Bedienungsanleitung ZEMO-VML-GK2 3.1.0

(Versichertenkarten-Mobil-Leser)
gem.
mobKT PTV1.3.0 (eGK Online-Rollout)

(Stand der Anleitung: V1.1.4, 18.04.2018)

1) Inhalt

2) Abbildungsverzeichnis

3) Vorwort

Herzlichen Glückwunsch zu Ihrer Kaufentscheidung!
Sie haben das leistungsfähige VML-GK2 erworben. Es ist zugelassen als mobiles Lesegerät für die Krankenversicherungskarte und die Gesundheitskarte (Onlinerollout). Die Funktionalität entspricht der Ausbaustufe 2 für mobile Kartenterminals. Es unterstützt das Lesen der geschützten Versichertendaten von der eGK.

Für das Lesen und Speichern von eGK´s und dem Übertragen von Kartendaten zum PC wird zwingend ein Heilberufsausweis (HBA) oder eine Institutskarte (SMC-B) benötigt.

Das VML-GK2 bietet Ihnen die Möglichkeit bei Hausbesuchen und Notdiensten Versichertenkarten und Gesundheitskarten zu speichern und anschließend in die Praxissoftware bzw. an den Drucker (mit optionalem Drucker-Konverter) zu übertragen.

Des Weiteren sehen Sie im großen Grafik-Display die wichtigsten Versichertendaten auf einen Blick. Wir wünschen Ihnen mit Ihrem neuen VML-GK2 viel Freude!
Ihre
ZEMO GmbH

4) Begriffserklärungen

Abbr	Abbruch der aktuellen Funktion
Abrechnungssystem	Primärsystem
Admin	Administrator, der autorisiert ist, das Gerät zu konfigurieren und Updates einzuspielen
Admin-PIN	Mit der Admin-PIN autorisiert sich der Administrator am Lesegerät.
AVS	Apothekenverwaltungssytem
Benutzer	Der Benutzer mit einer „berechtigten Karte“ kann eGK´s und KVK´s in das Lesegerät einlesen und zum PVS übertragen
Berechtigte Karte	Heilberufsausweis (HBA) oder Institutskarte (SMC-B) „berechtigen“ zum Auslesen der geschützten Daten der eGK
BSI	Bundesamt für Sicherheit in der Informationstechnik
C2C	Card-to-Card Authentifizierung zwischen berechtigter Karte und eGK, um die geschützten Daten der eGK frei zu schalten
Cross-CVC	Nachladbare Zertifikate die eine C2C-Authentifikation zwischen einer HPC und einer eGK mit unterschiedlichen Root-CA´s ermöglichen
eGK	elektronische Gesundheitskarte
gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
Gesicherte Umgebung	Als gesicherte Umgebung gilt der Bereich, der unter ständiger Kontrolle durch die berechtigten Benutzer oder den Administrator ist. Kann die Kontrolle für einen Zeitpunkt nicht ausgeübt werden, muss sichergestellt sein, dass das Lesegerät sicher verschlossen ist.
gVSD	geschützte Versichertendaten

HBA	Heilberufsausweis („berechtigte Karte“)
HBA-PIN	Pin zur Freischaltung des HBA
HBA / SMC	berechtigte Karten (HBA oder SMC-B)
HPC	„Health-Professional-Card“ = HBA oder SMC-B (siehe “Berechtigte Karte”)
KIS	Krankenhausinformationssystem
KVK	Krankenversichertenkarte
Mini-AK	Minianwendungskonnektor
Patientenkarte	Elektronische Gesundheitskarte (eGK)
Primärsystem	Computer an dem die Software PVS, KIS, AVS ausgeführt wird und mit dem Kartenleser kommuniziert
Primärsystemsoftware	Software, die auf dem Primärsystem installiert ist und bei Arzt / Apotheke / Krankenhaus eingesetzt wird
PUK	Personal Unblocking Key Ein PUK dient zum Entsperren einer Chipkarte, nachdem die PIN mehrmals falsch eingegeben wurde
PVS	Praxisverwaltungssystem
Slot1	seitlicher Kartenleser für eGK´s und KVK´s
Slot2	Hinterer Kartenleser für berechtige Karten
SMC	SMC = SMC-B Institutskarte („berechtigte Karte“)
SMC-PIN	Pin zur Freischaltung der SMC-B
SMC-B	Institutskarte („berechtigte Karte“)
VML-Security-Card	Die VML-Security Card ist eine Sicherheitskarte, die für einen alternativen Werksreset genutzt werden kann. Diese muss an einem gesicherten Ort (Tresor) aufbewahrt werden.
VSD	Versichertendaten

5) Sicherheitshinweise

Damit ein sicherer Betrieb gewährleistet ist, müssen die folgenden Hinweise beachtet werden:

Allgemeine Sicherheitshinweise:

- Überprüfen Sie vor jeder Inbetriebnahme des ZEMO VML-GK2, ob das Gehäuse unbeschädigt ist und die vorhandenen zwei Sicherheits-Siegel unversehrt sind (siehe Seite 15). Das Gehäuse ist so gebaut, dass die Siegel beim Öffnen zerstört werden. Dadurch können Manipulationen am Gerät sofort erkannt werden. Bitte wenden Sie sich bei Verdacht auf eine Manipulation an den Hersteller oder Ihren Lieferanten.
- Verfälschungen, Beschädigungen oder Verlust der Siegel führen zum Verlust der Zulassung des ZEMO-VML GK2; in diesem Fall darf es nicht weiter betrieben werden und muss zum Hersteller zur Überprüfung eingeschickt werden. Gewährleistungsansprüche sind in diesem Fall ausgeschlossen.
- Das ZEMO VML-GK2 muss aus Gründen der Datensicherheit stets sicher verwahrt werden und darf nur unter der verantwortungsvollen Obhut des Administrators oder des vom Administrator zugelassenen, berechtigten Benutzers benutzt werden.
- Bewahren Sie das ZEMO VML-GK2 bei Nichtbenutzung sicher in einer abgeschlossenen Umgebung auf. Es muss sichergestellt sein, dass ein Einbruch in diese abgeschlossene Umgebung in jedem Fall erkannt wird. Prüfen Sie bei der erneuten Nutzung, dass der Aufbewahrungsort nicht durch unsachgemäße Einwirkungen beschädigt wurde. Falls ja, darf das Gerät nicht

mehr verwendet werden und muss zum Hersteller eingesandt werden.

- Zur Vermeidung von externem Ausspähen der geheimen Informationen (PIN/PUK/Schlüssel/VSD) sollten Sie das VML-GK2 generell mindestens 1,0 Meter von allen technischen Geräten (z.B. Mobiltelefon / Empfangseinrichtungen / Radios / Abhöreinrichtungen usw.), sowie Kameras (Decke / Wand / Mobiltelefon usw.) und anderen Personen entfernt benutzen. Nebengeräusche während der PIN-Eingabe erschweren das akustische Ausspähen der PIN / PUK. Bewegung / Drehen bei der PIN-Eingabe erschweren das Ausspähen mittels externen Ausspäheinrichtungen.
- Beim Anschluss an einen PC stellen Sie sicher, dass das ZEMO VML-GK2 direkt mit der USB-Schnittstelle des PCs verbunden ist und keine weiteren Geräte zwischengeschaltet sind.
- Überprüfen Sie vor jeder Benutzung, ob das Datum und die Zeit des ZEMO VML-GK2 korrekt eingestellt sind.
- Autorisierte Personen müssen sicherstellen, dass sie, wenn sie das VML-GK2 übergeben, sich dieses nicht im autorisierten Zustand befindet. Das Lesegerät ist daher immer nur im ausgeschalteten Zustand zu übergeben.
- Laden Sie die aktuelle Bedienungsanleitung für das ZEMO VML-GK2 von der Webseite: www.zemo.de aus dem Bereich „Downloads“ herunter. Die Authentizität und die Integrität der Anleitung ist durch eine elektronische Signatur der Firma ZEMO GmbH, Franz-Mader-Str. 9 gewährleistet. Die Signatur können Sie, wie auf Seite 95 beschrieben, prüfen.
  Zur Info:
  Das BSI veröffentlicht im Zertifizierungsreport die SHA256-Checksumme der elektronischen Fassung der Anleitung und weist dort ebenfalls auf die Download-Möglichkeit hin. Der Zertifizierungsreport wird auf der BSI-Website

www.bsi.bund.de veröffentlicht. Sie haben die Möglichkeit, in den Zertifizierungsreport zu schauen und zu sehen, welche Versionen des Produktes zertifiziert sind und zu prüfen, ob ihnen auch die (mit-)zertifizierte Fassung der Anleitung vorliegt bzw. deren Integrität/Urheberschaft anhand der Checksumme zu prüfen.

- Die Bedienungsanleitung muss sowohl vom Admin, wie auch von allen Benutzern sorgfältig gelesen werden.
- Das Gerät darf nur gemäß der Bedienungsanleitung betrieben werden.
- Stellen Sie sicher, dass das VML-GK2 zur Datenübertragung nur mit einem Abrechnungssystem verbunden wird, welches Ihnen vertraut ist.

Sicherheitshinweise für den Administrator:

Der Administrator stellt sicher, dass:

- er die allgemeinen Sicherheitshinweise beachtet
- Uhrzeit und Datum des VML-GK2 immer korrekt gestellt sind
- ein Firmware-Update nur auf zertifizierte Versionen erfolgt
- die Administrator PIN umgehend nach einem Werksreset eingestellt wird
- nur gültige Heilberufsausweise (HBA) und gültige Institutskarten (SMC-B) als „Benutzer“ zugelassen werden
- er elektronisch im PC protokoliert, welche Person in welchem Zeitraum das Gerät mit einer Institutskarte (SMC-B) verwendet hat. Die Protokollierung von
  - autorisierende Person
  - Datum
  - Uhrzeit
  - autorisierte Fachkraft

kann z.B. mit einem Textverarbeitungs- oder Tabellenkalkulations-Programm erfolgen.

- die Zeit für die Benutzerinaktivität direkt nach dem Stellen der Admin-PIN eingestellt wird
- die Zeit für die Benutzerinaktivität direkt nach einem Werksreset eingestellt wird
- die Zeit für die Benutzerinaktivität auf einen möglichst geringen Wert eingestellt wird
- er die Admin-PIN geheim hält
- er bei PIN/PUK-Eingaben nicht beobachtet wird
- er die PUK für den Werksreset geheim hält
- er die VML-Security-Card sicher im Tresor aufbewahrt

Nach der Eingabe der Admin-PIN wird der sichere (Admin-autorisierte) Zustand beim VML-GK2 erreicht. Nach max. 15 Minuten Inaktivität setzt das VML-GK2 den Admin-autorisierten Zustand zurück. Der Administrator hat sicher zu stellen, dass die PIN-Eingabe nicht von Dritten beobachtet werden kann und das Gerät nach Nutzung wieder in den nicht Admin-autorisierten Zustand versetzt wird. Der Administrator muss sicherstellen, dass unberechtigte Personen keinen Zugang zu dem Gerät haben, wenn es sich im Admin-autorisierten Zustand befindet! Der Administrator darf das Gerät nur im ausgeschalteten Zustand an berechtigte Benutzer übergeben, da somit sichergestellt ist, dass das Gerät sich nicht im Admin-autorisierten Zustand befindet.

