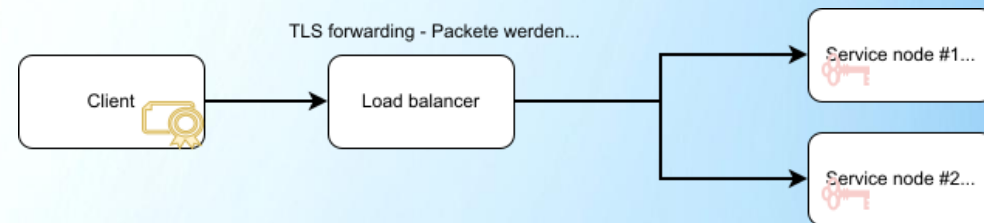
FHIR ISIK und FHIR Partner-Plattform

- TLS Kompatibilität
Cross-Signing Zertifikate



Clustering

- TLS Terminierung im Backend



Verschlüsselung : Screenshot – MEDICO PKI

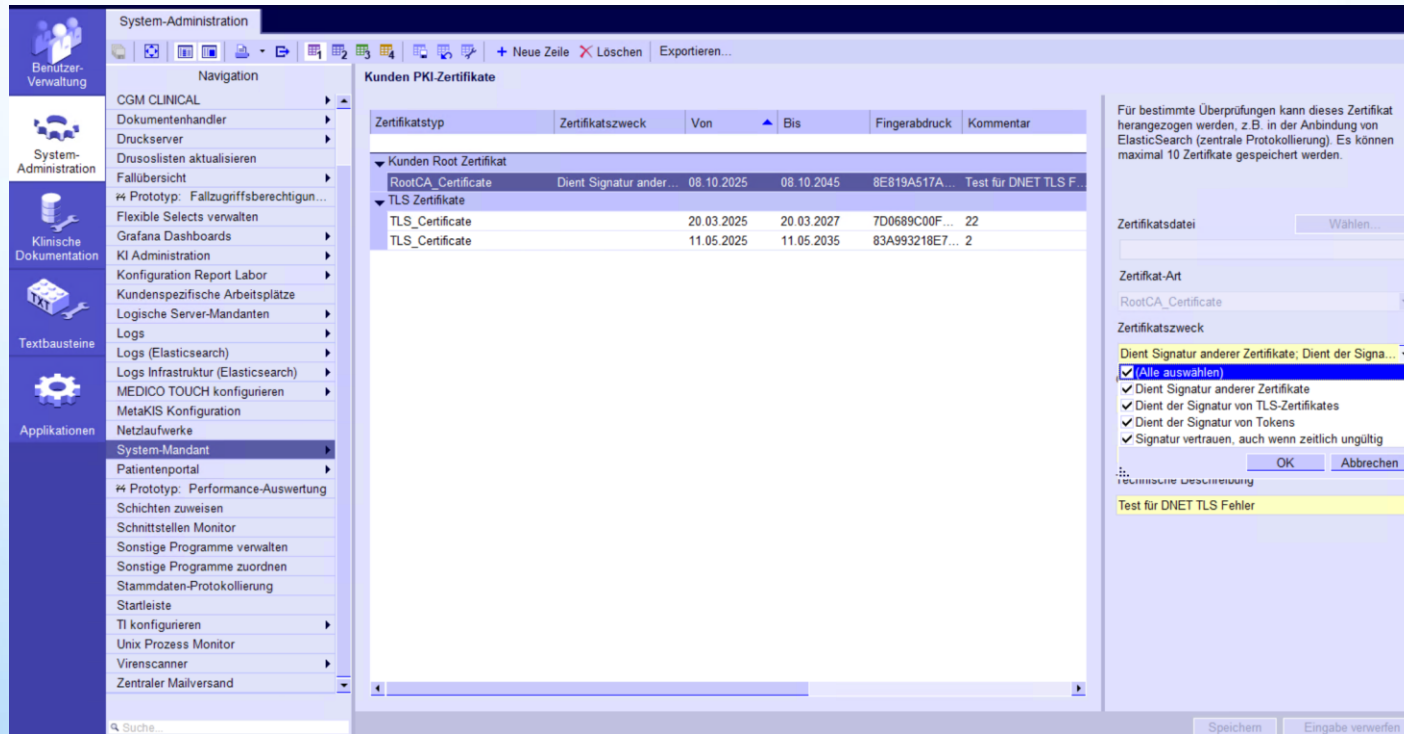
The screenshot displays the 'MEDICO PKI-Zertifikate' management interface. On the left is a navigation sidebar with categories: Benutzer-Verwaltung, System-Administration, Klinische Dokumentation, Textbausteine, and Applikationen. The main area shows a table of certificates with columns: Zertifikatstyp, Maschine, Von, Bis, Fingerabdruck, For..., Kommentar, Angelegt am, Angelegt von, Zuletzt geändert am, and Geändert von. The table is organized into sections: Root Zertifikat für System-Mandanten, MEDICO Intermediate Zertifikat, Zertifikat für Token-Signaturen, and TLS Zertifikate. A search bar is at the bottom left of the table area.

