

Z1

SCHULUNGS- UNTERLAGEN

TELEMATIKINFRASTRUKTUR

WISSENS- VORSPRUNG –

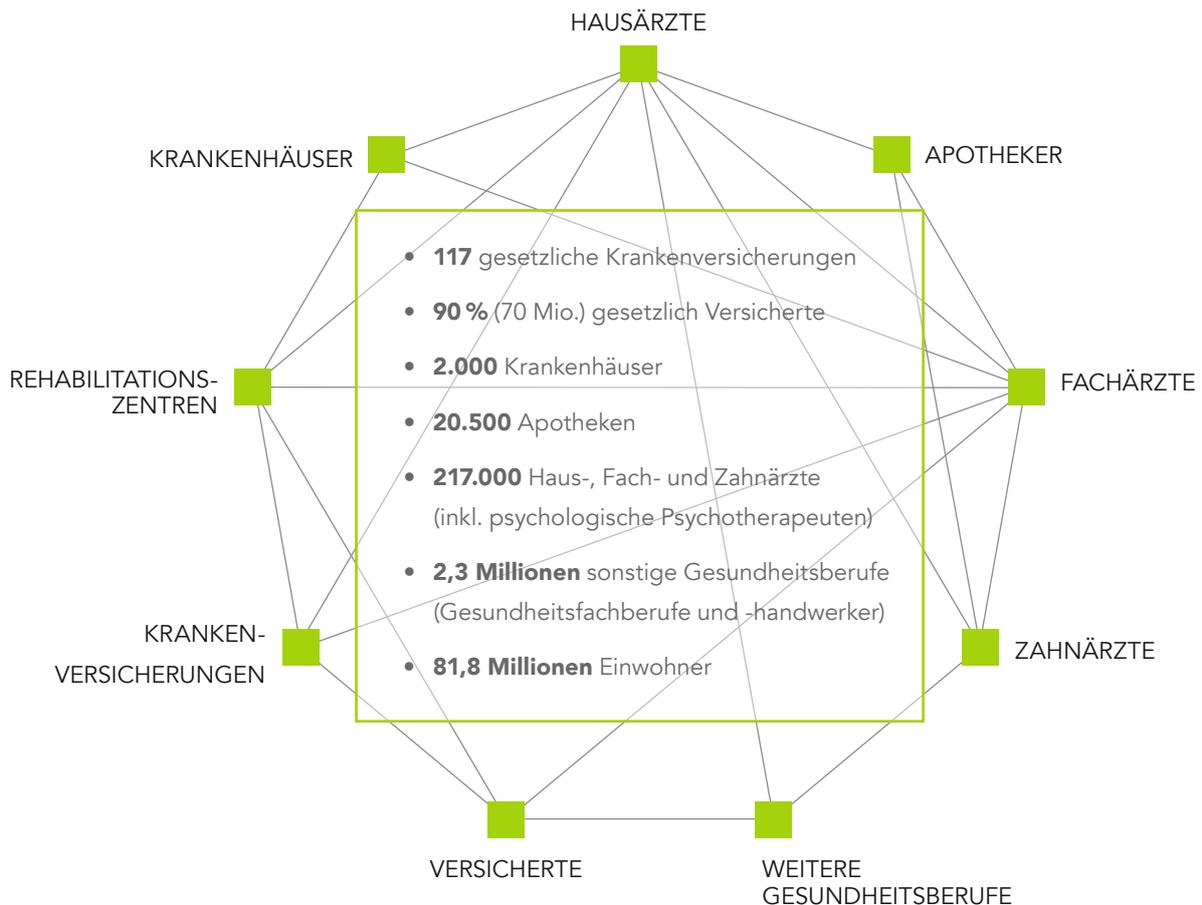
Wir können E-Health.

Synchronizing Healthcare



CompuGroup
Medical

ZIEL DER TELEMATIKINFRA- STRUKTUR IST EIN VERNETZTES GESUNDHEITSSYSTEM



VORTEILE VON eGK UND TELEMATIKINFRASTRUKTUR

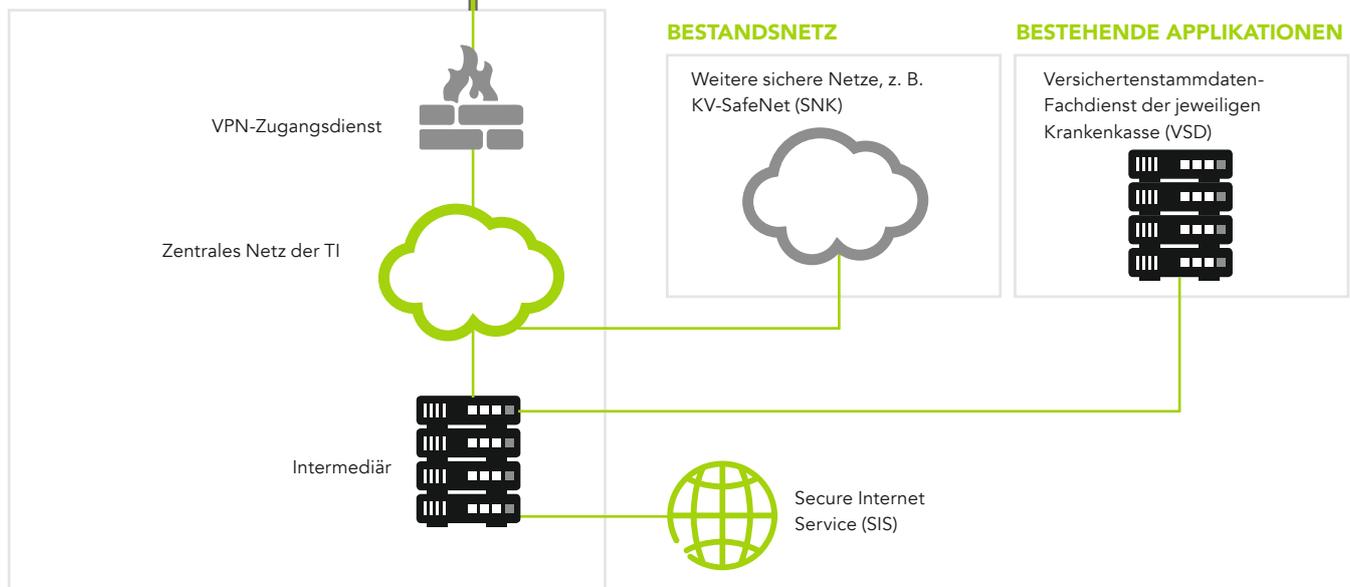
- **Verbesserung von Transparenz, Qualität und Wirtschaftlichkeit der Behandlung** von Patientinnen und Patienten durch ein elektronisch vernetztes Gesundheitssystem
- Eine individuelle, optimierte und **effiziente Versorgungssteuerung** einschließlich Notversorgung
- Deutliche **Verbesserung von Patientensouveränität** sowie Datenschutz und Datensicherheit im Gesundheitssystem
- Die **Vereinfachung des Informationsaustausches** zwischen allen Beteiligten und kürzere, schnellere und sicherere Kommunikationswege
- **Effizienz, Interoperabilität** und die Gewährleistung, dass die genaue Bedeutung der **ausgetauschten Informationen** auch für andere Systeme verständlich ist

VEREINFACHTE DARSTELLUNG DER TI-GRUNDSTRUKTUR

PRAXIS



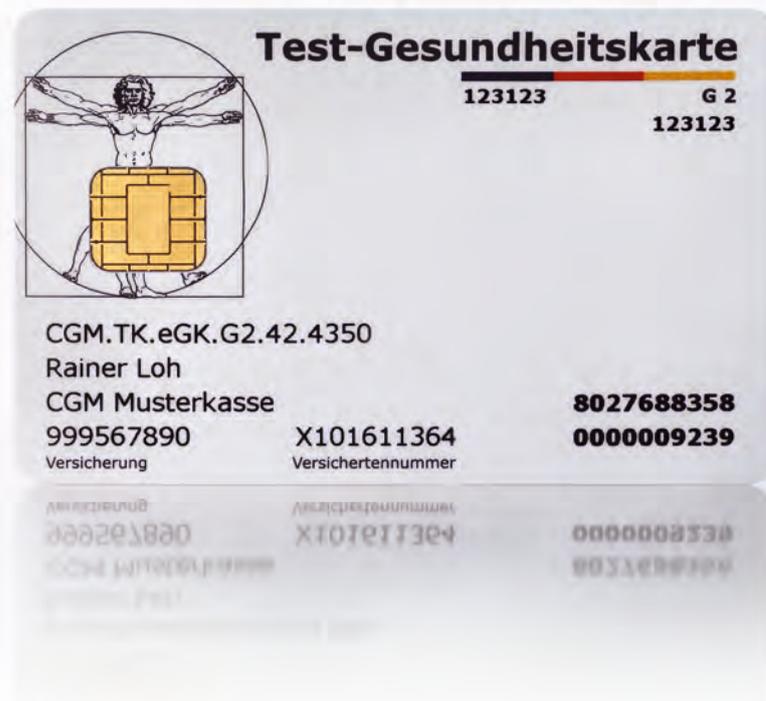
ZENTRALE TI-PLATTFORM



WAS MUSS FÜR DIE TI IN IHRER PRAXIS GEÄNDERT WERDEN?

- Aktualisierung des **Praxisverwaltungssystems**.
- Der zusätzliche **TI-Konnektor** verbindet das Netzwerk der Praxis sicher über die zentrale TI-Plattform mit den Servern der Krankenkassen.
- Die **eHealth-Kartenlesegeräte** werden nicht mehr direkt durch das Praxisverwaltungssystem gesteuert, sondern kommunizieren über das Praxisnetzwerk mit dem TI-Konnektor und stellen diesem die Sicherheitsmerkmale der verschiedenen **Karten (eGK, HBA, SMC-B)** zur Verfügung.