Sicherheitshinweise für den Benutzer (z.B. Arzt) mit HBA / SMC-B:

Der Benutzer mit Berechtigungskarte HBA / SMC-B (Arzt) stellt sicher, dass:

- er die allgemeinen Sicherheitshinweise beachtet
- er verantwortlich den sicheren Betrieb des VML-GK2, analog zum sichereren Betrieb von medizinischen Geräten und den gesetzlichen Datenschutzvorgaben, sowie der sicheren Aufbewahrung von Medikamenten, handhabt.
- er den Administrator anweist, eine möglichst geringe Zeit für die Benutzeraktivitätszeit einzustellen
- er regelmäßig prüft, ob Uhrzeit und Datum des VML-GK2 korrekt gestellt sind. (Beim Einschalten des Gerätes, ohne gesteckte Karten, werden Datum und Uhrzeit angezeigt)
- er die HBA/SMC-B-PIN geheim hält
- er bei PIN / PUK Eingaben nicht beobachtet wird
- er auf die Gültigkeit seines HBA/SMC-B achtet, da nach Ablauf der Zertifikatsgültigkeit des HBA / der SMC-B keine VSD mehr gespeichert und ausgelesen werden können
- er beim Lesen von Versichertendaten nicht beobachtet wird, mit der einzigen Ausnahme, dass er dem Versicherten seine Daten zeigen darf
- er nach Benutzung des Gerätes die HBA/SMC-B umgehend aus dem Leser entfernt, bzw. den HPC-autorisierten Status manuell beendet
- er vor Übertragung der VSD zum Primärsystem die Anschluss Leitung prüft, um ein Abhören der Übertragung zu verhindern
- er vor dem Drucken von VSD die Anschlussleitung zum Drucker prüft, um ein Abhören der Übertragung zu verhindern
- er die gespeicherten VSD täglich an sein Primärsystem überträgt.
- er die gespeicherten VSD nach Wegfall der Zweckbindung (Quartalsabrechnung) aus dem Speicher löscht, falls diese nicht schon vorher an das PVS übertragen wurden.
- bei Verwendung einer SMC-B als berechtigte Karte das Gerät ohne gespeicherte VSD übergeben wird.

6) Sicherheitssiegel

Das Gerät ist an den Stirnseiten mit je einem Sicherheits-Gehäusesiegel ausgestattet, mit dem die Trennfuge zwischen Ober- und Unterschale an zwei Stellen (Abb. 2) versiegelt ist.

Das Sicherheitssiegel weist folgende Authentizitätsmerkmale auf:
Das "BSI-Logo" und der Bundesadler sind mit einer Kippfarbe aufgedruckt, die in Abhängigkeit des Blickwinkels die Farbe von Rosa in Grün wechselt (Abb. 1).

Zusätzlich verfügt das Sicherheitssiegel über Stanzungen an den Rändern, die das zerstörungsfreie Ablösen erschweren.

Ein Siegel wird beschädigt durch:
- Versuch das Gehäuse zu öffnen
- beim Versuch das Siegel abzulösen
- durch mechanische oder thermische Belastung des Siegels.

Ein beschädigtes Siegel erkennt man an:
- Void-Effekt: helles Wabenmuster durch Farbumschlag (Abb. 3)
- Deformation oder eingerissene Kanten (Abb. 4)
- Zerstörung des Obermaterials durch Schnittfugen (Abb. 5)

Kontrollieren Sie beide Siegel regelmäßig auf ihre Unversehrtheit, um eine Manipulation des Gerätes auszuschließen. Verfälschung, Beschädigung oder Verlust der Siegel führen zum Verlust der Zulassung des ZEMO-VML GK2; in diesem Fall darf es nicht weiter betrieben werden und muss zur Überprüfung zum Hersteller gesandt werden!

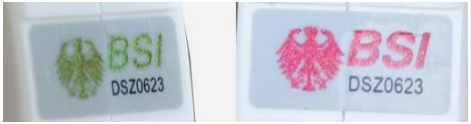


Abb. 1 (Sicherheitsmerkmal: Kippfarbe)

Abb. 2 (Sicherheitsmerkmal: Siegelposition Stirnseite vorne und hinten)

Abb. 3 (Siegel beschädigt, siehe helles Wabenmuster)

Abb. 4 (Siegel beschädigt, siehe eingerissene Kanten)

Abb. 5 (Siegel beschädigt, siehe Schnittkante)

7) Technische Daten

Speicherkapazität:	275 Krankenversichertenkarten (KVK) oder elektronische Gesundheitskarten (eGK)
Schnittstelle zum PC bzw. Drucker:	USB 2.0 (zum Anschluss eines Druckers mit serieller Schnittstelle ist der optionale VML-Drucker- Konverter notwendig)
Unterstützte Chipkarten:	Slot1 (seitlich): KVK, eGK Slot2 (hinten): HBA, SMC-B (gem. ISO 7816 Class A/B/C)
Spannungsversorgung:	mobil: 2x 1,5V Mignon (AA) Alkaline-Batterien stationär: USB-Schnittstelle PC
Temperaturbereich	
-Betrieb:	0 bis 40°C
-Transport:	-20 bis 60°C
Maße: (L x B x H)	155 x 62 x 25 mm
Gewicht:	ca. 206g incl. Batterien
Chipkartenleser:	2 Stk. Full-Size ID-1 Leser (ISO 7816) mit absenkenden, kartenschonenden Kontakten, 2 Stk. SIM-size ID-000 Leser (derzeit funktionslos)
Lieferumfang:	1x VML-GK2 Versichertenkartenleser, 2x 1,5V Batterie (Typ AA), 1x Mini-USB-Anschlusskabel, 1x Bedienungsanleitung, 1x Treiber-CD f. Windows 2000/XP/VISTA/Windows 7/8 und signierter Bedienungsanleitung
Zulassung:	gematik: mobKT (eGK Onlinerollout)

8) Grundlegende Bedienelemente

Tasten, Anzeige-Elemente, Kartenleser :

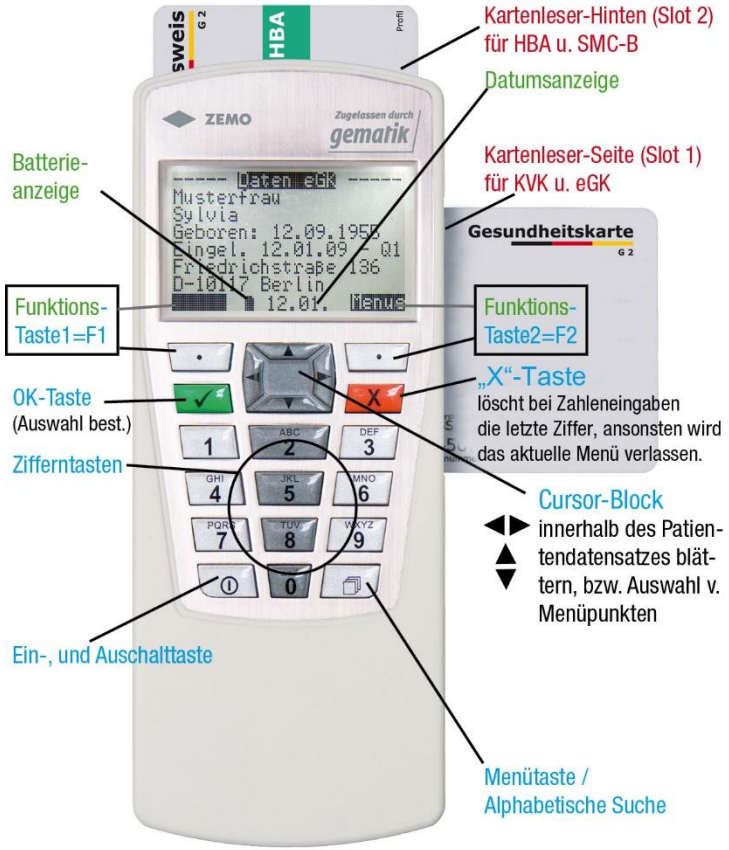


Abb. 6 (Grundlegende Bedienelemente)

Tasten und deren Funktion

Abb. 7 (Tasten und deren Funktionen)

9) Erste Schritte

1. Sie haben das VML-GK2 über den sicheren Lieferweg erhalten:
   a. Laden Sie sich das Dokument ***Zemo_sicherer_Lieferweg.pdf*** von der Webseite: ***https://www.zemo.de*** herunter.
   b. Das Dokument ist elektronisch signiert.
      Aussteller der Signatur ist:
      Ralf Sachling, ZEMO GmbH, 94036 Passau.
      Die Echtheit der digitalen Signatur können Sie mit einer dafür vorgesehenen Software oder auch im Internet, z.B. auf nachfolgender Website prüfen:
      www.signature-check.de.
   c. Lesen Sie sich das Dokument ***Zemo_sicherer_Lieferweg.pdf*** sorgfältig durch.
   d. Führen Sie alle Prüfungsschritte für das VML-GK2 entsprechend dem Dokument durch.
   e. Bei Unstimmigkeiten verwenden Sie das VML-GK2 nicht und informieren uns umgehend, damit wir Sie über die weitere Vorgehensweise beraten können!
2. Gerät für die erste Verwendung vorbereiten:
   Prüfen Sie den Packungsinhalt des Kartons nach dem Öffnen auf Vollständigkeit. (ZEMO VML-GK2 Leser, 2 Mignon Batterien, USB-Mini-Kabel, Anleitung, ZEMO VML-GK Treiber CD).
3. Lesen Sie sorgfältig die Sicherheitshinweise [s. Seite 10]
4. Lesen Sie das Kapitel zum Benutzerkonzept [s. Seite 24]
5. Überprüfen Sie vor jeder Inbetriebnahme die Unversehrtheit der Sicherheitssiegel des Lesegerätes [s. Seite 15]
6. Batterien einlegen
7. Gerät mit der Ein-/Ausschalttaste einschalten (mind. 1 Sek. drücken)

Das Gerät führt jetzt einen Selbsttest durch, hierbei wird auch die Integrität der Firmware geprüft [s. Seite 77]

8. Nach dem Einschalten prüfen Sie die Soft- und Hardwareversion des Gerätes und vergleichen Sie diese:

   a. mit dem auf der Geräterückseite aufgeklebten Produktlabel (Hardware-Version 2.0.0 = 2.0.0).