Zertifikatstyp	Maschine	Von	Bis	Fingerabdruck	For...	Kommentar	Angelegt am	Angelegt von	Zuletzt geändert am	Geändert von
MEDICO PKI-Zertifikate										
▼ Root Zertifikat für System-Mandanten										
RootCA_Cert...	ALL	08.10.2025	08.10.2045	8E819A517A...	PEM	RSA - 4096 Bits	08.10.2025	MEDICOCRTS...	08.10.2025	
▼ MEDICO Intermediate Zertifikat										
Intermediate_...	ALL	08.10.2025	08.10.2035	C4F34CEF08...	PEM	RSA - 4096 Bits	08.10.2025	MEDICOCRTS...	08.10.2025	
▼ Zertifikat für Token-Signaturen										
Token_Certifi...	ALL	06.02.2026	06.02.2027	D011A3D1A3...	PEM	RSA - 4096 Bits	06.02.2026	HOSTAUTHSVC	06.02.2026	
▼ TLS Zertifikate										
TLS_Certificate	dfeat5rh	08.10.2025	08.10.2026	80B3A09204...	PEM	RSA - 4096 Bits	08.10.2025	MEDICOCRTS...	08.10.2025	
TLS_Certificate	dfeat5rh	03.12.2025	03.12.2026	67B07DA32B...	PEM	RSA - 4096 Bits	03.12.2025	MEDICOCRTS...	03.12.2025	
TLS_Certificate	dfeat5rh	03.12.2025	03.12.2026	4CBC21E5...	PEM	RSA - 4096 Bits	03.12.2025	MEDICOCRTS...	03.12.2025	
TLS_Certificate	dfeat5rh	04.12.2025	04.12.2026	CCEC602A...	PEM	RSA - 4096 Bits	04.12.2025	MEDICOCRTS...	04.12.2025	
TLS_Certificate	dnext2rh	27.02.2026	27.02.2027	CAB0D2E353...	PEM	RSA - 4096 Bits	27.02.2026	HOSTAUTHSVC	27.02.2026	
TLS_Certificate	dfeat5ut.medi...	09.06.2026	09.06.2026	CC214B942F...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ui01.me...	09.06.2026	09.06.2026	D5073464118...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5partner....	09.06.2026	09.06.2026	BDBE828C2B...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ut.medi...	09.06.2026	09.06.2026	36A5D0A98A...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ui01.me...	09.06.2026	09.06.2026	721B012DF31...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5partner....	09.06.2026	09.06.2026	71A5D76E3B...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ut.medi...	09.06.2026	09.06.2026	E04DD2D78C...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ui01.me...	09.06.2026	09.06.2026	6CC140917F8...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5partner....	09.06.2026	09.06.2026	E634AFEDE1...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ut.medi...	09.06.2026	09.06.2026	483156353AF...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ui01.me...	09.06.2026	09.06.2026	0C6102408A...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5partner....	09.06.2026	09.06.2026	C3DEEDCD3...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ui01.me...	09.06.2026	09.06.2026	1BA889B624...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ui01.me...	09.06.2026	09.06.2026	615F12091F5...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ut.medi...	09.06.2026	09.06.2026	513C9D56C5...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ui01.me...	09.06.2026	09.06.2026	C9C93A4E9C...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5partner....	09.06.2026	09.06.2026	7415FA8D7B...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ui01.me...	09.06.2026	09.06.2026	F05B86C58E...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ut.medi...	09.06.2026	09.06.2026	E2407C346C...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	
TLS_Certificate	dfeat5ui01.me...	09.06.2026	09.06.2026	210A5D01A5...	PEM	RSA - 4096 Bits	09.06.2026	HOSTAUTHSVC	09.06.2026	

Zugriff und **Export** auf Zertifikate, die MEDICO erzeugt hat

CA wird auch erzeugt, wenn Kunde eigene Zertifikate veranlasst. Verwendung für einzelne Nicht-Kunden Zertifikate.

Verschlüsselung : Screenshot – Kunden PKI



Import Kunden-CA Zertifikate.