DIE ELEKTRONISCHE GESUNDHEITSKARTE (eGK)



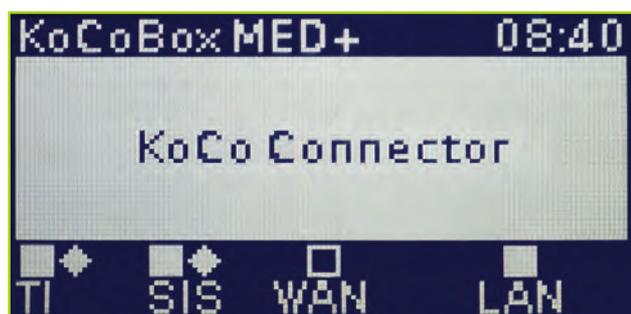
- Die **eGK** ist eine Mikroprozessorkarte und erlaubt die **Umsetzung vielfältiger Sicherheitsmechanismen**. Um künftig neue Anwendungsmöglichkeiten der eGK nutzen zu können, bedarf es der TI, die die Teilnehmer an der medizinischen Versorgung vernetzt.
- Zum **Schutz vor Missbrauch** wird die Gültigkeit der eGK bei jeder Nutzung überprüft.
- Auf der eGK sind die **Versichertenstammdaten** gespeichert, die von den Krankenkassen für die TI bereitgestellt und auch dort in den Bestandssystemen gepflegt werden. Außerdem wird der für die Abrechnung wichtige **Prüfungsnachweis auf der eGK** gespeichert.
- Geschützte Versichertendaten können **nur von berechtigten Personen** von der Gesundheitskarte ausgelesen werden. Dies wird technisch sichergestellt, da der Zugriff nur mittels einer Berechtigtenkarte (HBA oder SMC-B) möglich ist.
- **Es können sowohl G1plus- als auch G2-Karten** der eGK durch Versicherte vorgelegt werden.
- Es können **künftig weitere Anwendungsmöglichkeiten** wie das Notfalldatenmanagement, der elektronische Medikationsplan oder die elektronische Patientenakte mittels eGK realisiert werden. Die Nutzung wird freiwillig sein, Art und Umfang kann der Versicherte selbst festlegen.

Hinweis: Weitere wichtige Karten sind der Heilberufsausweis (HBA) des Arztes sowie die SMC-B (Security Module Card Typ B), über die die Praxis identifiziert wird. Zusätzlich sind im Konnektor und im eHealth-Kartenterminal die technischen Gerätekarten gSMC-K und gSMC-KT vorhanden.

KONNEKTOR ALS KERN DER DEZENTRALEN TI



Der Konnektor **koordiniert und verschlüsselt die Kommunikation** zwischen PVS, eGK, HBA/SMC-B und zentraler TI-Plattform. Er stellt damit das **Bindeglied** zwischen diesen Komponenten aufseiten des Leistungserbringers und der TI dar.



ANZEIGE DER VERBINDUNGEN:

- leeres Quadrat = keine Verbindung konfiguriert
- ausgefülltes Quadrat = Verbindung konfiguriert
- leere Raute = es besteht keine Verbindung zur TI/zum SIS
- volle Raute = sichere Verbindung zur TI/zum SIS

EINSATZ EINES MOBILEN KARTENTERMINALS (mobKT)



- Mobile Kartenterminals sind **speziell für den mobilen Einsatz** gedacht, zum Beispiel für Hausbesuche.
- Das mobile Kartenterminal wird im Gegensatz zum eHealth-Kartenterminal **direkt an den PVS-Rechner angeschlossen** und soll unter ständiger **persönlicher Kontrolle des LE** sein und bei Nichtnutzung zugriffsgeschützt verwahrt werden. Es **darf nicht** kontinuierlich mit dem PVS verbunden sein.
- Das Einlesen der Versichertendaten ist **nur mit freigeschalteter Berechtigungskarte** (SMC-B oder HBA) möglich. Dazu wird vor dem Einlesen zur Eingabe der Karten-PIN aufgefordert.
- Die Versichertenstammdaten werden im ersten Schritt ins mobKT eingelesen. Zum **Übertragen der Daten an das Primärsystem** im zweiten Schritt muss erneut die PIN dieser Karte eingegeben werden. Ein Einlesen von der eGK direkt ins PVS ist **nicht möglich**.
- Innerhalb eines vom Nutzer festgelegten Zeitraums (max. 60 Minuten) können dann weitere Karten ohne **erneute PIN-Eingabe** eingelesen werden.
- Die Daten können auch **nur mit derselben berechtigten Karte** wieder angezeigt, gedruckt oder ausgelesen werden, da sie verschlüsselt gespeichert werden.

Bildquelle: <https://ingenico.de>

VERSICHERTENSTAMMDATEN-MANAGEMENT (VSDM)

- Die **Versichertenstammdaten** (VSD) sind auf der elektronischen Gesundheitskarte gespeichert. Sie gliedern sich in die drei Bereiche PD (Persönliche Versichertendaten), VD (Allgemeine Versicherungsdaten) und GVD (Geschützte Versicherungsdaten wie z. B. „Zugehörigkeit zu besonderen Personengruppen“).
- Das VSDM ermöglicht neben dem Lesen der VSD eine **Online-Prüfung** und ggf. eine **Online-Aktualisierung** durch Abgleich mit den Daten der Krankenkasse. So kann bspw. eine **Adressänderung** direkt auf der eGK aktualisiert werden. Arztpraxen können dann über ihre Praxissoftware die aktuellen Daten von der eGK direkt einlesen.
- Das **Ergebnis der Online-Prüfung/-Aktualisierung** wird durch einen sogenannten **Prüfungsnachweis** auf der eGK gespeichert und an das Primärsystem übergeben (z. B. „Aktualisierung VSD auf eGK durchgeführt“ oder „Aktualisierung VSD auf eGK nicht notwendig“). Der **Zugriff auf geschützte Versichertendaten** wird protokolliert.
- Der **Umgang mit den weiteren möglichen Prüfungsergebnissen** (z. B. „Aktualisierung VSD auf eGK technisch nicht möglich“) wird im weiteren Verlauf ausführlich erläutert.

NUTZUNG DER BESTANDSNETZE

- **Anwendungen im Sicheren Netz der KVen** (SNK) sind weiter nutzbar. Die grundsätzliche Erreichbarkeit wird bei der Installation sichergestellt.
- Das **Sichere Netz der KVen** (SNK) soll die digitale Kommunikation zwischen Ärzten und anderen Leistungserbringern im Gesundheitswesen und den Kassenärztlichen Vereinigungen absichern und erleichtern.
- SNK ist ein abgeschottetes, **sicheres Kommunikationsnetz**, über das diverse Dienste wie beispielsweise die Online-Abrechnung angeboten werden.
- Wird bisher **KV-SafeNet als Zugangsweg** in das SNK genutzt, kann das KV-SafeNet-Endgerät durch den Konnektor ersetzt werden.

ÜBERSICHT DER STÖRUNGSFÄLLE

1. FEHLER BEIM LESEN DER VERSICHERTENSTAMMDATEN MIT ABRUCH DURCH UNGÜLTIGE eGK

ALS URSACHE KOMMEN FOLGENDE FEHLER INFRAGE:

- Gesundheitsanwendung gesperrt (Fehlercode 114)
- AUT-Zertifikat ungültig (Fehlercodes 106 und 107)
- Leseversuch von veralteter eGK (älter als G1plus) (Fehlercode 113)

Hinweis: Diese Meldungen sind keine technischen Fehler, sondern fachlich definierte Anwendungsfälle, um bspw. Missbrauch von gestohlenen Karten zu verhindern.

WAS IST ZU TUN?

- Wenn **eine der drei Fehlermeldungen** angezeigt wird, ist die vorliegende eGK **kein gültiger Leistungsanspruchsnachweis**.
- In diesem Fall **ist der Versicherte zu fragen**, ob er in der Zwischenzeit eine neuere eGK von der Kasse zugeschickt bekommen hat.
- Wenn der Versicherte **keine aktuellere eGK** besitzt, ist gemäß BMV-Ä Anlage 4a Anhang 1 Kap. 2.1. bzw. § 8 BMV-Z und § 12 EKVZ vorzugehen. Der Versicherte soll mit Verweis auf die Fehlermeldung (z. B. Versicherungsbeginn in der Zukunft) **an seine Krankenkasse** verwiesen werden.

2. FEHLER BEIM LESEN DER VERSICHERTENSTAMMDATEN MIT ABRUCH AUFGRUND VON TECHNISCHEN FEHLERN

WAS IST ZU TUN?

- Bei einem **Abbruch beim Lesen der VSD** aufgrund von technischen Fehlern ist es wichtig, den **spezifischen, vom System angezeigten Fehlercode** zur Fehlermeldung an den Support (User Help Desk (UHD)) zu übermitteln.
- Technische Fehler können dabei **nicht nur durch die eGK**, sondern auch durch andere Komponenten verursacht werden (z. B. Gerätefehler oder Softwarefehler).
- Bei den Fehlercodes **3041** und **3042** (HBA/SMC-B nicht freigeschaltet) ist eine erneute PIN-Eingabe erforderlich (3041: HBA, 3042: SMC-B).
- Bei den Fehlercodes **3039** und **3040** (Prüfungsnachweis nicht entschlüsselbar) ist eine Online-Prüfung der eGK erforderlich.
- Wenn die VSD auf der eGK inkonsistent sind (**Fehlercode 3001**), sollte erneut versucht werden, die Karte zu aktualisieren. Falls dann die Karte immer noch den Fehler aufweist, ist der Versicherte an seine Kasse zu verweisen.
- **In allen anderen Fällen** ist ein Fehlerticket im Support (UHD) mit der entsprechenden Fehlernummer einzustellen.
- Wenn die vorgelegte Gesundheitskarte aufgrund von technischen Fehlern nicht verwendet werden kann, findet das **Ersatzverfahren gemäß Bundesmantelvertrag** Anwendung.

