

# VSDM 2.0 – ZETA & POPP IM ZUSAMMENSPIEL MIT DER EPA

## Referenten

Torben Kalz – VP MEDICO

Andreas Wulf – Product Owner

St. Wolfgang Krankenhausstage 2026

## Überblick

- ▶ Was ändert sich mit VSDM 2.0?
- ▶ Zero Trust & PoPP erklärt
- ▶ Die Brücke zur ePA 3.1.3

# 20 Jahre Kartenstecken



**20 Jahre Kartenstecken –  
und, hat's Spaß gemacht?**

# Was sich ändert – in 60 Sekunden

Drei fundamentale Unterschiede zwischen VSDM 1.0 und 2.0:

<b>DATEN-QUELLE</b>	eGK stecken ► Konnektor ► Kassendienst ► VSD
	PoPP-Token ► FHIR R4 ► VSD direkt vom Fachdienst
<b>NETZ-WERK</b>	Primärsystem ► VPN-Tunnel ► TI-Netz ► Fachdienst
	ZETA Client ► ZETA Guard prüft Token ► Fachdienst (Internet)
<b>FOR-MAT</b>	SOAP Request ► XML Payload ► XML Parsing
	REST GET ► FHIR R4 / JSON ► HTTP ETag-Caching

# Zero Trust – einfach erklärt




Bisher hatten alle im Krankenhaus einen Generalschlüssel (VPN). Wer drin war, kam überall hin. Zero Trust ändert das grundlegend.

## Bisher: VPN = Generalschlüssel

- ✗ Einmal verbunden = Zugang zu allem
- ✗ Keine Prüfung einzelner Anfragen
- ✗ Wenn der Tunnel steht, wird vertraut
- ✗ Ein Angreifer im Netz hat vollen Zugriff

## Neu: Zero Trust = Einzelprüfung

- ✓ Jede Anfrage wird einzeln geprüft
- ✓ Wer bist du? Darfst du das? Ist das Gerät sicher?
- ✓ Kurzlebige Tokens statt Dauersitzung
- ✓ Selbst im eigenen Netz: kein blindes Vertrauen

 MEDICO fragt an →  ZETA Guard:  
„Ausweis bitte!“ →  Zugriff gewährt

Wie eine Ausweiskontrolle bei jeder Tür – statt einem VIP-Bändchen für das ganze Gebäude.

# „Aber ist das ohne VPN überhaupt sicher?“

Ja, sogar sicherer. Statt einer Mauer (VPN) gibt es jetzt mehrere unabhängige Sicherheitsschichten.

## Schicht 1: mTLS

- ✓ Jede Verbindung TLS-verschlüsselt
- ✓ mTLS: auch der Client weist sich per Zertifikat aus
- ✓ Beide Seiten beweisen ihre Identität

## Schicht 2: ZETA Guard

- ▶ PEP prüft jede einzelne Anfrage
- ▶ PDP entscheidet anhand aktueller Regeln
- ▶ Keine Anfrage ohne gültiges Access Token

## Schicht 3: Client-Attestation

- ▶ Einmalige Registrierung am Authorization Server
- ▶ App-Integrität, OS/HW-Eigenschaften geprüft
- ▶ Kompromittierte Geräte werden abgewiesen

## Schicht 4: Überwachung (TI-SIEM)

- ▶ Alle Zugriffe in Echtzeit überwacht
- ▶ Policies sofort aktualisierbar
- ▶ Bei ZETA: jede Aktion ist sichtbar

VPN schützt den Weg – Zero Trust schützt das Ziel.

# PoPP – Proof of Patient Presence

Der Patient ist da – und das System weiß es.

## Stufe 1 – eGK + Kartenterminal

- ✓ eGK wird am Kartenterminal gesteckt
- ✓ PoPP-Service erzeugt ein PoPP-Token
- ✓ Enthält: KVNR + IK-Nummer
- ✓ Token wird als Bearer-Token bei jeder Anfrage mitgesendet

## Stufe 2 (geplant)

- ▶ GesundheitsID statt physischer Karte
- ▶ Patient authentifiziert sich digital
- ▶ Gleicher Token-Mechanismus
- ✓ Keine physische Karte mehr nötig

**JWT**  
Token-Typ

**KVNR+IK**  
Inhalt

**24h**  
Gültigkeit

# So sieht's im MEDICO aus

Der neue Aufnahme-Workflow in drei Schritten:

1. eGK am Terminal → 2. PoPP-Token erzeugt → 3. VSD abgerufen

## Ablauf im Detail

- ▶ Patient erscheint → eGK wird gesteckt
- ▶ PoPP-Service erzeugt Token mit KVNR + IK
- ▶ Fachdienstlokalisierung → richtiger Kassendienst
- ▶ VSD-Abruf via FHIR R4 → Stammdaten aktuell
- ▶ Fall anlegen → Versicherungsstatus geprüft

# Die Brücke: PoPP öffnet die ePA

PoPP ist nicht nur für VSDM –  
es ist der Schlüssel zur ePA.