Abb. 8 (Hard- und Software-Version)

   Stimmt die im Gerät angezeigte HW-Version 2.0.0 nicht mit dem auf dem Aufkleber aufgedruckten HW-Version überein, wenden Sie sich bitte an den Hersteller oder Lieferanten und verwenden Sie das Gerät nicht.

   b. Die oben in Abb. 8 angezeigte Softwareversion ist 3.1.0. Informationen über zertifizierte Firmwareversionen finden Sie auf der Internetseite des BSI: *www.bsi.bund.de* (Zert.-ID: BSI-DSZ-CC-0623), sowie unter *https://www.zemo.de*. Befindet sich die im Gerät angezeigte SW-Version nicht in der Liste der zertifizierten Firmwareversionen, prüfen Sie, ob ein Update möglich ist [s. Seite 69], oder wenden Sie

sich an den Hersteller oder Lieferanten und verwenden Sie das Gerät nicht.

9. Nun müssen Sie die Transport-PIN eingeben und die ADMIN-PIN vergeben [s. Seite 50]
10. Falls Sie das VML-GK2 auffordert die VML-Security-Card einzulegen, ist dieser Schritt durchzuführen [s. Seite 56]. Die VML-Security-Card kann bei Zemo bestellt werden.
11. Überprüfen Sie die Uhrzeit und das Datum und korrigieren Sie dies evtl. [s. Seite 57]
12. Bevor Sie das Gerät das erste Mal mit dem PC verbinden, führen Sie das Installationsprogramm für das Gerät von der mitgelieferten CD auf Ihrem PC aus [s. Seite 31].
13. Legen Sie einen Benutzer an, der das Gerät zur Speicherung und Übertragung von Versichertendaten verwenden kann [s. Seite 26]. Sie benötigen dazu eine gültige HPC.
14. Jetzt ist das Gerät betriebsbereit und kann zum Einlesen von elektronischen Gesundheitskarten (eGK) oder Krankenversichertenkarten (KVK) durch den/die Benutzer verwendet werden [s. Seite 37].

10) Benutzer

Benutzer-Rollen:

- **Admin** („Administrator“)
  Der Admin ist der Administrator des Gerätes.

  Der Admin hat folgende Aufgaben / Rechte:
  - Benutzer anlegen / Verwalten (S. 26)
  - Das Gerät konfigurieren (S. 60)
  - Firmware-Updates durchführen (S. 69)
  - Einspielen von Cross-CVC’s (S. 66)

  Relevanz der Handbuch-Kapitel für den Admin:
  - Alle

  Autorisierung mittels:
  - Admin-PIN

  Autorisierungsstatus wird aufgehoben:
  - Spätestens nach 15 Minuten Inaktivität
  - Durch Ausschalten des Gerätes
  - Durch Verlassen des Admin-Menüs

- **Benutzer mit „berechtigter Karte“ (HBA / SMC-B)**
  Um Zugriff auf die geschützten Daten einer eGK zu erlangen, ist eine Freischaltung der eGK mittels einer berechtigten Karte (HBA oder SMC-B) erforderlich. Der Benutzer mit einer „berechtigten Karte“ wird im Folgenden „**Benutzer**“ genannt. Der Admin muss die berechtigte Karte (HBA oder SMC-B) des Benutzers beim Gerät zuerst zulassen, bevor diese mit dem Gerät verwendet werden kann.

  Der Benutzer hat folgende Aufgaben / Rechte:

- Einlesen und Speichern von eGKs und KVKs (S. 37)
- Übertragen der gespeicherten VSD-Daten zum PC (S. 40)
- Druck von Formularköpfen über einen angeschlossenen Drucker (S. 47)
- Änderung der PIN der „berechtigten Karte“ (S. 68)

Relevanz der Handbuch-Kapitel für den Benutzer:

- Begriffserklärungen (S. 8)
- Sicherheitshinweise (S. 10)
- Sicherheitssiegel (S. 15)
- Grundlegende Bedienelemente (S. 19)
- Benutzer-Rollen: (S. 24)
- Versichertenkarten speichern (S. 37)
- VSD-Kontextmenü (S. 39)
- Gespeicherte Versichertendaten an den PC übertragen (S.40)
- Formularkopfdruck (S. 47)
- Benutzer-Menü (S. 67)
- Selbsttest / Firmwareprüfung (S. 77)
- Manuelles Abschalten des VML-GK2 (S. 85)
- Batteriebetrieb – Stromsparmodus (S. 86)
- Event-/Fehlercodes (S. 90)

Autorisierung mittels:

- Einstecken „berechtigter Karte“ in Slot2 +
- Eingabe der zugehörigen PIN

Autorisierungsstatus wird aufgehoben:

- Durch Ausschalten des Geräts
- Entnehmen der „berechtigten Karte“
- Nach Ablauf der eingestellten Benutzerinaktivitätszeit

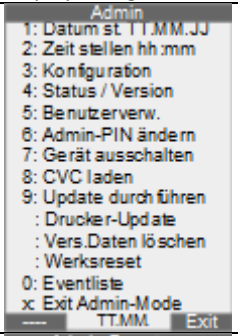
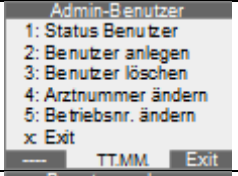
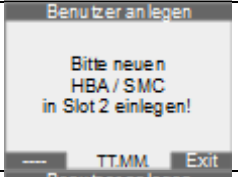
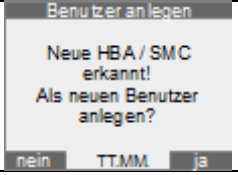
Benutzer anlegen

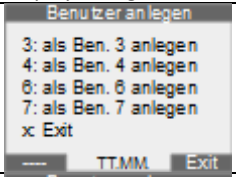
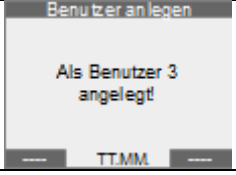
Ziel:
- Neuen Benutzer mit „berechtigter Karte“ (HBA oder SMC-B) anlegen

Ausgangssituation:
- Sie befinden sich im Admin-Menü [s. Seite 60]

Hinweise:
- Der Admin muss darauf achten, dass nur echte und gültige HBA´s und SMC-B‘s verwendet werden
- Es können bis zu 9 Benutzer angelegt werden
- Sind bereits 9 Benutzer angelegt, muss erst ein bestehender Benutzer gelöscht werden, bevor ein neuer angelegt werden kann. Es erfolgt die Meldung „Speicher voll! Schon 9 Benutzer angelegt“
- Der Admin darf das Gerät auch als Benutzer verwenden.
- Nach einem Firmware-Update oder einem Werksreset müssen alle Benutzer vom Admin neu angelegt werden!
- Durch einen Werksreset oder Firmware-Update sind alle bis dahin gespeicherten VSD und Konfigurationsdaten aller Benutzer gelöscht

Aktion:
- Folgende Schritte ausführen:

Displayanzeige	Tastatur-Eingabe
	5
	2
	Bitte die „berechtigte Karte“ (HBA oder SMC-B) in Slot 2 einlegen
	„OK-Taste“ drücken

Displayanzeige	Tastatur-Eingabe
	Bitte Nr. eines freien Benutzers eintippen
	

Benutzer löschen

Ziel:

- bestehenden Benutzer mit „berechtigter Karte“ (HBA oder SMC-B) löschen

Ausgangssituation:

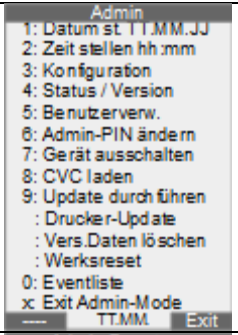
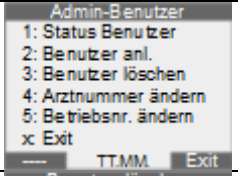
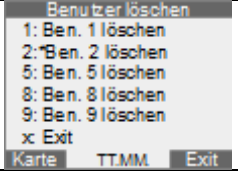
- Sie befinden sich im Admin-Menü [s. Seite 60]
- Der Benutzer, der gelöscht werden soll, ist bereits angelegt

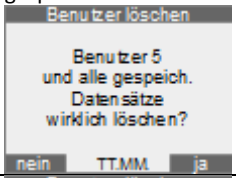
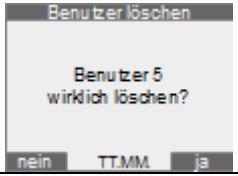
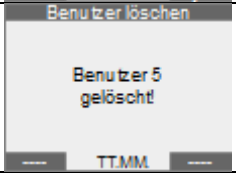
Hinweise:

- Achtung! Beim Löschen des Benutzers werden auch die von ihm im Gerät gespeicherten VSD gelöscht
- Ist noch kein Benutzer im Gerät angelegt, erfolgt die Meldung „Kein Benutzer angelegt“

Aktion:

- Folgende Schritte ausführen:

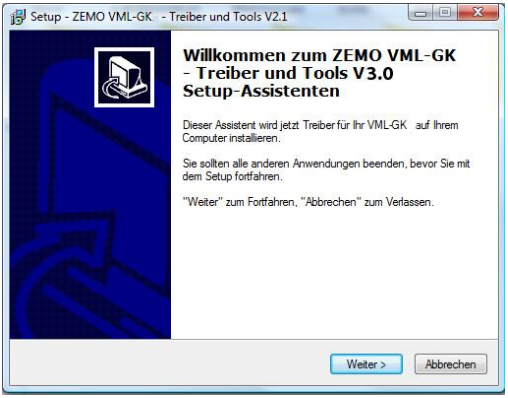
Displayanzeige	Tastatur-Eingabe
	5
	3
	Bitte Nr. des zu löschenden Benutzers eintippen

Displayanzeige	Tastatur-Eingabe
Je nachdem ob zu dem Benutzer Karten gespeichert sind oder nicht:  	„OK-Taste“ drücken
	

11) PC-Installation

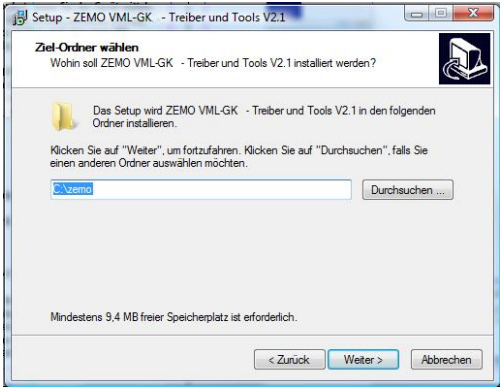
Microsoft Windows

1) Bevor Sie das ZEMO VML-GK2 mit dem PC verbinden, installieren Sie bitte zuerst die Treiber von der beiliegenden Treiber&Tools-CD. Unter Windows XP kann während der Installation folgende Meldung erscheinen: „Die Software hat den Windows Logo Test nicht bestanden“. Wichtig! Sie müssen die Installation dann trotzdem fortsetzen!
    a. Installationsstart:

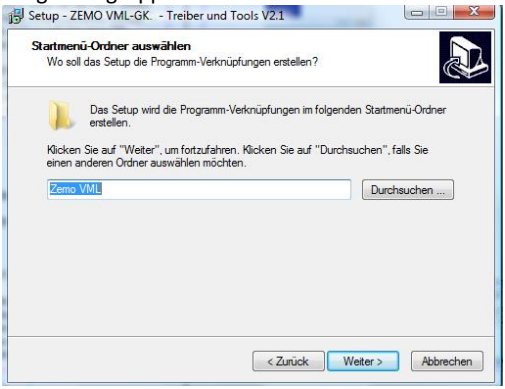


b. Akzeptieren der Lizenzvereinbarung

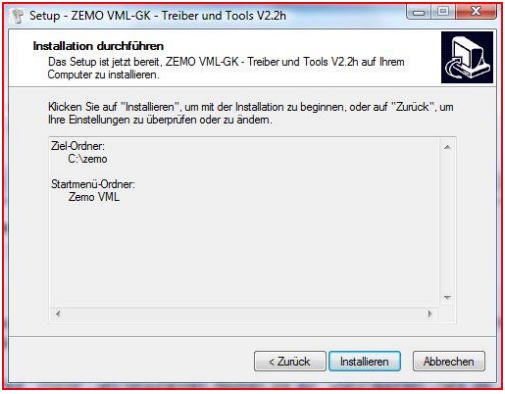
c. Installationsordner wählen:



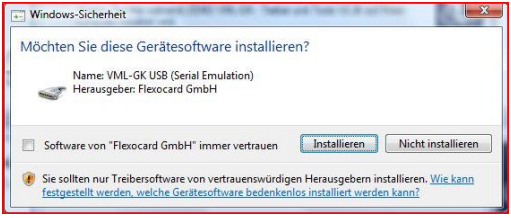
d. Programmgruppe wählen:



e. Klicken Sie auf Installieren:



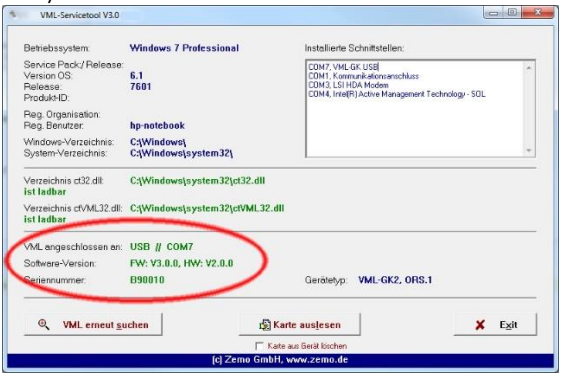
f. Klicken Sie auf Installieren:



g. Klicken Sie auf „Fertigstellen“:

2) Nun können Sie das VML-GK2 mit dem beiliegenden USB-Mini-Kabel an Ihren PC anschließen. Es wird ein “virtueller” COM-Port (serielle Schnittstelle) auf ihrem PC eingerichtet. Die Nummer dieses COM-Portes benötigen Sie für die Konfiguration in Ihrer Praxissoftware.

3) Um herauszufinden unter welchem COM-Port das ZEMO VML-GK2 angelegt wurde, starten Sie bitte das Programm: VML-Servicetool. (Dieses finden Sie unter Start->Programme->Zemo VML)



Linux / MAC OS X

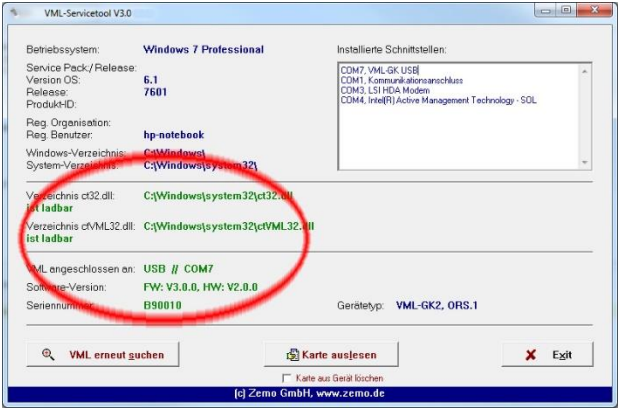
Die Betriebssysteme Linux und MAC OS werden vom Hersteller nicht unterstützt [Anmerkung: Das VML-GK2 wird unter Linux/Mac OS als serielles Gerät erkannt, ein Treiber für den USB-Anschluss ist nicht notwendig. Eine CTAPI wird vom Hersteller nicht zur Verfügung gestellt]

Ansteuerung des ZEMO VML-GK2 durch Ihre Praxissoftware:

Damit das Lesegerät korrekt mit Ihrer Praxissoftware arbeiten kann, muss es in Ihrer Praxissoftware korrekt konfiguriert werden. Konsultieren Sie hierzu das Handbuch Ihrer Praxissoftware bzw. den Ansprechpartner für Ihre Praxissoftware.

a) Ansteuerung mit eigenem Treiber der Praxissoftware:
Zur Einstellung in Ihrer Praxissoftware benötigen Sie den COM-Port, an dem das Lesegerät angeschlossen ist.

b) Ansteuerung mittels standardisierter CT-API-Schnittstelle unter Windows: Zur Einstellung in Ihrer Praxissoftware benötigen Sie den COM-Port an dem das Lesegerät angeschlossen ist. Zusätzlich müssen Sie als CTAPI-Datei: ctVML32.dll in Ihrer Praxissoftware eintragen. Diese wurde bei der Installation automatisch in das Windows-System32- bzw. Syswow64-Verzeichnis installiert. Ob die Installation erfolgreich war können Sie mit dem Programm "VML-SERVICETOOL" testen. Sie finden es unter Start-Programme-ZEMO VML.



12) Versichertenkarten speichern

Ziel:

- Einlesen und Speichern der VSD einer eGK oder einer KVK

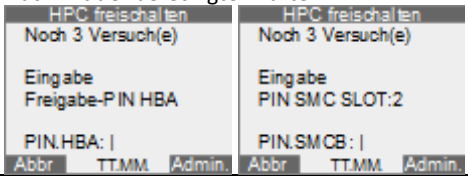
Ausgangssituation:

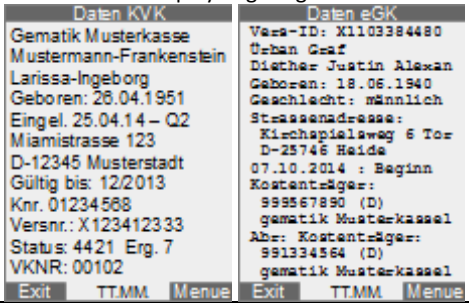
- VML-GK2 ist ausgeschaltet
- Der Benutzer ist mit seiner „berechtigten Karte“ ist im Gerät angelegt
- Die „berechtigte Karte“ ist noch gültig

Sicherheitshinweise:

- Prüfen Sie bei jedem Speichern von VSD, dass das Datum im Lesegerät korrekt gestellt ist. Falls die VSD zu einem falschen Datum gespeichert werden, können diese evtl. nicht mehr für die Abrechnung verwenden werden.
- Bitte entfernen Sie die „berechtigte Karte“ nach dem erfolgreichen Lesevorgang aus dem Gerät und bewahren Sie diese getrennt auf, damit die Karte nicht zusammen mit dem Gerät verloren gehen kann

Notwendige Schritte zum Einlesen der eGK oder KVK:

Displayanzeige	Aktion
Keine	„berechtigte Karte“ in Slot2 einlegen
Nach Art der berechigten Karte: 	SMC / HBA -PIN eingegeben OK-Taste drücken

Displayanzeige	Aktion
	eGK bzw. KVK in Slot1 stecken
Nach erfolgreicher Speicherung werden die VSD-Daten im Display angezeigt. 	eGK / KVK und die „berechtigte Karte“ aus dem Lesegerät entfernen

<u>Tastenbelegung während die VSD im Display angezeigt werden:</u>
Das Anzeigefenster kann man verschieben, um Daten mit mehr Zeichen als die Displaybreite/-höhe darstellen zu können. Bei langen Zeilen wird die Möglichkeit des Schiebens durch einen inversen Pfeil angezeigt.

Pfeil links:	Lange Zeilen eine Stelle nach rechts
Pfeil rechts:	Lange Zeilen eine Stelle nach links
Pfeil hoch:	Fenster eine Zeile höher
Pfeil runter:	Fenster eine Zeile tiefer
Taste 1:	Lange Zeilen an den Anfang
Taste 3:	Lange Zeilen an das Ende
Taste 7:	An den Anfang des Anzeigefensters
Taste 9:	An das Ende des Anzeigefensters

Taste 0: Umschaltung Normale Ansicht/Rezeptansicht
Taste 5: Umschaltung normale Ansicht / Vollbild

Hinweise:

- Durch das Drücken der Menütaste bei angezeigten VSD gelangen Sie in das VSD-Kontextmenü [siehe Seite 39]. In diesem können Sie z.B. die im Gerät gespeicherten VSD der angezeigten Karte manuell löschen oder einen Formularkopfdruck auslösen
- Falls sich die Gültigkeit der „berechtigten Karte“ innerhalb des Ablauf-Zeitraums „Vorwarnzeit Gültigk.“ befindet, wird ein Warnhinweis angezeigt, dass die Gültigkeit der „berechtigten Karte“ bald abläuft
- Nach Ablauf des Gültigkeitszertifikats des HBA bzw. der SMC-B lassen sich keine KVK / eGK mehr in das VML-GK2 einlesen! Bitte beachten Sie, dass die Neubeschaffung eines HBA / SMC-B rechtzeitig erfolgt!
- Ist die Gültigkeit der KVK / eGK abgelaufen, erfolgt ein Hinweis
- Sollte die Karte für das aktuelle Quartal bereits gespeichert sein, werden die gespeicherten VSD im VML-GK2 aktualisiert
- Bei Anzeige eines Fehlercodes [siehe Seite 90]

13) VSD-Kontextmenü

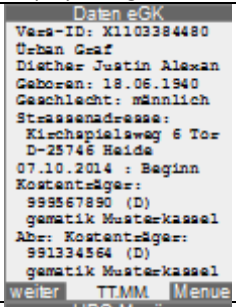
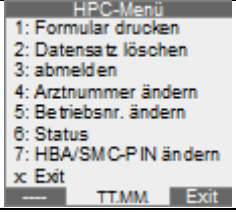
Mögliche Ziele:

- Formularkopf drucken
- Gespeicherten VSD-Datensatz löschen
- Abmelden (Autorisierungsstatus der „berechtigten Karte“ beenden)
- Arztnummer ändern (für Formularkopfdruck)
- Betriebsnummer ändern (für Formularkopfdruck)
- Speicherstatus anzeigen lassen
- HBA/SMC-PIN ändern