Verwendung:

(1) TLS für MEDICO-Server

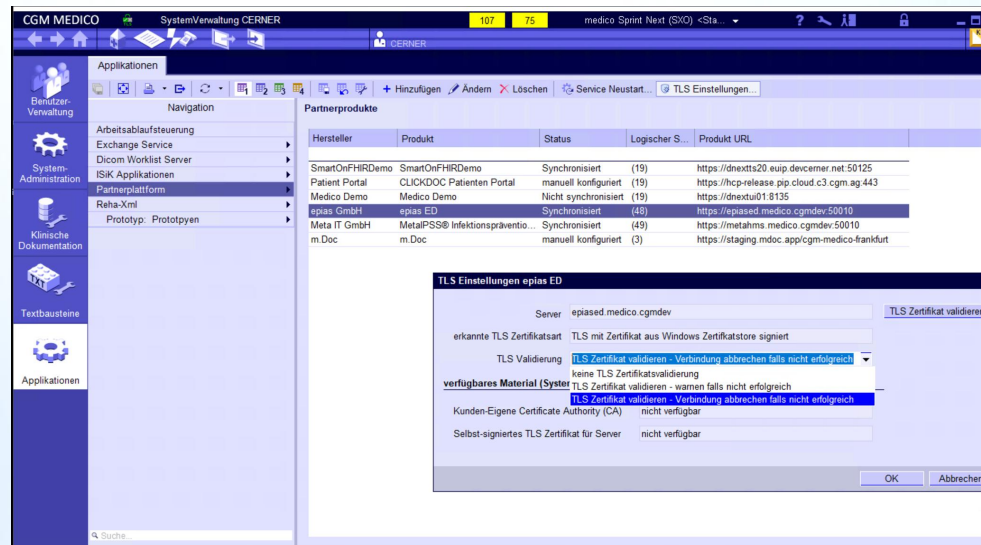
Diese werden auch hier angezeigt

(2) Validierung nicht-MEDICO Server

z.B. Partner-Plattform, elasticSearch

Verschlüsselung zu externen Server

- Datenbank – Kommunikation zu Oracle, Ingres, Postgres
→ Verschlüsselung dringend empfohlen
- Partner Plattform (epias, IPSS)
Validierung TLS muss eingeschaltet werden – dringend empfohlen



LINUX HOST

Verschiedene Sicherheitsthemen

Grundsätzliches – Linux Host App Server

- Nutzung **nur** durch (logische) Admins zugelassen
 - Das dürfen nur root, dps bzw. User der Gruppe loesung
- Dateiberechtigung
 - Ebenfalls nur dps, loesung
 - Für /DPS in 30.0 automatisch gesetzt, jedoch nicht dps_worklst
- SMB v1, v2 **abschalten**

Nmap (mit NSE-Engine): Das weltweit meistgenutzte Tool. Mit dem Skript `--script smb-protocols` prüft es vollautomatisch IP-Ranges (z. B. `192.168.1.0/24`) ab und listet Systeme mit SMBv1/v2 auf.  +1



Linux Host - Härtung




- Data-In-Rest Verschlüsselung
 - Nutzung SAN/Hypervisor oder LuKS -> Möglich bei Servermigrationsprojekten
- Durchführung von MITSEC Projekte
 - Deaktivierung nicht genutzter Benutzer (OS, SAMBA, DB) und unsichere Protokolle (z.B. FTP)
 - Einführung von ServiceAccounts
 - Setzen sicherer Passwörter
- Dateiberechtigung
 - Härtung der Dateiberechtigungen von Scripten/Lösungspaketen/Produktbestandteile durch CGM (z.B. Zugriffe auf dps_worklst, Systemanalysescripts,...)

Linux Host - NTLM

NTLM Deprecation & CGM MEDICO-Betrieb

- NTLM-Ende: Microsoft stellt den Support für NTLM mit Windows Server 2025 ein
- Die Konsequenz: Ohne Kerberos-/AD-Anbindung ist kein SAMBA-Zugriff mehr auf die CGM MEDICO Linux-Applikationsserver möglich
- Das Kernproblem: Die aktuelle Kerberos/AD-Integration (Microsoft vs. Open Source) läuft instabil - dies gefährdet die CGM MEDICO-Verfügbarkeit

Dringender Handlungsbedarf / mittelfristige Ziele

RISIKOBEREICH	STATUS	MASSNAHME / ZIEL
Infrastruktur-Freigaben	 Kritisch	Vollständiger Verzicht -> Migration von z.B. pc_integ
DPER-Schnittstellen	 Kritisch	Eliminierung direkter Zugriffe -> Migration auf Embedded MDM
CGM MEDICO	 In Prüfung	Evaluierung weiterer Maßnahmen durch CGM