PoPP-Token → Versorgungskontext → ePA-Befugnis (vom Fachdienst erstellt) → ePA-Zugriff ✓

## So funktioniert es

- ▶ ePA 3.1.3 braucht Zugriffsbefugnisse für jede LEI
- ▶ PoPP-Token liefert den Versorgungskontext
- ✓ Befugnis wird automatisch erstellt

## 🔑 Bearer-Token & Befugnis

- ▶ PoPP-Token (JWT) als Bearer im HTTP-Header
- ▶ Fachdienst prüft Token → erzeugt ePA-Befugnis
- ▶ PoPP-Token signiert mit ES256 (HSM-Schlüssel)
- ▶ Enthält: KVNR, IK, Zeitstempel, Proof-Methode

**24h**  
Token-Gültigkeit

**gemSpec**  
Quelle: PoPP Service





# Was passiert, wenn das Token nicht gültig ist?

Fünf realistische Szenarien – und wie MEDICO damit umgeht.

	<b>Token abgelaufen (24h)</b> Patient war gestern da – heute neuer Besuch ohne erneuten Check-in.	<ul style="list-style-type: none"><li>✓ MEDICO erkennt abgelaufenes Token automatisch</li><li>✓ Aufforderung: „Bitte eGK erneut stecken“</li></ul>
	<b>Kein Token vorhanden</b> eGK nicht gesteckt, Kartenterminal defekt oder PoPP-Service nicht erreichbar.	<ul style="list-style-type: none"><li>✓ Fallback auf VSDM 1.0 – Konnektor springt ein</li><li>✓ MEDICO zeigt klaren Status</li></ul>
	<b>Signaturprüfung fehlgeschlagen</b> Token manipuliert oder technisch defekt. ZETA Guard weist ab (HTTP 401).	<ul style="list-style-type: none"><li>✓ ZETA Guard blockt – kein Datenzugriff</li><li>✓ Neues Token anfordern (erneuter Check-in)</li></ul>
	<b>SMC-B abgelaufen oder gesperrt</b> LEI-Identität ungültig – PoPP-Service verweigert Token-Ausstellung.	<ul style="list-style-type: none"><li>✗ Betrifft ALLE Arbeitsplätze!</li><li>✓ Neue SMC-B beim Kartenherausgeber beantragen</li></ul>
	<b>Fachdienst / Internet nicht erreichbar</b> Token gültig, aber ZETA Guard oder Fachdienst antwortet nicht.	<ul style="list-style-type: none"><li>✓ Automatischer Retry mit Exponential Backoff</li><li>✓ Fallback auf VSDM 1.0 über Konnektor</li><li>▶ Vorbauen: Netzwerk-Monitoring + redundanter Internetzugang</li></ul>

# Was bringt ePA 3.1.3?

Endlich wissen, was der Hausarzt verordnet hat.

## Digitaler Medikationsprozess

- eML – Elektr. Medikationsliste
- eMP – Elektr. Medikationsplan
- Aktuelle Medikation – kassenübergreifend

## Volltextsuche (ab Mitte 2027)

- Suche über alle Dokumente in der ePA
- Forschungsdatenexport (FDZ)

## Mehrwert für den Arzt

- ✓ Medikation sofort sichtbar
- ✓ Arztbriefe in MEDICO abrufbar
- ✓ Kein Fax-Ping-Pong mehr

# Zeitplan – wann kommt was?

Die Pilotphase läuft ohne MEDICO, bis die meisten Kassen umgestellt sind – wir beobachten und bereiten vor.