Ausgangssituation:

- Es werden VSD im Display angezeigt

Notwendige Schritte zum Aufruf des VSD-Kontextmenüs:

Displayanzeige	Aktion
	Funktionstaste 2 Drücken
	Menüpunkt auswählen

14) Gespeicherte Versichertendaten an den PC übertragen

Ziel:

- Übertragen von gespeicherten VSD an den PC

Ausgangssituation:

- VML-GK2 ist ausgeschaltet
- Das VML-GK2 ist korrekt im PVS konfiguriert

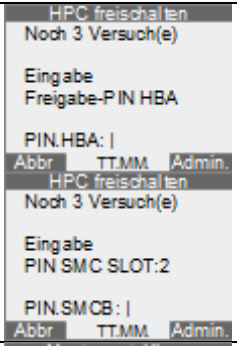
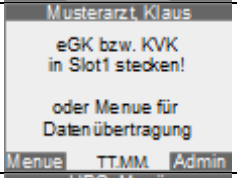
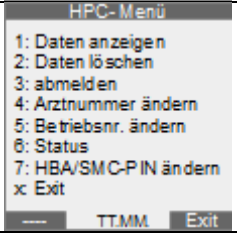
- Das PVS verwendet das richtige Übertragungsprotokoll. Für KVK gilt standardmäßig das PC-ASN.1-Format
- Der Benutzer ist mit seiner „berechtigten Karte“ im Gerät angelegt
- Die „berechtigte Karte“ ist noch gültig
- Es befindet sich keine eGK / KVK in Slot1

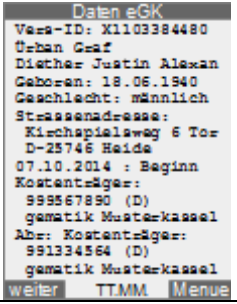
Sicherheitshinweise:

- Schließen Sie das VML-GK2 nur an ein Primärsystem an, welches Ihnen bekannt und vertraut ist.
- Stellen Sie sicher, dass das VML-GK2 über eine direkte Kabelverbindung mit dem Primärsystem verbunden ist.
- Der Benutzer kann nur die mit seiner „berechtigten Karte“ eingelesenen Daten anzeigen und zum PC übertragen
- Durch Eingabe der SMC / HBA – PIN wird die „berechtigte Karte“ freigeschaltet und befindet sich damit im HPC-autorisierten Zustand. Dieser Zustand wird durch die folgenden Ereignisse beendet
    - Ausschalten des Gerätes
    - Entnahme der „berechtigten Karte“
    - Überschreiten der Benutzerinaktivitätszeit
- Bitte entfernen Sie die „berechtigte Karte“ nach dem erfolgreichen Übertragungsvorgang aus dem Gerät und bewahren Sie diese getrennt und sicher auf, damit sie nicht mit dem Gerät verloren gehen kann.

Notwendige Schritte zum Übertragen von VSD zum PC:

Displayanzeige	Aktion
Keine	„berechtigte Karte“ in Slot2 einlegen
Nach Art der berechigten Karte:	SMC / HBA -PIN eingegeben OK-Taste drücken

	
	Funktionstaste1 oder Menue-Taste drücken
	Menüpunkt „1: Daten anzeigen“ Auswählen
Sobald **VSD-Daten angezeigt** werden,	Im Praxisverwaltungssystem den „Lesebefehl“ zum Einlesen von VSD geben. Konsultieren Sie hierzu die Anleitung Ihres PVS.

ist das VML-GK2 zur **Datenübertragung bereit** 	
	Im Anschluss an die erfolgreiche Übertragung werden die übertragenen VSD im Lesegerät durch das PVS gelöscht und es wird der nächste VSD-Satz im Display angezeigt (soweit vorhanden).

Hinweise:

- Erfolgt keine korrekte Übertragung eines Datensatzes (einer Karte) mit anschließendem Löschbefehl durch die Software, lässt sich nur noch dieser Datensatz (diese Karte) übertragen, solange bis dieser gelöscht wird. Im Display sehen Sie die Meldung “Datensatz fixiert” (Fortschaltsperre).

Tastenbelegung während die VSD im Display angezeigt werden:

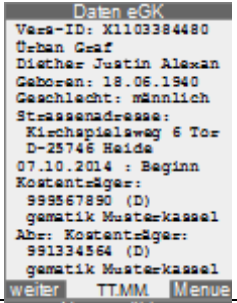
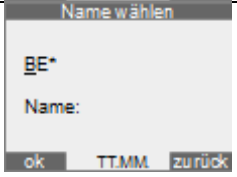
Das Anzeigefenster kann man verschieben, um Daten mit mehr Zeichen als die Displaybreite/-höhe darstellen zu können. Bei langen Zeilen wird die Möglichkeit des Schiebens durch einen inversen Pfeil angezeigt.

Pfeil links:	Lange Zeilen eine Stelle nach rechts
Pfeil rechts:	Lange Zeilen eine Stelle nach links
Pfeil hoch:	Fenster eine Zeile höher
Pfeil runter:	Fenster eine Zeile tiefer
Taste 1:	Lange Zeilen an den Anfang
Taste 3:	Lange Zeilen an das Ende
Taste 7:	An den Anfang des Anzeigefensters
Taste 9:	An das Ende des Anzeigefensters
Taste 0:	Umschaltung Normale Ansicht/Rezeptansicht
Taste 5:	Umschaltung normale Ansicht / Vollbild
Taste 4:	vorheriger Datensatz
Taste 6:	nächster Datensatz
F1-Taste:	weiter zum nächsten Datensatz (nur falls vorhanden)
F2-Taste:	VSD-Kontext-Menü aufrufen
Menü-Taste:	Alphabetische Suche aufrufen
X-Taste:	2 mal drücken ->zum Speichermodus wechseln

VSD-Datensätze mittels „Suche“ finden

Ziel:

- Auffinden von VSD nach Namen (alphabetisch)

	Drücken Sie die Menü-Taste/Alph. Suche
	Wenn mehr als ein VSD-Datensatz gespeichert ist, werden alle im Gerät befindlichen Anfangsbuchstaben der Nachnamen angezeigt

Tastenbelegung bei der Namensauswahl:

- Pfeil rechts: springt zum nächsten Buchstaben
- Pfeil links: springt zurück zum vorherigen Buchstaben
- OK: übernimmt den Buchstaben, und zeigt den Folgebuchstaben an, wenn kein weiterer vorhanden ist, wird der Patient mit dem gewählten Buchstaben angezeigt.

Hinweis:

- Die Sortierung erfolgt entweder alphabetisch oder chronologisch (nach Einlese Datum), wie im Admin-Menü unter “5: Sortierung einst.“ konfiguriert

15) Druckeinstellungen für Formularkopfdruck

Ziel:

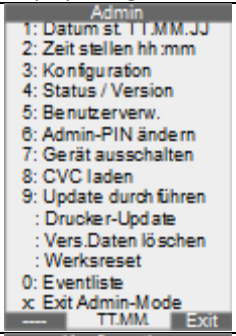
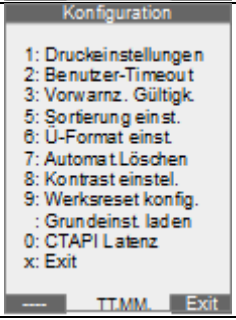
- Drucker für Formularkopfdruck konfigurieren

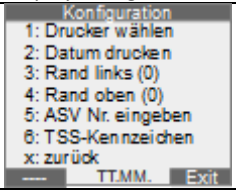
Ausgangssituation:

- Sie befinden sich im Admin-Menü [s. Seite 60]

So gelangen Sie ins Drucker-Konfigurationsmenü:

- Folgende Schritte ausführen:

Displayanzeige	Tastatur-Eingabe
	3
	1

Displayanzeige	Tastatur-Eingabe
	Gewünschten Menüpunkt auswählen

Beschreibung der Menüpunkte

- 1: Drucker wählen:
  - Auswahl des angeschlossenen Druckertyps.
    Hinweis: Es werden nur diese Drucker unterstützt!
    Beim ZEMO VML-GK Arztbüro: Formulardruck. 1
- 2: Datum drucken
  - Einstellen, ob das Datum mitgedruckt wird
- 3: Rand links (0):
  - Über Rand links lässt sich der linke Druckrand Zeichenweise nach rechts verschieben
- 4: Rand oben (0):
  - Über Rand oben lässt sich der obere Druckrand Zeilenweise nach unten verschieben
- 5: ASV Nr. eingeben:
  ASV-Nummer eingeben oder ändern (für Formularkopfdruck)

- 6: TSS-Kennzeichen:
  Druck des TSS-Kennzeichens aktivieren (ein) /deaktivieren (aus) (für Formularkopfdruck)

16) Formularkopfdruck

Ziel:

- Formularkopf drucken

Ausgangssituation:

- Es werden VSD im Display angezeigt
- Ein kompatibler Drucker ist mit dem VML-GK2 verbunden und korrekt konfiguriert [s. S. 46]

Sicherheitshinweise:

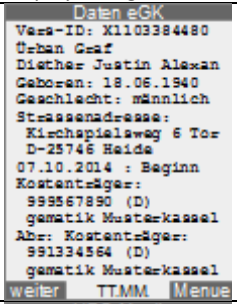
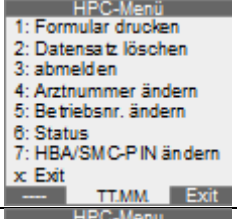
Um ein Abhören der Versichertendaten bei der Übertragung zum Drucker zu verhindern, muss die Übertragungsleitung zum Drucker geprüft werden.

Hierbei muss sichergestellt sein, dass das Lesegerät über eine direkte Kabelverbindung mit dem Drucker verbunden ist, die sich komplett im Sichtbereich befindet.

Hinweis:

- ASV-Kennzeichen: Wenn in der Druckerkonfiguration die ASV-Nr. eingegeben wurde, wird beim Formularkopfdruck abgefragt, ob die ASV-Nummer (anstelle der Betriebsstätten-Nummer) gedruckt werden soll.
- TSS-Kennzeichen: Wenn in der Druckerkonfiguration das TSS-Kennzeichen aktiviert wurde, wird beim Formularkopfdruck zusätzlich abgefragt, ob es sich um Entlass-Management handelt.

Notwendige Schritte zum Aufruf des VSD-Kontextmenüs:

Displayanzeige	Aktion
	F2-Taste Drücken
	Menüpunkt 1 auswählen
	

17) Transport-PIN / Admin-PIN ändern

Transport-PIN

Transport-PIN nach Versand über sicheren Lieferweg:

Wenn das VML-GK2 über den sicheren Lieferweg versandt wird, erhalten Sie kurz vor Lieferung des Gerätes eine individuelle Transport-PIN und einen Prüfcode. Diese Informationen sind sicher zu verwahren (z.B. Tresor), denn nach einem Werksreset müssen Sie die individuelle Transport-PIN erneut eingeben.