3. VERSICHERTENSTAMMDATEN LESEN MIT WARNUNG IM PRÜFUNGSNACHWEIS

FOLGENDE WARNUNGEN KÖNNEN BEIM LESEN DER VSD AUFTRETEN:

- Aktualisierung VSD auf eGK technisch nicht möglich (Prüfungsnachweis 3)
- Online-Prüfung des Authentifizierungszertifikats technisch nicht möglich (Prüfungsnachweis 5)
- Aktualisierung VSD auf eGK technisch nicht möglich und maximaler Offline-Zeitraum überschritten (Prüfungsnachweis 6)

WAS IST ZU TUN?

- In diesen Fällen gilt die Karte als gültiger **Leistungsanspruchsnachweis**. Bei einem weiteren Besuch im Quartal muss jedoch eine erneute Online-Prüfung durchgeführt werden.
- Falls der entsprechende Fehler öfter auftritt, ist ein **Fehlerticket** mit dem detaillierten Fehlercode im Support einzustellen.

FOLGENDE WARNUNG ERFORDERT EINE ANDERE AKTIVITÄT:

- Authentifizierungszertifikat eGK ungültig (Prüfungsnachweis 4)

- Die vorliegende eGK ist **kein gültiger Leistungsanspruchsnachweis**.
- **In diesem Fall** ist der Versicherte zu fragen, ob er in der Zwischenzeit eine neuere eGK von der Kasse zugeschickt bekommen hat.
- Wenn der Versicherte **keine aktuellere eGK** besitzt, ist gemäß BMV-Ä Anlage 4a Anhang 1 Kap. 2.1. bzw. § 8 BMV-Z und § 12 EKVZ vorzugehen. Der Versicherte soll mit Verweis auf die Fehlermeldung (z. B. Versicherungsbeginn in der Zukunft) **an seine Krankenkasse** verwiesen werden.

4. UNGÜLTIGER LEISTUNGSANSPRUCHSNACHWEIS AUFGRUND FACHLICHER PRÜFUNG IM PRIMÄRSYSTEM

WAS IST ZU TUN?

- Falls nach dem erfolgreichen Einlesen der VSD im Primärsystem bei der fachlichen Prüfung festgestellt wird, dass die Karte **kein gültiger Leistungsanspruchsnachweis** ist (Versicherungsbeginn in der Zukunft oder Versicherungsende in der Vergangenheit), ist gemäß **BMV-Ä** Anlage 4a Anhang 1 Kap. 2.1. bzw. **§ 8 BMV-Z** und **§ 12 EKVZ** vorzugehen.

ÜBERSICHT DER STÖRUNGSFÄLLE

WEITERE HINWEISE ZUM UMGANG MIT STÖRUNGEN BEI DER TI-NUTZUNG

- Vergewissern Sie sich bitte immer zunächst bei allen allgemeinen Störungen der TI-Nutzung, dass **alle Kabel** (Stromanschluss, Netzwerk) an die Geräte (insbesondere den TI-Konnektor) angeschlossen und diese eingeschaltet sind.
- Danach prüfen Sie bitte, ob zur aufgetretenen Störung eine Hilfestellung in der **Hilfefunktion des Primärsystems** enthalten ist und ob diese die Störung beseitigt.
- Sollte sich die Störung mit Hilfe der FAQ nicht beheben lassen, kontaktieren Sie bitte Ihren **Service-Partner** oder den **OPB User Help Desk**.

Stempel Service-Partner:

OPB User Help Desk: 0800 5515512

ALLGEMEINE SICHERHEITSHINWEISE ZUM KONNEKTOR

- Wurde bei Lieferung eines TI-Konnektors das Verpackungssiegel äußerlich beschädigt, informieren Sie bitte Ihren Service-Partner.
- Stellen Sie bitte in Abstimmung mit Ihrem Service-Partner sicher, dass der Konnektor nur in einer zugriffsgeschützten Umgebung eingesetzt wird (nicht am Empfangsschalter!) und überprüfen Sie ihn bei der Nutzung hin und wieder auf Gehäusebeschädigungen. Öffnen Sie **niemals** das Gehäuse des Konnektors.

Wichtig: Ihr Konnektor, die KoCoBox MED+, darf **nur mit unverletzten Sicherheitsiegeln** in Betrieb genommen und genutzt werden.



Sicherheitsiegel
im Originalzustand



Ansicht nach
Manipulation

ALLGEMEINE SICHERHEITSHINWEISE ZU KARTENTERMINALS

- Das Kartenterminal **muss hinreichend vor Manipulation geschützt werden**. Betreiben Sie das Gerät so, dass ein Missbrauch auszuschließen ist. Das Gerät unterstützt Sie dabei, indem es (nicht erkennbare) physische Manipulationen für einen Zeitraum von **30 Minuten** verhindert.
 - **Überprüfen Sie regelmäßig** vor der Nutzung und nach Abwesenheit die Unversehrtheit des Geräts (Prüfen der Sicherheitsmerkmale, insbesondere der Siegel).
 - **PINs müssen stets unbeobachtet** eingegeben werden. Die Eingabe einer PIN darf nur dann erfolgen, wenn das Gerät den sicheren Eingabemodus anzeigt und eine PIN-Eingabe erwartet wird. Die PIN wird dann sicher an die Karte übertragen. Eine Übertragung der PIN an ein anderes Gerät findet so unter keinen Umständen statt.
 - **Angaben zur Version** finden Sie für die Hardware auf dem Typenschild (häufig an der Unterseite des Geräts) sowie für die Firmware über die Menüsteuerung des Geräts (siehe Handbuch des Geräts).
- Ein Kartenterminal ist an mehreren Stellen mit einem **Gehäusesiegel** versiegelt, um es vor unerlaubtem Öffnen zu schützen.

Unbeschädigtes Gehäusesiegel Beschädigtes Gehäusesiegel Fehlendes Gehäusesiegel
 - eHealth-Kartenterminals haben zudem ein **Slotsiegel**, mit dem der Slot für die Gerätekarte nach dem Einschub der gSMC-KT versiegelt wird.

Unbeschädigtes Slotsiegel Beschädigtes Slotsiegel Fehlendes Slotsiegel
 - Berühren Sie beim Umgang mit dem Gerät möglichst **nicht die Siegel** bzw. behandeln Sie diese mit Vorsicht, um sie nicht zu beschädigen.
 - Um Manipulationen am Gerät zu erkennen, **prüfen Sie regelmäßig die Siegel** auf Unversehrtheit und Echtheit.

Hinweis: Details und weitere Abbildungen finden Sie in Ihrem Produkthandbuch.

SCHULUNGS- UNTERLAGEN



Dentalinformationssystem

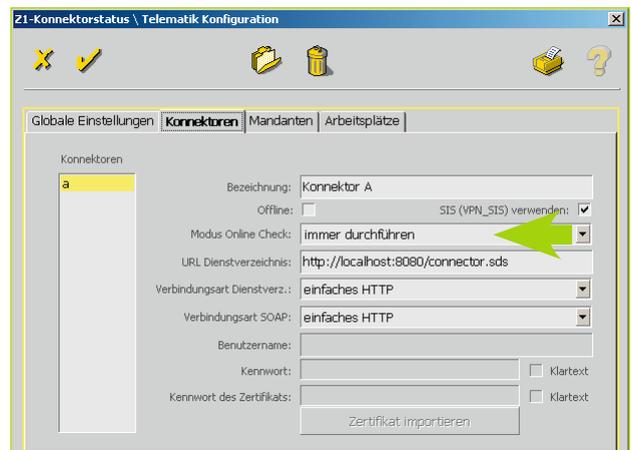
Telematik-Konfiguration	14	Unterschiedliche Szenarien zu den Einlesevorgängen	21
Online-Prüfung der eGK	14	Modus Online Check = immer durchführen	21
Karte (SMC-B/HBA) freischalten/ändern mit Transport-PIN	15	Modus Online Check = beim ersten Besuch im Quartal	23
SMC-B/HBA freischalten/ändern (PIN/PUK)	16	Mit einem technischen Problem	23
Anwendung	18	Vom mobKT in das Primärsystem	26
Die Z1-Konnektorstatus-Anzeige	18	Änderung der Versichertendaten – Abgleich nach Online-Prüfung	28
Erläuterung zur Z1-Konnektorstatus-Anzeige/ Symbole	19	Hinweis zum Einlesevorgang KVK/VSD aus mobKT	29
Das Ampelsystem	19	Support-Informationen	30
Anzeige/Status des aktivierten HBA oder der aktivierten SMC-B	20	Abbruch beim Einlesen aufgrund von technischen Fehlern	31
Anzeige/Status bei gesteckter eGK des Patienten	20	Service & Kontaktdaten	32
Einlesevorgang der eGK (manuell)	20	Symbole	32
		Glossar	34

TELEMATIK-KONFIGURATION

Die Aktivierung und Konfiguration des Konnektors nimmt Ihr Vertriebs- und Servicepartner vor. Neben den allgemeinen Konnektor-Einstellungen können Sie festlegen, wie häufig eine Online-Prüfung der eGK erfolgen soll.

ONLINE-PRÜFUNG DER eGK

Über die Registerkarte **Konnektoren** können Sie festlegen, wie häufig eine Online-Prüfung der eGK erfolgen soll. Sie wählen die entsprechenden Einstellungen über die Liste **Modus Online Check** aus.