**30.06.2026** Pilot VSDM 2.0 – 1 große Kasse + mind. 1 KIS/PVS (ohne MEDICO)

**Q3 2026** Erweiterung auf weitere Kassen & Primärsysteme

**Q3 2026** ePA 3.1.3 Teil 1 – Pilot (dgMP, eML, eMP)

**Okt 2026** ePA 3.1.3 Teil 1 – Bundesweiter Rollout bis zum Jahreswechsel

**Jan 2027** Zeta 1.0 & PoPP 1.0

**Q2 2027** VSDM 2.0 – Live (verschoben gematik am 10.06.26)  
ePA 3.1.3 Teil 2 – Bundesweiter Rollout

## Wie funktioniert der Parallelbetrieb?

- VSDM 1.0 läuft weiter – Konnektor + eGK wie bisher
- Kassen schalten VSDM 2.0 schrittweise frei
- MEDICO prüft per DNS-SRV-Lookup der IK-Nr. ob VSDM 2.0 aktiv
  - ✓ DNS-Antwort vorhanden → neuer Pfad (FHIR/REST via ZETA)
- Kein DNS-Eintrag → automatischer Fallback auf Konnektor
  - ✓ Für den Anwender ändert sich nichts

# Was müssen Sie tun?

Die meiste Hardware haben Sie schon.

## **Konnektor / TI-Gateway**

Aktuell? Firmware-Update ggf. erforderlich.

## **Kartenterminal(e)**

PoPP braucht eHealth-Terminal.

## **SMC-B**

Gültig und freigeschaltet?

## **Netzwerk – Zero Trust braucht Internet**

Kein geschlossenes TI-Netz mehr. Jede Anfrage wird einzeln per Token authentifiziert und über das öffentliche Internet gesendet. Der ZETA Guard prüft: Wer fragt an? Ist das Token gültig?

## **TI 2.0 Client – wo läuft er?**

- ▶ Lokaler REST-Proxy, kapselt Konnektor-SOAP
- ▶ Auf MEDICO AppServer oder dediziertem TI-Server
- ▶ Konnektor + KT bleiben erforderlich

 **Fazit: Wenig neue Hardware, aber Netzwerk, TI 2.0 Client & Software vorbereiten.**

# Wo läuft der Ti 2.0 Client? – 3 Szenarien

Je nach Arbeitsplatz-Typ unterscheidet sich die Topologie – der REST-API-Aufruf aus MEDICO bleibt identisch.

## A: Desktop-Arbeitsplatz

- ✓ 1 Client pro PC (gematik-Präferenz)
- ✓ Geräteattestierung (TPM, OS)
- ✓ API nur über localhost
- ✓ Höchste Zero-Trust-Konformität

Empfohlen

## B: Virtueller Arbeitsplatz

- ▶ 1 Client pro Server/VM
- ▶ Systemdienst läuft persistent
- ▶ API über Netzwerk (nicht nur localhost)
- ▶ Shared Sessions: alle User teilen Token-Pool

KH-typisch

Kernprinzip: Der ZETA Client läuft immer dort, wo der Konnektor erreichbar ist – für MEDICO ändert sich am REST-Aufruf nichts.

# Ausblick: Die kartenlose Zukunft

Notaufnahme Freitagnacht – und niemand sucht eine Karte.

## GesundheitsID

- ▶ Digitale Identität auf dem Smartphone
- ▶ Gespeichert in der Krankenkassen-App
- ▶ Basiert auf dem sektoralen IDP der Kasse
- ▶ Patient authentifiziert sich aktiv

## Mobile Szenarien

- ✓ Hausbesuche – Arzt identifiziert Patient vor Ort
- ✓ Rettungsdienst – Patientenakte sofort verfügbar
- ✓ Ambulante Pflege – kein Kartenterminal nötig

## TI 2.0 als Plattform

Nicht nur VSDM – auch KIM 2.0, eRezept, ePA und weitere Fachdienste laufen künftig über ZETA. Die Zero-Trust-Architektur wird zum Fundament der gesamten TI.

# 3 Take-Aways

1

## Zero Trust ist sicherer UND einfacher

Kein VPN-Tunnel mehr – jede Anfrage wird individuell gesichert. Weniger Infrastruktur, mehr Sicherheit.

2

## PoPP verbindet VSDM + ePA – ein Token, zwei Welten

Der Versorgungskontext öffnet automatisch die ePA-Befugnis. Keine Extra-Schritte.

3

## Neue Prinzipien ersetzen die alten

VPN-Tunnel → Zero Trust (ZETA) | SOAP/XML → REST/FHIR R4 | eGK lesen → PoPP-Token | Konnektor lokal → TI 2.0 Client

**Fragen? Wir freuen uns auf die Diskussion.**

## 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](https://cgm.com/medico)

[cgm.com/de](https://cgm.com/de)