Beim Festlegen der Admin-PIN die Variante 1 wählen.

Transport-PIN nach Einspielen eines Updates:

Mit Einspielen eines Updates wird die Transport-PIN des VML-GK2 auf den Standard-Wert „00000000“ zurückgesetzt. Der Prüfcode entfällt. Diese Einstellung ist auch nach Durchführung des Werksreset aktiv.

Beim Festlegen der Admin-PIN die Variante 2 wählen.

Sicherheitshinweise:

- Die Admin-PIN hat eine Länge von 8-12 Ziffern!
- Zur Sicherheit sollten Sie keine leicht erratbare Kombination wählen. Z.B. Nicht 8-12 x die gleiche Ziffer verwenden oder ihr Geburtsdatum!
- Bei Verlust der Admin-PIN ist das Gerät evtl. nicht mehr verwendbar!
- Die Admin-PIN schützt die Management-Schnittstelle, für das Auslesen und Übertragen von VSD wird die HBA- / SMC-B-PIN benötigt!
- Die individuelle Transport-PIN und der Prüfcode sind sicher zu verwahren (z.B. Tresor), da nach der Durchführung eines Werksresets diese Daten zur Inbetriebnahme benötigt werden. Bei Verlust muss

das VML-GK2 zum Hersteller zur kostenpflichtigen Rücksetzung eingesandt werden!

- Sollte das VML-GK2 die individuelle Transport-PIN nicht akzeptieren, oder der Prüfcode stimmt nicht mit der Vorgabe überein, darf das Gerät nicht verwendet werden. Der Hersteller ist umgehend zu informieren!

Ziel – Admin-PIN festlegen:

- Admin-PIN vergeben (z.B. bei Neugerät oder nach Werksreset)

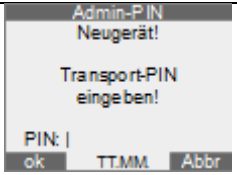
Ausgangssituation:

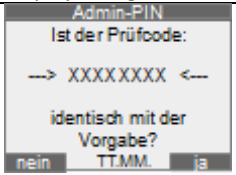
- VML-GK2 ist ausgeschaltet
- Es wurde noch keine Admin-PIN vergeben oder die Admin-PIN wurde durch ein Firmware-Update oder einen Werksreset zurückgesetzt

Variante 1:
Sie haben das VML-GK2 über den sicheren Lieferweg erhalten, Ihnen liegt die individuelle Transport-PIN und der Prüfcode zu dem Gerät vor.

Aktion:

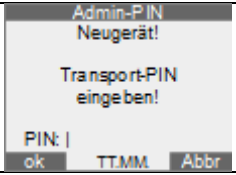
- Einschalttaste drücken und folgende Schritte ausführen:

Displayanzeige	Tastatur-Eingabe
	XXXXXXXX* OK-Taste drücken * *die individuelle Transport-PIN eingeben, die Ihnen mitgeteilt wurde*

Displayanzeige	Tastatur-Eingabe
	Prüfen Sie, ob der angezeigte Prüfcode identisch zum mitgeteilten Prüfcode ist. • Prüfcode identisch: Wählen Sie „ja“ • Prüfcode nicht identisch: Wählen sie „nein“ Das Gerät darf in diesem Fall nicht verwendet werden!

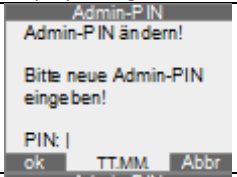
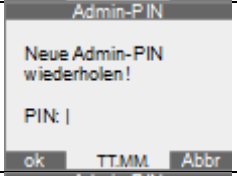
Variante 2:
Sie haben ein Update in das VML-GK2 eingespielt.

Aktion:
- Einschalttaste drücken und folgende Schritte ausführen:

Displayanzeige	Tastatur-Eingabe
	00000000 OK-Taste drücken

Festlegen der Admin-PIN (beide Varianten):

Aktion:
- Folgende Schritte ausführen:

Displayanzeige	Tastatur-Eingabe
	Admin-PIN eingegeben OK-Taste drücken
	Admin-PIN wiederholen OK-Taste drücken
	

Admin-PIN ändern

Ziel:
- Admin-PIN ändern

Ausgangssituation:
- Sie befinden sich im Admin-Menü [s. Seite 60]

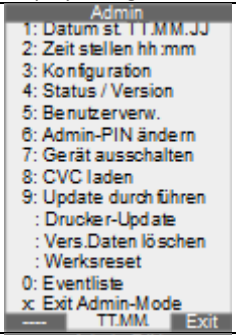
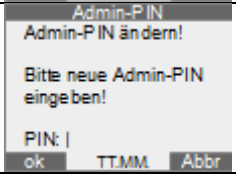
Sicherheitshinweise:
- Die Admin-PIN hat eine Länge von 8-12 Ziffern!
- Verwenden Sie keine leicht erratbaren Kombinationen:
  - Zur Sicherheit sollten Sie nicht 8-12 x die gleiche Ziffer verwenden

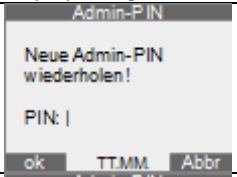
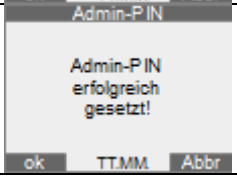
- Verwenden Sie auch nicht ihr Geburtsdatum oder auf/absteigende Ziffernfolgen

- Bei Verlust der Admin-PIN ist das Gerät evtl. nicht mehr verwendbar!
- Die Admin-PIN schützt die Management-Schnittstelle, für das Auslesen und Übertragen von VSD wird die HBA- / SMC-B-PIN benötigt!

Aktion:

- Folgende Schritte ausführen:

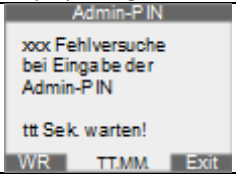
Displayanzeige	Tastatur-Eingabe
	6
	Admin-PIN eingegeben OK-Taste drücken

Displayanzeige	Tastatur-Eingabe
	Admin-PIN wiederholen OK-Taste drücken
	

18) Sperrzeit bei wiederholt falscher Admin-PIN-Eingabe

Nach mehr als 2 Fehlversuchen bei der Admin-PIN-Eingabe, sperrt das VML-GK2 die folgende Admin-PIN-Eingabe aus Sicherheitsgründen:

Anzahl erfolgloser Eingaben	Dauer der Sperre
3-6	1 Minute
7-10	10 Minuten
11-20	1 Stunde
>20	1 Tag

Displayanzeige	Beschreibung
	XX = Anzahl der Fehlversuche tt = aktuell verbleibende Wartezeit

Hinweis:

- Die Sperrzeit wird durch das Aus-/Einschalten des Gerätes weder gelöscht, noch neu gestartet. Sie können während der Sperrzeit aus Stromspargründen das Gerät abschalten
- Nach Ablauf der Sperrzeit wird die Nummer des PIN-Eingabeversuches angezeigt
- Wird eine zu kurze PIN Eingegeben erfolgt ein Piepton.
  Eine zu kurze PIN-Eingabe wird nicht als Fehlversuch gezählt.

19) VML-Security-Card

Die VML-Security-Card dient zum Autorisieren eines Updates und kann für einen „Alternativen Werksreset“ aktiviert werden.

Die VML-Security-Card wird zur Verwendung in den hinteren Kartenleser eingeschoben, **während Nichtverwendung ist die VML-Security-Card an einem gesicherten Ort (Tresor) aufzubewahren!**

Mit einer aktivierten VML-Security-Card können Sie das VML-GK2 wieder auf die Werkseinstellung zurücksetzen, falls Sie Ihre ADMIN-PIN vergessen haben. Siehe „Alternativer Werksreset“ auf S. 77

Hinweis: Eine verwendete VML-Security-Card kann an einem weiteren VML-GK2 nicht genutzt werden.

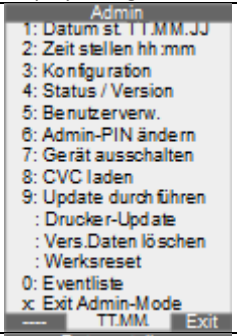
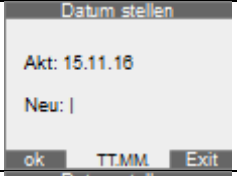
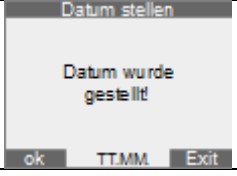
20) Datum / Uhrzeit einstellen

Ziel:
- Datum und Uhrzeit stellen

Ausgangssituation:
- Sie befinden sich im Admin-Menü [s. Seite 60]

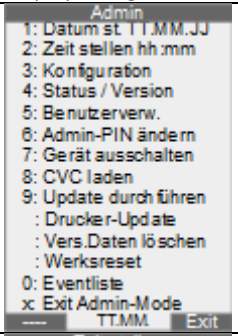
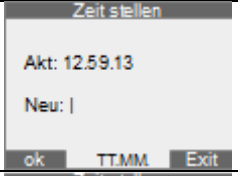
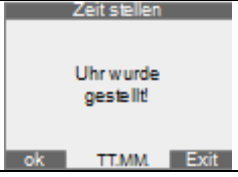
Sicherheitshinweise:
- Die Uhrzeit lässt sich jederzeit vom ADMIN stellen
- Das Datum lässt sich nur ändern, wenn keine VSD im Gerät gespeichert sind
- Die Uhrzeit wird automatisiert zwischen Sommer/Winterzeit umgestellt

Aktion für Datum stellen:
- Folgende Schritte ausführen:

Displayanzeige	Tastatur-Eingabe
	1
	Datum stellen OK-Taste drücken
	

Aktion für Uhrzeit stellen:

- Folgende Schritte ausführen:

Displayanzeige	Tastatur-Eingabe
	2
	Zeit stellen OK-Taste drücken
	

21) Admin-Menü

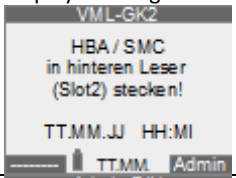
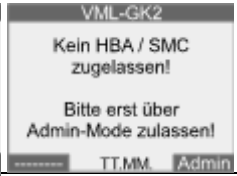
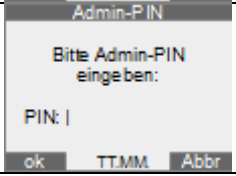
Aufruf des Admin-Menüs (Admin-PIN bereits gesetzt)

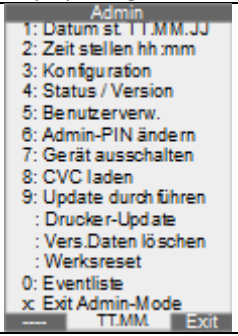
Ausgangssituation:

- VML-GK2 ist ausgeschaltet
- es befinden sich keine Chipkarten in den Leseschlitzen
- die Admin-PIN ist bereits vergeben

Aktion:

- Einschalttaste drücken
- Folgende Schritte ausführen:

Displayanzeige	Tastatur-Eingabe
Wenn ein Benutzer bereits angelegt ist, erscheint die linke, ansonsten die rechte Displaymeldung:  	Funktionstaste „2“ drücken
	Admin-PIN eingegeben OK-Taste drücken

Displayanzeige	Tastatur-Eingabe
	Menüauswahl treffen

Tastenbelegung:

- Die Zifferntasten wählen die Menüpunkte direkt
- OK-Taste wählt den ausgewählten Menüpunkt
- Pfeiltasten wechseln zwischen den Menüpunkten
- X-Taste springt jeweils eine Menüebene zurück. In der obersten Menüebene wird das Admin-Menü mit der der X-Taste beendet.