Folgende Möglichkeiten stehen zur Verfügung:

Immer durchführen:	Die Online-Prüfung wird immer gestartet.
Beim ersten Besuch im Quartal:	Sofern ein Prüfungsnachweis im aktuellen Quartal in den Versichertenstammdaten gespeichert ist, findet keine automatische Online-Prüfung statt.
Niemals:	Wenn das System offline eingestellt ist.
Auf Anforderung des Benutzers:	Sie erhalten eine Abfrage, ob eine Online-Prüfung durchgeführt werden soll.

Weitere Informationen zur Online-Prüfung finden Sie unter „Unterschiedliche Szenarien zu den Einlesevorgängen“.

KARTE (SMC-B/HBA) FREISCHALTEN/ÄNDERN MIT TRANSPORT-PIN

Das Nutzen einer SMC-B/eines HBA erfordert einen erhöhten Sicherheitszustand. Daher muss die PIN der Karte im Rahmen einer Inbetriebnahme geändert werden. Per rechter Maustaste in der Zeile des zugeordneten Mandanten wird der Vorgang gestartet:

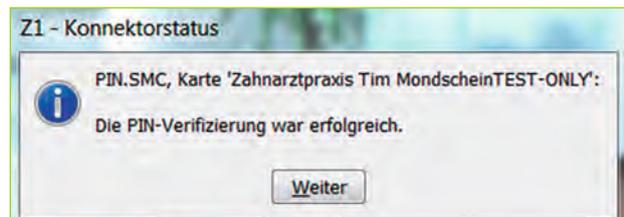
Kartenterminal	Slot	Kartentyp	ICCSN	Inhaber
GT900	1	EGK	80276881235543405101	Doris RU-Ochtum
GT900	2	SMC-B	80276883580000000018	Zahnarztpraxis Tim Mond
GT900				PIN SMC-B mitälsieren
GT900	4	SMC-KT	80276883580000006499	80276883580000006499
Mobiles Lesegerät				

Telematik-Mandant: 01 - Mandant 1
 PIN SMC-B: Transport-PIN
 Karte gesteckt: 12.06.2015 13:17:22
 Zertifikat gültig bis: 16.10.2019

Die Eingabe der PIN erfolgt über das Kartenterminal:



Die SMC-B bzw. der HBA ist nun freigeschaltet:



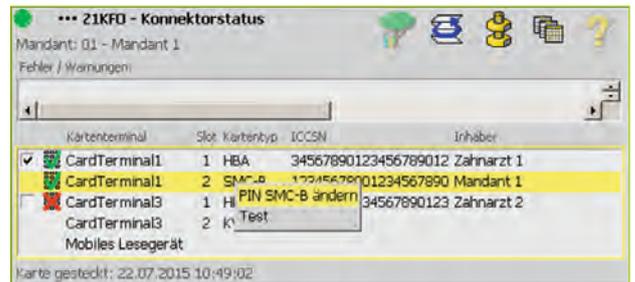
Die Karte erhält ein grünes Häkchen und im unteren Teil (Z1-Konnektorstatus-Anzeige) wird textuell angezeigt, dass die Karte verifiziert ist.

Kartenterminal	Slot	Kartentyp	ICCSN	Inhaber
GT900	1	EGK	80276881235543405701	Johann RU-Ehlers
GT900	2	SMC-B	80276883580000000019	Zahnarztpraxis Hilda
GT900	3	SMC-KT	80276883580000008436	80276883580000008436
GT900	4			
zf	1	EGK	80276881235543405101	Doris RU-Ochtum
zf	2			
zf	3	UNKNOWN		
zf	4			
CARD STAR/medic:	1			
CARD STAR/medic:	2			

Telematik-Mandant: 01 - Mandant 1
 PIN SMC-B: verifiziert
 Karte gesteckt: 24.07.2015 11:53:04
 Zertifikat gültig bis: 16.10.2019

SMC-B/HBA FREISCHALTEN/ÄNDERN (PIN/PUK)

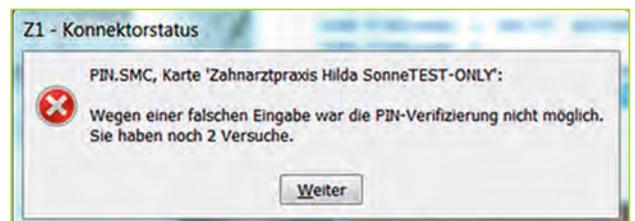
Ändern einer PIN der SMC-B am CardTerminal 1 für Mandant 1 auf Anforderung: In der Konnektorstatus-Anzeige kann per rechter Maustaste in der Zeile des Mandanten eine Änderung der PIN vorgenommen werden.



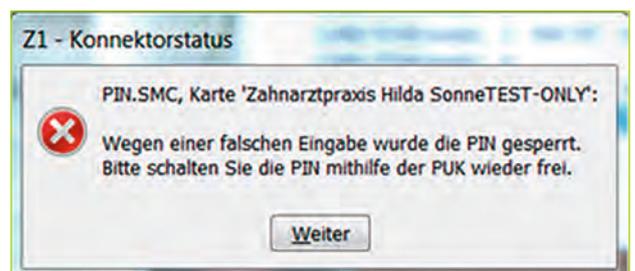
Im Anschluss erfolgt die Aufforderung im Kartenterminal-Display, die PIN am entsprechenden Gerät (im Beispiel CardTerminal1) einzugeben:



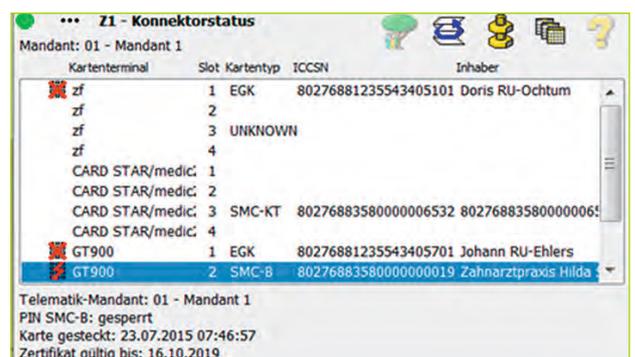
Bei einer falschen Eingabe der PIN erscheint in CGM Z1 folgender Hinweis:



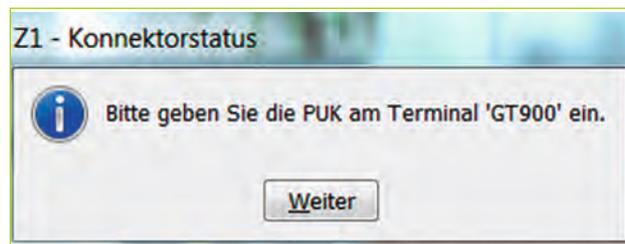
Waren die letzten beiden Versuche ebenfalls nicht korrekt, wird die PIN-Eingabe gesperrt:



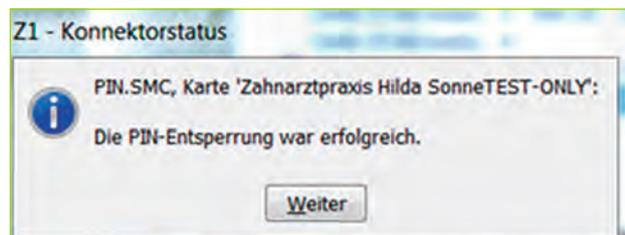
Das Einlesen von elektronischen Gesundheitskarten für diesen zugeordneten Mandanten ist zu diesem Zeitpunkt nicht möglich, da die SMC-B gesperrt ist.



Zum Entsperren der Karte muss die PUK-Eingabe erfolgen:



Nach Eingabe der PUK erfolgt der Hinweis:



Nach Eingabe der neuen PIN wird die Änderung für diesen Mandanten bestätigt:



ANWENDUNG

Mit dem Start von CGM Z1 werden immer alle benötigten Systeme, Einstellungen und angeschlossene Geräte geprüft. Dazu zählen:

- der Konnektor
- die Verbindung zur Telematikinfrastruktur
- die zugeordneten Kartenterminals, Arbeitsplätze, Karten zum Mandanten, Freischaltungen und Gültigkeit der Karten
- VPN TI / VPN SIS

Sofern alle Komponenten ohne Fehler oder Störung identifiziert wurden, erscheint folgender Hinweis:



DIE Z1-KONNEKTORSTATUS-ANZEIGE

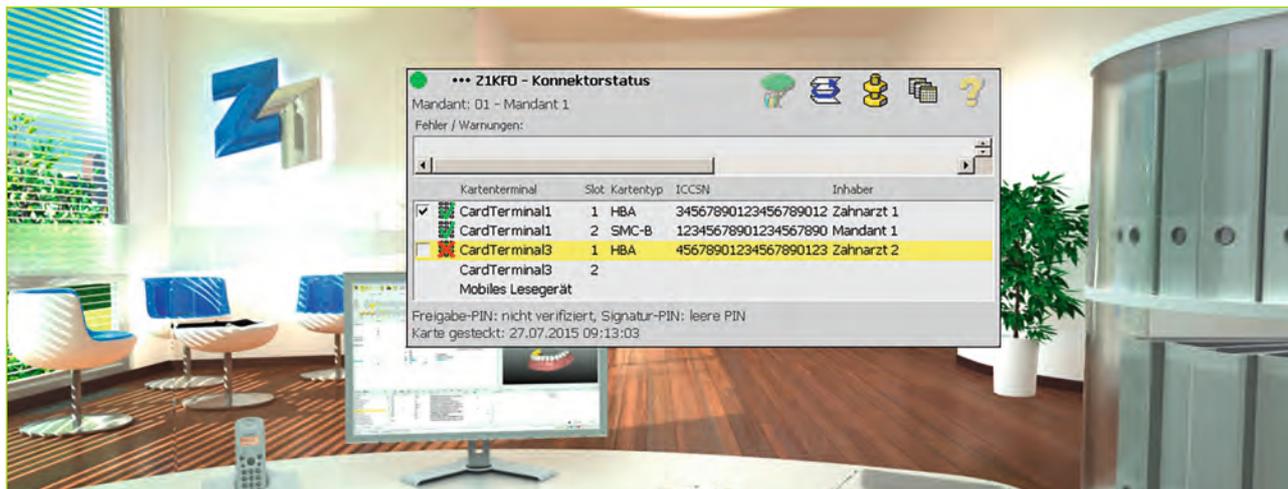
Nach erfolgreicher Konfiguration der Hard- und Software für die Telematikinfrastruktur wird an allen zugeordneten Arbeitsplätzen die Z1-Konnektorstatus-Anzeige auf dem Bildschirm angezeigt.