VERSCHIEDENES

Sicherheitsthemen

Verschiedenes

- **PC_KUNDE:\server Verzeichnis**
Kapselt Binaries und Konfigurationen weg, die Endnutzer nicht mehr sieht
- **TLS-Handshake – MEDICO Services**
→ Clients benötigen nur Root-Zertifikat
- **Passwort Hash**
ARGON2 – Standardmäßige Verwendung
- **Ausgeschiedene Benutzer**
Deaktivierung von MEDICO User Account nach Zeit ohne Anmeldung

Applikationsserver Setup (30.0)

Logische Server-Mandanten

Ser...	Clustername	Servertyp	FQDN
1	DefaultFHIRPartner	Server	DNEXTUI01.m...
2	FHIR Partner (1)	Server	DNEXTUI04.m...
3	FHIR Partner (2)	Server	N-BPSHPV2
4	pap	Server	aaa bbb
5	FHIR Partner (8)	Server	N-3RDS8S3
6	BIExportServer	Server	DNEXTUI03.m...
7	DNEXT-MC	Cluster	DNEXT-MC
8		Server	DNEXTWFM...
9		Server	DNEXTUT.ME...
10		Server	N-39Y9S64.LO...
11		Server	N-39Y9S64

Basisangaben

Server-ID: 11

Type: Cluster

Logischer FQDN: DNEXT-MC

Name: DNEXT-MC

Kommentar: automatisch generiert

Mitglieder (nur bei Cluster)

FQDN:

- dnextui01.medico.cgmedev
- dnextui03.medico.cgmedev
- dnextui02.medico.cgmedev

Funktionen des logischen Servers

Funktion des logischen Servers	Aktiv
FHIR Service / Partner Platform Profile	✓
Portal App Service	✓

Logische Server-System Mandanten

Ser...	Clustername	Servertyp	FQDN
1	DNEXT-MC	Cluster	DNEXT-MC
2		Server	DNEXTUT.MEDICO.CGMD
4		Server	N-39Y9S64.LOCAL
5		Server	N-39Y9S64

Basisangaben

Server-ID: 1

Type: Cluster

Logischer FQDN: DNEXT-MC

Name: DNEXT-MC

Kommentar: automatisch generiert

Mitglieder (nur bei Cluster)

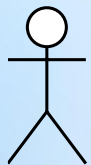
FQDN:

- dnextui01.medico.cgmedev
- dnextui03.medico.cgmedev
- dnextui02.medico.cgmedev
- n-39y9s64

Funktionen des logischen Servers

Funktion des logischen Servers	Aktiv
Center Service	✓

Festlegen, was gestartet wird



Setup: Festlegen, ob gestartet wird...

Windows Server

«Applicationserver»...

Text is not SVG - cannot display



Herzlichen
DANK



KONTAKT

CGM Clinical Europe GmbH
Maria Trost 21
56070 Koblenz

europe.clinical.info.de@cgm.com
www.cgm.com.de

Disclaimer

Die Informationen des vorliegenden Dokumentes sind vertraulich und urheberrechtlich geschützt. Sie dürfen ohne Genehmigung der CGM Clinical Europe GmbH nicht an Dritte weitergegeben werden.

Sämtliche Angaben geben die Sicht zu dem Zeitpunkt wieder, zu dem sie getroffen wurden. Sie unterliegen diversen Risiken und Unwägbarkeiten, durch die die tatsächlichen Ergebnisse von den angestrebten Zielsetzungen abweichen können. Alle in Software-Screenshots oder in anderer Art und Weise in diesem Dokument dargestellten Personen und Patientendaten sind rein fiktiv.

Die Beschreibungen und Informationen in diesem Dokument begründen keine zugesicherten, bzw. definierten Eigenschaften oder eine rechtliche Verpflichtung zur Auslieferung von Programmen, Modulen oder Funktionen. Sie können von

CGM Clinical Europe GmbH jederzeit aus beliebigen Gründen und ohne vorherige Ankündigung geändert werden. Im Übrigen verweisen wir auf unsere Allgemeinen Geschäftsbedingungen in der jeweils gültigen Fassung.

Die Software Module CGM MEDICO Fieberkurve und CGM MEDICO Assessment und Scoring sind Medizinprodukte der Klasse IIa gemäß der Verordnung (EU) 2017/745 (MDR) und dürfen nur entsprechend ihrer Zweckbestimmung angewandt werden.

CE 0483

Copyright © 2025 CGM Clinical Europe GmbH – Alle Rechte vorbehalten. CGM, CGM MEDICO, CGM MEDICO TOUCH sind eingetragene Marken von CGM in Deutschland und/oder anderen Ländern. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

Kontakt

CGM Clinical Europe GmbH

Maria Trost 21

56070 Koblenz

cgm.com/medico

cgm.com/de