Menüstruktur des Admin-Menüs

Menüpunkte:	***Default-Werte bei Auslieferung***
1: Datum st. TT.MM.JJ	*Aktuelles Tagesdatum*
2: Zeit stellen	*Aktuelle Zeit*
3: Konfiguration	
1: Druckereinstellung	
1: Drucker wählen	*1:Standarddrucker*
2: Datum drucken	*1:Datum drucken*
3: Rand links	*0*
4: Rand oben	*0*
5: ASV Nummer	*leer*
6: TSS-Kennzeichen	*aus*
X: zurück	
2: Benutzer-Timeout	*60 Min.*
3: Vorwarnzeit Gültigk.	*90 Tage*
5: Sortierung einst.	*3:Alphabet*
6: Ü-Format einst.	*1:ASN.1*
7: Automat. Löschen	*1:Löschenn. Kommando*
8: Kontrast einstellen	*5*
9: Werksreset konfig.	
: Grundeinst. Laden	
0: CTAPI Latenz	AUS
X: Exit	
4: Status / Version	*(Siehe S. 21)*
5: Benutzerverw.	
1: Status Benutzer	*Anzahl angelegter User: 0*
2: Benutzer anlegen	
3: Benutzer löschen	
4: Arztnummer ändern	*leer*
5: Betriebsnr. ändern	*leer*
X: Exit	
6: Admin PIN ändern	
7: Gerät ausschalt.	
8: CVC laden	
9: Update durchf.	
: Drucker-Update	
: Vers. Daten löschen	
: Werksreset	
0: Eventliste	*leer*

x: Exit Admin-Mode

Beschreibung der Menüpunkte des Admin-Menüs:

1: Datum stellen
Siehe Seite 57

2: Zeit stellen
Siehe Seite 57

3.1: Druckereinstellungen
Siehe Seite 46

3.2: Benutzer-Timeout
Der Benutzertimeout dient der Rücksetzung des Autorisierungsstatus nach Ablauf der hier eingestellten Benutzerinaktivitätszeit in Minuten. Der Minimalwert beträgt 1 Minute, der Maximalwert 60 Minuten. Der Administrator stellt sicher, dass die Benutzerinaktivitätszeit auf einen minimalen Wert gestellt wird.

3.3: Vorwarnzeit Gültigkeit
Ist die Restgültigkeit der „berechtigten Karte“ kleiner als die hier eingestellte Zeit (in Tagen), erscheint ein Warnhinweis im Display des VML-GK2. So können Sie rechtzeitig erkennen, dass die berechtigte Karte abläuft. Minimalwert: 10 Tage, Maximalwert: 150 Tage

3.5: Sortierung einstellen
Je nach eingestellter Sortierung werden die VSD-Daten alphabetisch oder chronologisch bei der Datenausgabe [siehe S. 44] angezeigt

3.6: Ü-Format einst.
Hier können Sie das Übertragungsformat für KVKs festlegen. Das Standard-Übertragungsformat für KVKs ist das ASN.1-Format.

3.7: Automat. Löschen
Falls Ihr Primärsystem keinen Löschbefehl nach erfolgreicher Übertragung an den PC an das Lesegerät sendet, können Sie „2: Automatisch löschen“ einstellen. Dann wird die Karte auch ohne „Löschbefehl vom PC“ nach erfolgreicher Übertragung aus dem Gerät gelöscht. Soll die Karte nach erfolgreicher Übertragung durch den Löschbefehl des PC gelöscht werden, wählen Sie „1: Löschen nach Kommando“.

3.8: Kontrast einstellen
Hier können Sie den optimalen Kontrast des Displays einstellen

3.9: Werksreset konfigurieren
Der „alternative Werksreset“ bietet die Möglichkeit das Gerät auf den Auslieferungszustand zurückzusetzen, falls Sie die Admin-PIN vergessen haben. Der „alternative Werksreset“ muss erst durch den Admin aktiviert und konfiguriert werden, bevor er verwendet werden kann. Das VML-GK2 bietet den „alternativen Werksreset“ über eine PUK, die von Ihnen vergeben werden kann oder über die VML-Security-Card, welche vom Admin autorisiert werden muss. Der „alternative Werksreset“ lässt sich über die Menüpunkte „3.9.1 Werksreset via PUK“ und „3.9.2 Werksreset via Chipkarte“ aktivieren und konfigurieren.

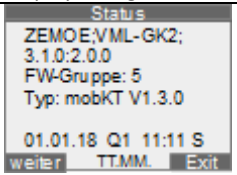
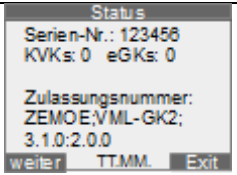
3. : Grundeinst. Laden
Grundeinstellungen laden dient dazu, Grundeinstellungen wie z.B. Übertragungsformat, Druckereinstellungen auf den Auslieferungszustand zurückzusetzen. Hierbei werden keine Benutzer gelöscht und die Admin-PIN wird auch nicht zurücksetzt.

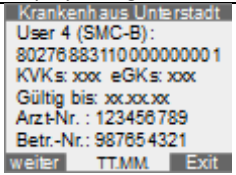
3.0: CTAPI Latenz
Falls das ZEMO VML-GK2 in einer Terminal-Server-Umgebung betrieben wird, kann es zu einer Verzögerung bei der Kommunikation zwischen Lesegerät und Terminal-Server kommen. Durch die Einstellung der CTAPI

Latenz auf „EIN“ wird eine Verzögerung (Latenz) bei der PC-Kommunikation aktiviert. Die Standard-Einstellung ist CTAPI Latenz „AUS“.

4: Status / Version (Selbstauskunft)

Es werden Ihnen verschiedene Statusinformationen angezeigt. Zwischen den einzelnen Status-Informationen können Sie mit den Pfeiltasten blättern.

Displayanzeige	Beschreibung
	Hersteller: ZEMOE Produkt: VML-GK2 Firmwareversion: 3.1.0 Hardwareversion: 2.0.0 Firmware-Gruppe: 4 Produkttyp: mobKT Produkttypversion: 1.3.0
	Serien-Nr. des Gerätes Anzahl gespeicherter Karten Gematik-Zulassungsnummer
	Zeigt die Anzahl angelegter Benutzer

Displayanzeige	Beschreibung
	Zeigt an, wie viele Karten für den jeweiligen Benutzer gespeichert sind, sowie das Ablaufdatum seiner „berechtigten Karte“

5: Benutzerverwaltung
Siehe Seite 24

6: Admin-PIN ändern
Siehe Seite 53

7: Gerät ausschalt.
Schaltet das VML-GK2 aus

8: CVC laden
Bei der Ausgabe einer neuen Kartengeneration könnte es zu einer Änderung der Root-CA kommen. Damit die Karten der bestehenden Root-CA und der neuen Root-CA sich gegenseitig authentifizieren können, sind Cross-CVCs notwendig. Diese könnten Sie über diesen Menüpunkt nachladen. Siehe auch S. 69

9: Update durchf.
Siehe S. 69

: Drucker-Update
Siehe S. 69

: Vers. Daten lösch.
Ermöglicht das Löschen aller im Gerät gespeicherten VSD. Stellen Sie sicher, dass sie alle Benutzer des Gerätes konsultiert haben, ob noch Daten benötigt werden, bevor Sie diese löschen!

: Werksreset
Setzt das Gerät auf den Auslieferungszustand zurück. Alle Benutzer und Daten werden gelöscht. Beachten Sie hierzu die Sicherheitshinweise aus dem Kapitel „Alternativer Werksreset“. Siehe Seite 77.

0: Eventliste
Zeigt die letzten 10 aufgetretenen Ereignisse mit Datum und Uhrzeit an. Die Fehlercodes finden Sie auf Seite 90.

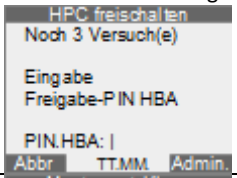
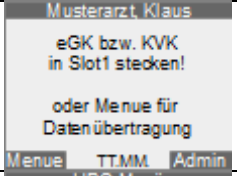
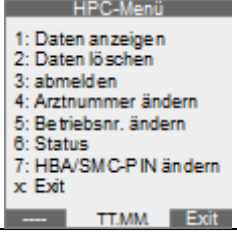
x: Exit Admin-Mode
Verlässt das Admin-Menü und „meldet“ den Admin vom Gerät ab. Der Admin-Autorisierungsstatus ist damit zurückgesetzt.

22) Benutzer-Menü

Aufruf des Benutzer-Menüs

Ausgangssituation:
- VML-GK2 ist ausgeschaltet
- es befinden sich keine Chipkarten im Gerät
- Der Benutzer ist bereits angelegt

Aktionen:

Displayanzeige	Aktion
Keine	„berechtigte Karte“ in Slot2 einlegen
Nach Art der berechigten Karte: 	SMC / HBA -PIN eingegeben OK-Taste drücken
	Funktionstaste1 drücken
	gewünschten Menüpunkt auswählen

Menüpunkte des Benutzermenüs:

- **1: Daten anzeigen**
  Dient zur Anzeige der gespeicherten Karten dieses Benutzers, sowie zur Übertragung der VSD zum PC
- **2: Daten löschen**:
  1: alte Quartale
  2: aktuelles Quartal
  3: alle Daten

x: zurück

- **3: abmelden**
  Hebt den Autorisierungszustand des Benutzers auf
- **4: Arztnummer ändern**
  Einstellen der Arztnummer für den Formularkopfdruck
- **5: Betriebsnr. ändern**
  Einstellen der Betriebsstättennr. für den Formularkopfdruck
- **6: Status**
  Anzeige der Anzahl gespeicherter eGKs u. KVKs, sowie das Gültigkeitsablaufdatum der „berechtigten Karte“
- **7: HBA/SMC-PIN ändern**
  Ändern der PIN der „berechtigten Karte“

23) Sicheres Firmware-Update

Ziel:
Sicherer Firmware-Download:
Durchführung einer Aktualisierung der gespeicherten Betriebssoftware oder der Konfigurationseinstellungen oder um das Gerät an geänderte Anforderungen anpassen zu können. Um zu garantieren, dass nur unveränderte Originalsoftware installiert wird, ist die Firmware digital signiert. Die Erstellung der Signatur erfolgt mittels des Hash-Algorithmus SHA-2 (256 Bit) und des asymmetrischen RSA Algorithmus unter Nutzung einer Schlüssellänge von 2048 Bits. Die Korrektheit der Update-Datei wird vom Gerät geprüft.