Im Ruhezustand verkleinert sich die Z1-Konnektorstatus-Anzeige automatisch, sodass nur noch ein Rechteck zu sehen ist und insbesondere das Ampelsystem beobachtet werden kann. Weitere Informationen hierzu finden Sie unter „Das Ampelsystem“.

Sobald die Maustaste zur Anzeige geführt wird, klappt die Z1-Konnektorstatus-Anzeige wieder auf, sodass alle Informationen (z. B. welche SMC-B an welchem CardTerminal verifiziert ist, ob und wo eine Karte steckt etc.) wieder sichtbar sind.

Tipp: Die Z1-Konnektorstatus-Anzeige kann per gedrückter linker Maustaste an eine beliebige Stelle des oberen Rands gezogen werden.

Die Verbindung zur Telematikinfrastruktur unterliegt einer ständigen Überprüfung, sodass ein Umschalten der Ampel auf Rot (z. B. weil die Verbindung zur Infrastruktur unterbrochen ist) sofort sichtbar ist und die notwendigen Maßnahmen getroffen werden können.



ERLÄUTERUNG ZUR Z1-KONNEKTORSTATUS-ANZEIGE/SYMBOLS

Kartenterminal	Slot	Kartentyp	ICCSN	Inhaber
<input checked="" type="checkbox"/>  CardTerminal1	1	HBA	34567890123456789012	Zahnarzt 1
<input checked="" type="checkbox"/>  CardTerminal1	2	SMC-B	12345678901234567890	Mandant 1
<input type="checkbox"/>  CardTerminal3	1	HBA	45678901234567890123	Zahnarzt 2
<input type="checkbox"/>  CardTerminal3	2	EGK	44444444444444444444	Königsstein
Mobiles Lesegerät				
Versichertenr.: K220635158				

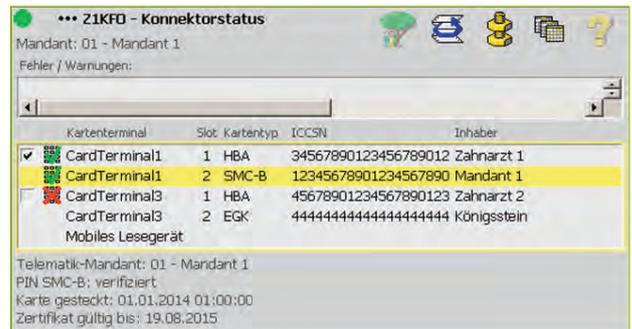
DAS AMPELSYSTEM

Die Ampelsystem zeigt die Betriebsbereitschaft bzw. Störungen des Konnektors oder anderer Komponenten an. Gleichzeitig werden diese durch Hinweise in der Z1-Konnektorstatus-Anzeige dargestellt.

	Alle Komponenten laufen fehlerfrei.
	Eingeschränkte Betriebsbereitschaft. Karten sind noch einlesbar (z. B. weil nur eines von zwei Kartenterminals defekt ist).
	Ausfall! Karten sind nicht über die Telematikinfrastruktur einlesbar (es ist kein aktueller Prüfungsnachweis oder Abgleich der Versichertenstammdaten via Internet möglich).

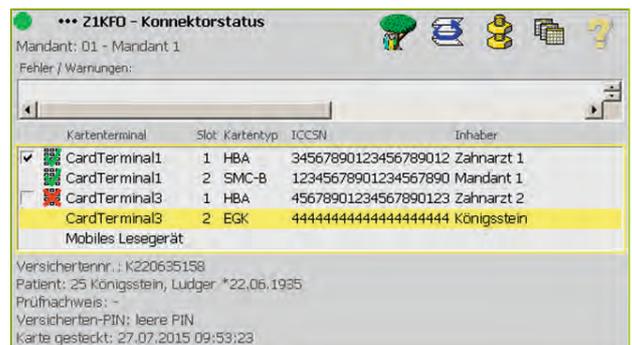
ANZEIGE/STATUS DES AKTIVIERTEN HBA ODER DER AKTIVIERTEN SMC-B

Das grüne Häkchen weist bereits auf die freigeschaltete Karte hin. Im unteren Teil können weitere Informationen über die Karte eingeholt werden.



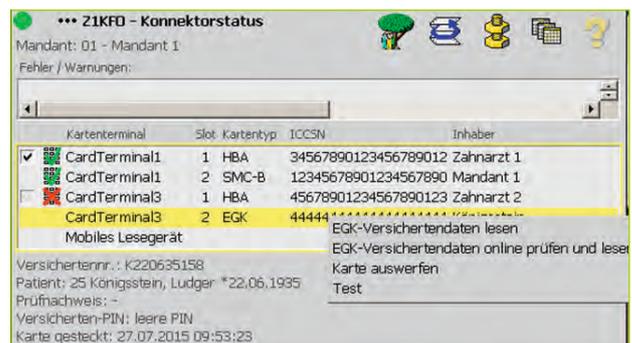
ANZEIGE/STATUS BEI GESTECKTER eGK DES PATIENTEN

Bei gesteckter eGK werden im unteren Teil folgende Daten angezeigt: Versichertennummer, Patientnummer, Name, Vorname, Geburtsdatum und Prüfungsnachweisstatus des Versicherten (in diesem Beispiel ist noch kein Prüfungsnachweis erfolgt), Datum und Zeitpunkt vom Stecken der eGK.

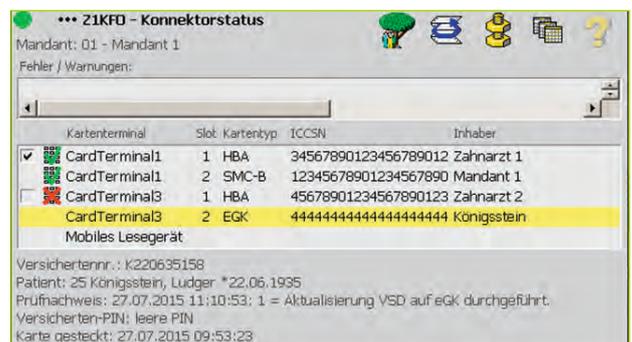


EINLESEVORGANG DER eGK (MANUELL)

Das Einlesen der eGK erfolgt in gewohnter Weise. Sobald die Karte gesteckt wird, startet der Einlesevorgang, insofern das Primärsystem entsprechend konfiguriert wurde. Es besteht aber auch die Möglichkeit, den Einlesevorgang manuell zu starten. Per rechtem Mausklick können nur die Versichertendaten und die Online-Prüfung gestartet werden.



Im unteren Teil können bei noch gesteckter Karte Informationen zum Versicherten und dem Prüfungsnachweis eingeholt werden.



UNTERSCHIEDLICHE SZENARIEN ZU DEN EINLESEVORGÄNGEN

Über den Bereich Modus Online Check kann im Z1-Konnektorstatus über Konnektoren ausgewählt werden, wie oft die Online-Prüfung der eGK durchgeführt werden soll. Weitere Informationen hierzu finden Sie unter „Online-Prüfung der eGK“.



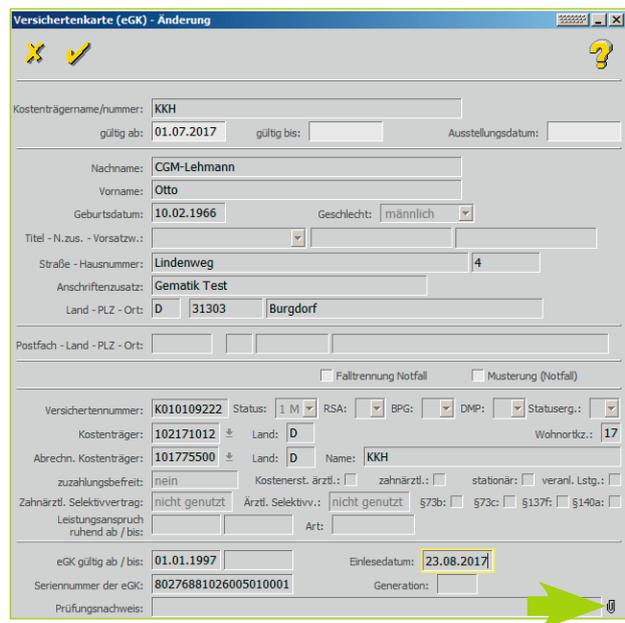
MODUS ONLINE CHECK = IMMER DURCHFÜHREN

Einstellung im Konnektor im Bereich **Modus Online Check**:

Beispiel: Der Patient hat noch keinen Prüfungsnachweis im aktuellen Quartal.



Mit Mausklick auf die Büroklammer in der Zeile Prüfungsnachweis können die vorhandenen **Prüfungsnachweise** eingesehen werden:



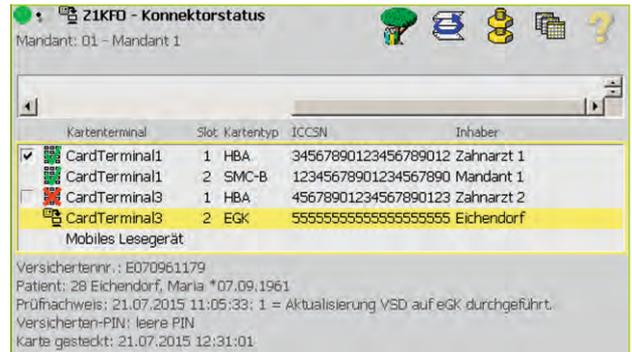
Das Versichertensymbol zeigt dennoch die eGK als gelesen an.



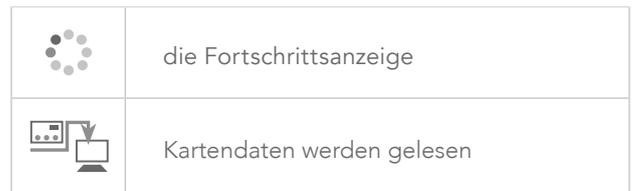
In der Konnektorstatus-Anzeige steht ein „-“ in der Zeile **Prüfnachweis**.



Der Einlesevorgang beginnt mit Stecken der Karte, die Online-Prüfung startet automatisch:

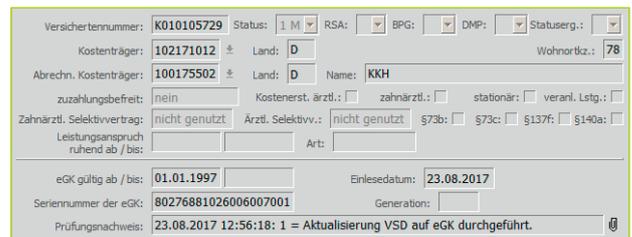


Während des Einlesevorgangs und der Online-Prüfung erscheinen neben der grünen Ampel zwei Symbole:



Bei noch gesteckter Karte steht im unteren Teil der Z1-Konnektorstatus-Anzeige, wann der Prüfungsnachweis stattgefunden hat.

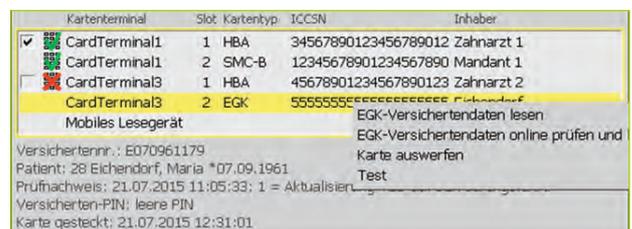
Im Primärsystem werden in **Stammdaten > Versichertenkarte (eGK)-Änderung** alle Daten zu diesem Versicherten eingetragen. Der Prüfungsnachweis wird im Feld Prüfungsnachweis mit Datum, Uhrzeit und Aktualisierung (1 oder 2 = positiv) eingetragen.



Hinweis: In diesem Feld steht immer der zuerst gültige Prüfungsnachweis des aktuellen Quartals. Falls kein gültiger Prüfungsnachweis vorhanden ist, wird der letzte ungültige Prüfungsnachweis angezeigt. Das Versichertensymbol wird jetzt zusätzlich mit einem grünen Häkchen versehen.

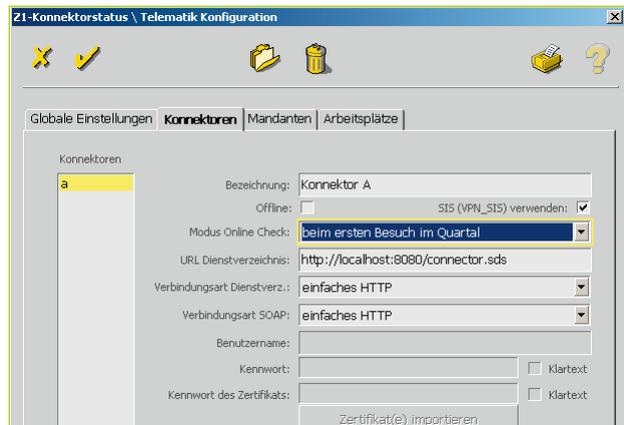
Der Einlesevorgang ist beendet.

Die Karte kann im Anschluss mit rechter Maustaste und Bestätigung der Option **Karte auswerfen** oder durch Herausziehen der Karte dem Terminal entnommen werden.

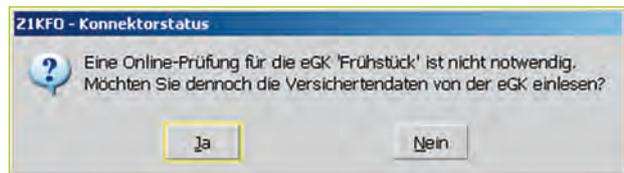


MODUS ONLINE CHECK = BEIM ERSTEN BESUCH IM QUARTAL

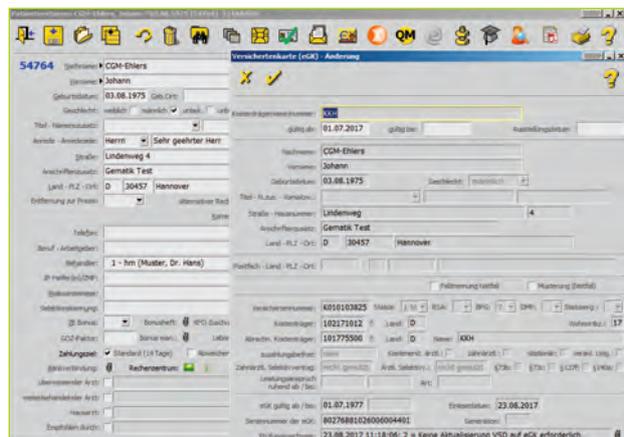
Beispiel: Patient hat bereits einen Prüfungsnachweis im aktuellen Quartal.



Nachdem das Primärsystem die Versichertendaten überprüft und festgestellt hat, dass ein aktueller Prüfungsnachweis schon vorhanden ist, erscheint folgender Hinweis:

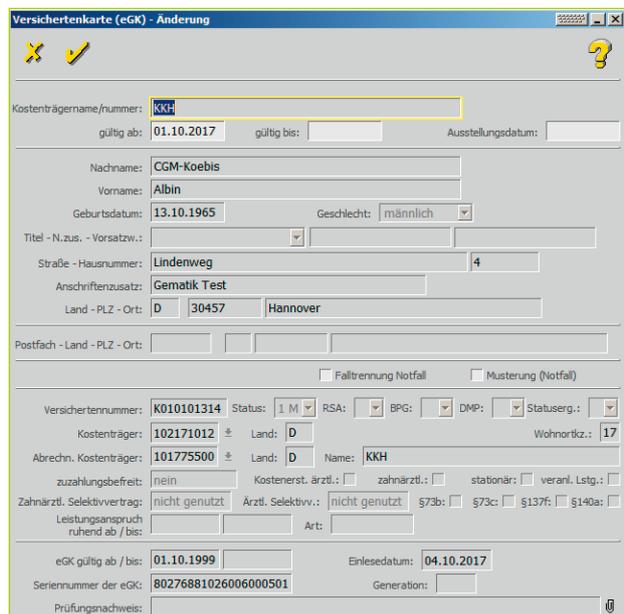


Nach Bestätigung mit **Ja** werden ausschließlich die Versichertendaten des Patienten und das Einlesedatum in den Versicherungsdaten im Primärsystem aktualisiert.



MIT EINEM TECHNISCHEN PROBLEM

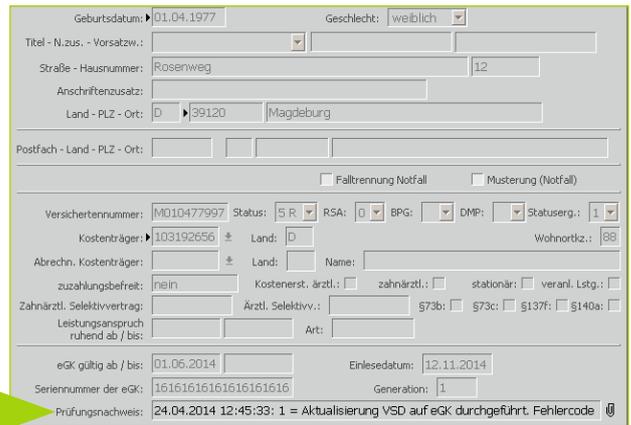
Beispiel: Der Patient hat keinen aktuellen Prüfungsnachweis. Eine Online-Prüfung soll durchgeführt werden.



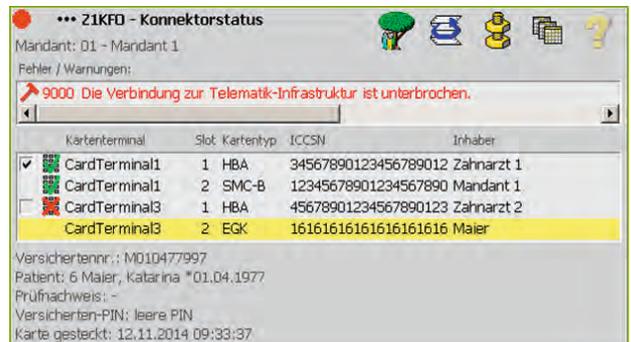
In der Konnektorstatus-Anzeige schaltet die Ampel auf Rot und ein Hinweis erscheint.



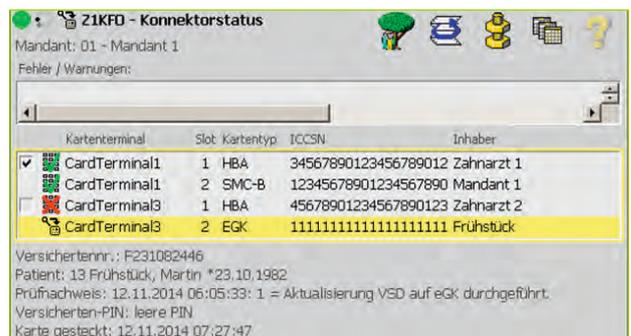
In einem solchen Fall werden trotzdem die Versicherungsdaten und das Einlesedatum in den Versicherungsdaten im Primärsystem aktualisiert. Im Feld **Prüfnachweis** bleibt der zuletzt gültige Prüfnachweis bestehen:



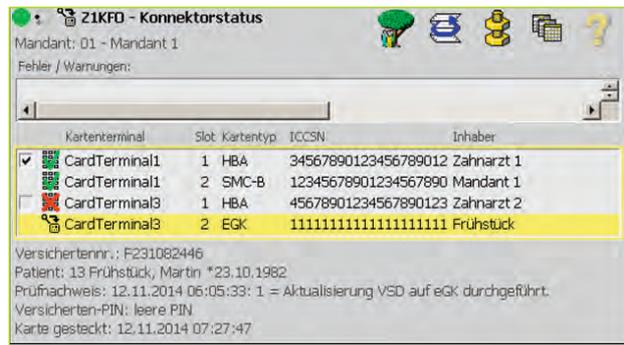
Die Konnektorstatus-Anzeige zeigt bei Prüfnachweis ein „-“ an.



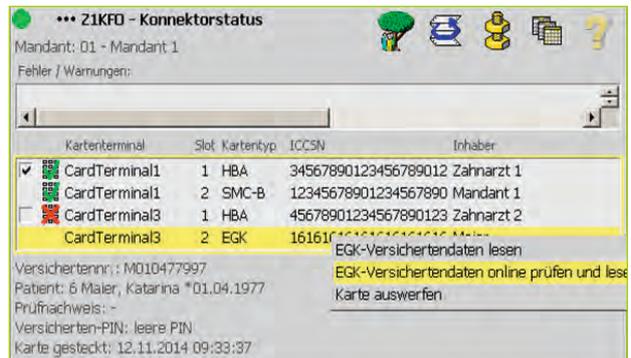
Konnte die Störung schnell behoben werden, weil z. B. nur ein Kabel lose war, ...



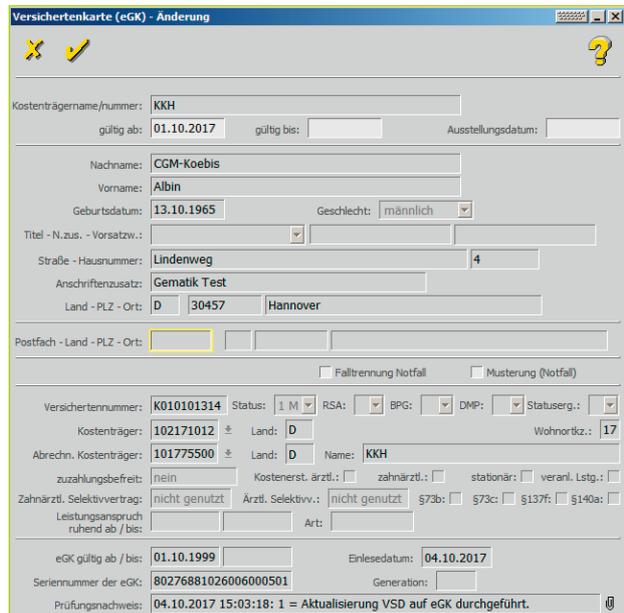
... wechselt die Ampel in der Konnektorstatus-Anzeige wieder auf Grün ...



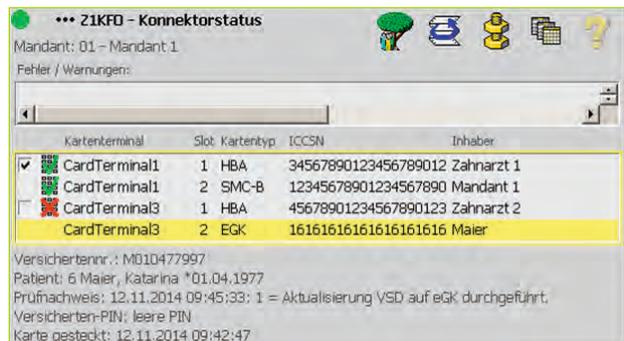
... und die Online-Prüfung kann bei noch gesteckter Karte manuell über die rechte Maustaste angestoßen werden, damit der Prüfungsnachweis aktualisiert werden kann.



Nach Behebung des technischen Problems und manuellem Anstoßen der Online-Prüfung ist der aktuelle Prüfungsnachweis im Feld Prüfungsnachweis mit Datum und Uhrzeit gespeichert ...



... und auch in der Konnektorstatus-Anzeige aktualisiert und sichtbar.



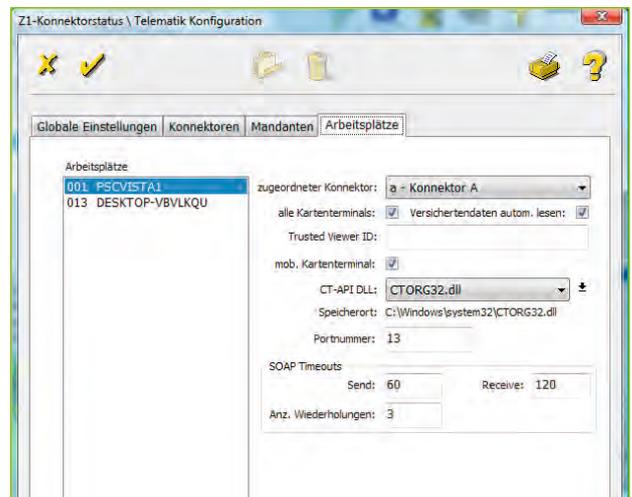
VOM MOBKT IN DAS PRIMÄRSYSTEM

Beispiel: Datensatz vom mobilen Kartenterminal (mobKT) in das Primärsystem übertragen. Das mobile Kartenterminal ist ein offline arbeitendes Kartenterminal für den mobilen Einsatz (Hausbesuch), das zur Datenübernahme direkt an das PS angeschlossen wird.

Es bildet somit die Ausnahme gegenüber allen anderen KT, die über den Konnektor verwaltet und über dessen Schnittstellen angesprochen werden.

Nachdem das mobile Kartenlesegerät mit dem Primärsystem über die CT-API-Schnittstelle verbunden ist, kann dieses in der Z1-Konnektor-Konfiguration konfiguriert werden:

- Aktivieren des mobilen Kartenterminals im Z1-Konnektorstatus/Telematik-Konfiguration
- Angabe der CT-API DLL
- Portnummer (Gerätemanager im PS)



Im Z1-Konnektorstatus wird das mobile Kartenterminal angezeigt:

Mittels rechter Maustaste kann der Datensatz vom mobilen Kartenleser angefordert, gelesen und in CGM Z1 gespeichert werden.



Da das mobile Kartenterminal nie eine Verbindung zur TI hat, können Versichertendaten auch dann eingelesen werden, wenn die Konnektor-Statusanzeige (Ampel) rot ist.

Hinweis: Die Schnittstelle zum mobilen Kartenterminal stellt für die eGK-Daten eine Leseoperation mit 4 Ausprägungen zur Verfügung, mit denen die PD, VD, GVD sowie Statusinformationen übernommen werden können.



Beispiel: eingelesene VSD im Kartenarchiv des mobKT.

Nachname, Vorname

Neuer, Tamara

Geburtsdatum, Geschlecht

25.09.1985, W

Wohnsitzländercode, Postleitzahl, Ort

D 56070 Koblenz

Straße, Hausnummer

Hauptstr. 23

Versicherten-ID

X808807073

Beginn

27.09.2014

Ende

26.09.2019

Kassenträger-Kennung

999567890

Kostenträger – Ländercode

D

Zuzahlungsstatus

0: von Zahlungspflicht nicht befreit

Kostenträgername

CGM Musterkasse

Abrechnender Kostenträger – Kennung

997834560

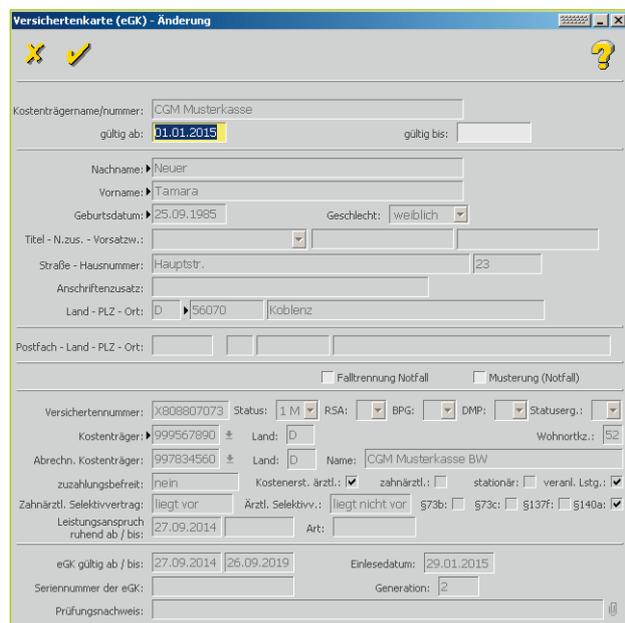
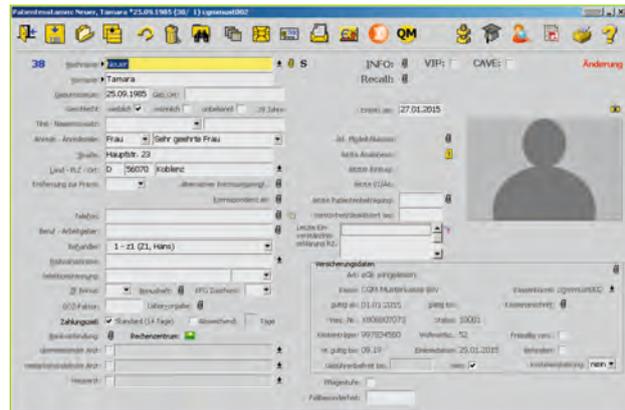
Abrechnender Kostenträger – Name

CGM Musterkasse BW

Art des Versicherten

1: Mitglied

Ein Prüfungsnachweis kann mit einem mobilen Kartenleser NIE erzeugt werden, somit wird das Feld **Prüfungsnachweis** in CGM Z1 nicht ausgefüllt.



HINWEIS ZUM EINLESEVORGANG KVK/VSD AUS MOBKT

Es gibt zwei Einlesevorgänge, die von der Funktion der Online-Prüfung (unabhängig von den Konfigurationen) ausgeschlossen sind. Das Primärsystem erkennt diese automatisch:

- eine KVK von sonstigen Kostenträgern (z. B. Bundespolizei), die auch nach dem 01.01.2015 ihre Gültigkeit hat
- das Einlesen der VSD vom mobilen Kartenleser in das PS

Dabei werden ausschließlich die Versicherungsdaten eingelesen.

SUPPORT-INFORMATIONEN

Beim Lesen der Versichertenstammdaten können verschiedene Störungsfälle auftreten, die zu einem Abbruch des Kartenlesevorgangs führen, z. B. durch eine ungültige eGK (Anzeige der Fehlercodes 114, 106, 107).

Wenn diese Fehlermeldungen angezeigt werden, ist die vorliegende eGK kein gültiger Leistungsanspruchsnachweis. Bitte fragen Sie den Patienten, ob er möglicherweise von seiner Krankenkasse eine neuere eGK erhalten hat. Ist dies nicht der Fall, bitten Sie den Patienten, Kontakt zu seiner Krankenkasse aufzunehmen.

Im Folgenden erhalten Sie einen Überblick über die Fehlermeldungen, die das Primärsystem anzeigen kann:

FEHLERCODE 114: Gesundheitsanwendung auf eGK gesperrt	<p>Zeigt das Primärsystem diese Fehlermeldung an, ist die vorliegende eGK kein gültiger Leistungsanspruchsnachweis.</p> <p>In diesem Fall ist der Versicherte zu fragen, ob er in der Zwischenzeit eine neuere eGK von der Kasse zugeschickt bekommen hat. Wenn der Versicherte keine aktuellere eGK besitzt, muss er an seine Krankenkasse verwiesen werden.</p> <p>Hinweis: Für Fehlercode 113 (Leseversuch von veralteter eGK) gilt die gleiche Handlungsempfehlung.</p>
FEHLERCODE 106: Zertifikat auf eGK gesperrt	<p>Zeigt das Primärsystem diese Fehlermeldung an, ist die vorliegende eGK kein gültiger Leistungsanspruchsnachweis.</p> <p>In diesem Fall ist der Versicherte zu fragen, ob er in der Zwischenzeit eine neuere eGK von der Kasse zugeschickt bekommen hat. Nur wenn der Versicherte keine aktuellere eGK besitzt, muss er an seine Krankenkasse verwiesen werden.</p>
FEHLERCODE 107: Zertifikat auf eGK ungültig	<p>Zeigt das Primärsystem diese Fehlermeldung an, ist die vorliegende eGK kein gültiger Leistungsanspruchsnachweis.</p> <p>In diesem Fall ist der Versicherte zu fragen, ob er in der Zwischenzeit eine neuere eGK von der Kasse zugeschickt bekommen hat. Nur wenn der Versicherte keine aktuellere eGK besitzt, muss er an seine Krankenkasse verwiesen werden.</p>

ABBRUCH BEIM EINLESEN AUFGRUND VON TECHNISCHEN FEHLERN

Wird das Einlesen der Versichertenstammdaten aufgrund von technischen Fehlern abgebrochen, ist es wichtig, dass Sie den spezifischen Fehlercode der Fehlermeldung an den Support (UHD) übermitteln.

Sind die Versichertenstammdaten auf der eGK inkonsistent (Fehlercode 3001), sollten Sie erneut versuchen, die Karte zu aktualisieren. Falls die Karte anschließend immer noch den Fehler aufweist, ist der Versicherte an seine Kasse zu verweisen. In allen anderen Fällen müssen Sie an den Support (UHD) ein Fehlerticket mit der entsprechenden Fehlernummer schicken.

In den Fällen, wo die vorgelegte Gesundheitskarte nicht verwendet werden kann, können Sie das Ersatzverfahren gemäß Bundesmanteltarifvertrag (BMV-Ä Anlage 4a Anhang 1 Kap. 2.4 bzw. bei BMV-Z und EKVZ die Vereinbarung zum Inhalt und Anwendung der elektronischen Gesundheitskarte, Anhang Abs. 3) anwenden. Diesem Gesetz entsprechend kann der Arzt vom Versicherten vorerst eine Privatvergütung verlangen. Der Patient hat dann die Möglichkeit, die Karte (innerhalb von 10 Tagen) nachzureichen, woraufhin das Geld zurückerstattet wird.

Warnung im Prüfungsnachweis (Prüfungsnachweis 3)

Aktualisierung VSD auf eGK technisch nicht möglich.

Fehlermeldung: Authentifizierungszertifikat eGK ungültig (Prüfungsnachweis 4)

Die eGK des Versicherten ist nicht gültig. Informieren Sie in diesem Fall den Patienten, dass er sich bei seiner Krankenkasse melden muss. Geben Sie ihm hierzu den Patientenflyer zum Online-Rollout Stufe 1 der gematik zur weiteren Erläuterung mit.

Aktualisierung VSD auf eGK technisch nicht möglich und maximaler Offline-Zeitraum überschritten (Prüfungsnachweis 6)

In diesem Fall gilt die Karte als gültiger Leistungsanspruchsnachweis. Bei einem weiteren Besuch im Quartal müssen Sie jedoch eine erneute Online-Prüfung der Karte durchführen.

Hinweis: Falls der entsprechende Fehler öfters auftritt, müssen Sie ein Fehlerticket mit dem genauen Fehlercode an den Support schicken.

Ungültiger Leistungsanspruchsnachweis aufgrund fachlicher Prüfung im Primärsystem

Falls nach dem erfolgreichen Einlesen der Versichertenstammdaten in das Primärsystem bei der fachlichen Prüfung festgestellt wird, dass die Karte kein gültiger Leistungsanspruchsnachweis ist (Versicherungsbeginn in der Zukunft oder Versicherungsende in der Vergangenheit), ist gemäß BMV-Ä Anlage 4a Anhang 1 Kap. 2.1. bzw. § 8 BMV-Z und § 12 EKVZ vorzugehen. Der Arzt kann in diesem Fall vorerst eine Privatvergütung verlangen. Im Anschluss kann der Patient die Karte (innerhalb von 10 Tagen) nachreichen, woraufhin das Geld erstattet wird.

SERVICE & KONTAKTDATEN

Bei Fragen wenden Sie sich an CompuGroup Medical Dentalsysteme GmbH, Maria Trost 25, 56070 Koblenz
Sie erreichen uns unter der Telefonnummer: 0800 450 0 650 (kostenfrei)
per E-Mail: technik.support.budental.de@cgm.com oder im Internet unter: cgm-dentalsysteme.de

Bei Fragen steht Ihnen natürlich jederzeit Ihr zuständiger Vertriebs-und Servicepartner zur Verfügung:

Stempel ZDVO

Die Unterlagen wurden ausgehändigt am: _____
Ort, Datum

SYMBOLE

	Patientenstamm des markierten Patienten
	Neuaufbau der Liste
	Telematik-Konfiguration (ausführliche Beschreibung nachfolgend)
	Fehlerhistorie (ausführliche Beschreibung nachfolgend)
	Hilfe (noch inaktiv)
	Liste Ereignisse / Abo, welches durch Anklicken geöffnet wird
	eGK wurde eingelesen, jedoch kein Prüfungsnachweis vorhanden
	eGK wurde mit erfolgreichem Prüfungsnachweis eingelesen
	eGK wurde im Quartal nicht eingelesen

FEHLERKATEGORIEN

•	Administrator
•	Leistungserbringer
	Anwender
	Hersteller
TI	gematik/Telematik

KARTENZUSTÄNDE

	Zugriffsfehler
	PIN blockiert
	PIN verifizierbar

INFRASTRUKTURZUSTÄNDE

	Telematikinfrastruktur-Verbindung unterbrochen
	Sichere Internetverbindung unterbrochen

FORTSCHRITTSANZEIGE (UHR)

	Patientenstamm des markierten Patienten
---	---

EREIGNISSE

	Karte gesteckt
	Karte entfernt
•••	Im Wartezustand
	Online-Prüfung läuft
	Kartenaktualisierung läuft
	Kartendaten werden gelesen
	Kartenzertifikat wird demnächst ablaufen
	Kartenzertifikat ist abgelaufen
	Fehler bei Online-Prüfung/Prüfungsnachweis fehlerhaft
	Kartenfehler

GLOSSAR

AIS	Arztinformationssystem
ZIS	Zahnarztinformationssystem
VPN	Virtual Private Network
LE	Leistungserbringer
LEI	Leistungserbringerinstitution
ORS	Online-Rollout Stufe ...
TI	Telematikinfrastruktur
VSD	Versichertenstammdaten
VSDM	Versichertenstammdatenmanagement
PS	Primärsystem
mobKT	mobiles Kartenterminal
KT	Kartenterminal

SCHULUNGS- UNTERLAGEN

TELEMATIKINFRASTRUKTUR

CompuGroup Medical Deutschland AG

Geschäftsbereich Telematikinfrastruktur

Maria Trost 21 | 56070 Koblenz

F +49 (0) 261 8000-2399

TI Support-Hotline

0800-551 551 2

cgm.com/wissensvorsprung

Synchronizing Healthcare



**CompuGroup
Medical**