Nachfolgende Punkte können entweder einzeln oder gesamthaft durch ein Firmware-Update aktualisiert werden:

- **Firmware**
  Die Firmware ist die Betriebssoftware des Gerätes
- **Firmwaregruppen**

In den Firmwaregruppen befinden sich Informationen über zulässige Firmwareversionen auf die ein Up-/Down-Grade durchgeführt werden darf

- **Cross-CVS´s**
  Bei einer Änderung der Root-CA der eGKs oder der HBAs/SMC-Bs können für die C2C-Authentifizierung Cross-CVS notwendig werden. Diese können nachträglich in das Gerät geladen werden
- **Druckerkonfiguration**
  Änderung von Druckersteuerzeichen / Druckerkonfigurationen

Hinweis:
Bei einer Aktualisierung der Firmware im Gerät kann es sich um ein Update auf eine neuere Version, eine gleiche Version, sowie ein Downgrade auf eine ältere Version handeln.

Mögliche Konsequenzen im Falle eines Downgrades:

- Ein Downgrade kann dazu führen, dass nicht mehr alle derzeitigen Funktionalitäten des Gerätes zur Verfügung stehen
- Das Lesen der aktuellen Versichertenkarten könnte von einer älteren Firmware nicht unterstützt sein

Sicherheitshinweise:

- Der Admin stellt sicher, dass er die Begleitdokumentation zu der neuen Firmware vollständig liest und die darin befindlichen Hinweise beachtet.
- Der Admin stellt sicher, dass er das Kapitel „Sicherheitshinweise“ auf S. 10 vollständig gelesen hat und die Hinweise beachtet.
- Der Admin stellt sicher, dass alle Benutzer alle Versichertenkarten zum PC übertragen haben, da alle Daten bei einem Firmware-Update gelöscht werden!

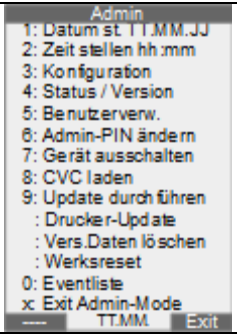
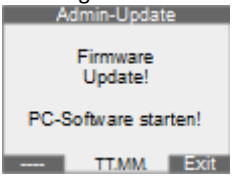
- Bei einem Update werden beim VML-GK2 die Grundeinstellungen geladen, die angelegten Benutzer gelöscht und die Transport-PIN aktiviert
- Der Admin stellt sicher, dass er nach dem Update umgehend eine neue Admin-PIN vergibt
- Nach dem Update (egal ob fehlerhaft oder nicht), startet das VML-GK2 nach einiger Zeit neu und führt einen Integritätscheck der Firmware durch. Stellt die Prüfroutine einen Fehler fest, wird angezeigt „Gerät fehlerhaft“. Diese Anzeige bleibt permanent, das Gerät muss zum Lieferanten / Hersteller eingesendet werden, ein weiterer Betrieb ist nicht mehr möglich
- Der Admin stellt sicher, dass alle Benutzer über ein durchgeführtes Firmware-Update umgehend informiert werden.
- Der Admin muss nach dem Update die Benutzer neu anlegen

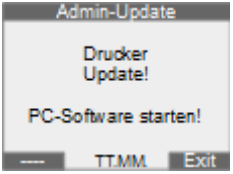
Voraussetzungen:

- Die Treiber-/Tools des VML-GK2 wurden auf dem PC installiert
- Sie verfügen über eine korrekte, von der gematik zugelassene Firmware-Datei
- Das VML-GK2 ist mit ihrem PC direkt per USB-Kabel verbunden

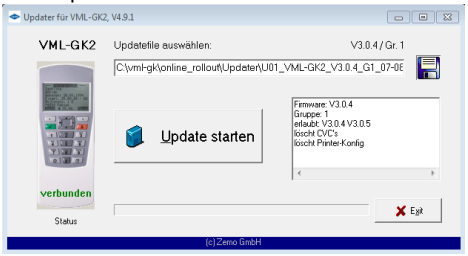
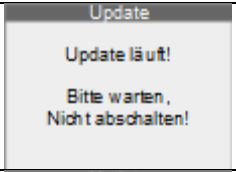
Aktionen für die Durchführung:

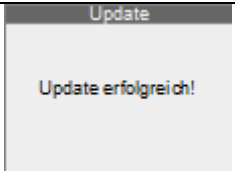
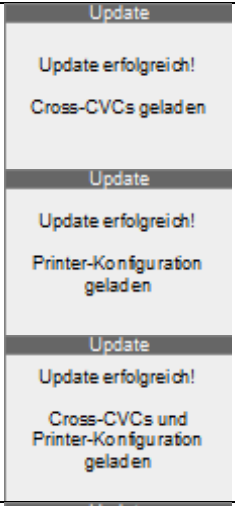
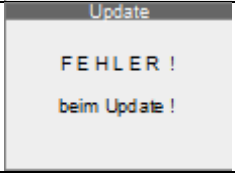
- Rufen Sie das Admin-Menü auf [siehe S. 60]

<table>
<tr>
<td> 
</td>
<td>Menüauswahl je nach Updatevariante treffen:
8: CVC laden
9: Update durchf.
: Drucker Update</td>
</tr>
<tr>
<td>Je nach Auswahl erscheint die folgende Meldung:
 

 
</td>
<td>Verbinden Sie das VML-GK2 mittels des mitgelieferten USB-Kabels mit dem PC.
Starten Sie den VML-Updater auf Ihrem PC (Start-Programme-ZEMO VML-Service)</td>
</tr>
</table>

VML-Updater am PC:  	• Wählen Sie die Update Datei aus. • „Update starten“ drücken • „Alle Daten werden gelöscht“ bestätigen • „Autorisierung, bitte Update-Passwort eingeben:“ (Dies haben Sie mit der Update Datei erhalten)
 	Das Gerät nicht ausschalten, solange „Update läuft“ angezeigt wird!
 	Nach dem Update startet das Gerät neu und führt einen Firmware-Test durch.

	Die Firmware wurde erfolgreich aktualisiert. Es wurde ein Werks-Reset durchgeführt
	Es wurde entweder Cross-CVC's oder Printer-Konfiguration geladen, oder beides zusammen aktualisiert.
	Das Update war nicht erfolgreich.

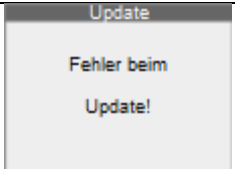
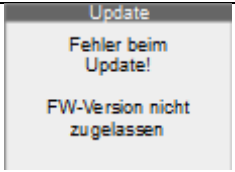
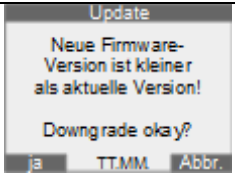
Aktionen nach dem erfolgreichen Update:

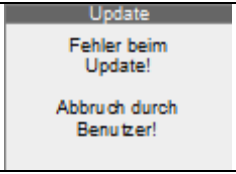
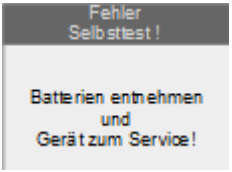
- Neue Admin-PIN vergeben [s. Seite 50]
- Prüfen, ob im Gerät die neue Software aktiviert ist:
  (Beim Einschalten des Gerätes wird beim Selbsttest die SW-Version

angezeigt. Vergleichen Sie diese mit der Software-Version der ihnen übersandten Firmware. Entspricht die Anzeige der neuen Softwareversion der Version der Update-Firmware, ist der Update-Prozess fehlerfrei verlaufen. Wird weiterhin die alte Software-Version angezeigt, wenden Sie sich bitte an Ihren Lieferanten/Hersteller.

- Benutzer neu anlegen [s. Seite 26]

Mögliche Fehlermeldungen beim Update:

Displayanzeige	Fehlerbeschreibung
	Tritt während dem Update-Ladevorgangs irgendein Fehler auf, wird das Update mit der Meldung „FEHLER beim Update!“ beendet. Diese Anzeige bleibt für ca. 6 Sekunden auf dem Display des VML-GK2 stehen, anschließend zieht das VML-GK2 einen Reset und aktiviert die alte Software.
	Die vorliegende FW-Version-Datei ist für ein Update des Gerätes nicht (mehr) zugelassen. Das Gerät befindet sich anschließend in einem Zustand wie vor dem Update, jedoch sind alle VSDs gelöscht.
	Die bereits im Gerät gespeicherte Firmware ist aktueller, als die Firmware die Sie einspielen möchten. Bitte prüfen Sie, ob ein Rückschritt auf eine ältere Version sinnvoll ist (Firmware-Hinweise beachten). Sie können durch Auswahl von „Abbr.“ den

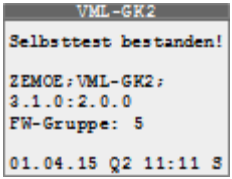
	Downgrade-Prozess an dieser Stelle abbrechen, oder mit „ja“ fortsetzen.
	Wenn Sie den „Downgrade“-Prozess abgebrochen haben, befindet sich das Lesegerät in einem Zustand wie vor dem Update, jedoch sind alle VSDs gelöscht.
	Nach dem Update (egal ob fehlerhaft oder nicht) startet das VML-GK2 nach einiger Zeit neu und führt einen Integritätscheck der Firmware durch. Stellt die Prüfroutine einen Fehler fest, wird angezeigt „Fehler Selbsttest“. Diese Anzeige bleibt permanent, das Gerät muss zum Lieferanten / Hersteller eingesendet werden, ein weiterer Betrieb ist nicht mehr möglich.

24) Selbsttest / Firmwareprüfung

Das Gerät führt bei jedem Einschalten einen kurzen Selbsttest durch. Wenn vom Gerät ein Spannungsverlust erkannt wurde, d.h. alle Pufferspeicher im Gerät sind sicher entladen, was nach spätestens 30 Sekunden Spannungsverlust der Fall ist, wird zusätzlich zu dem kurzen Selbsttest eine Prüfung der Integrität der Firmware (langer Selbsttest) durchgeführt.
Zur manuellen Prüfung der Integrität der Geräte-Firmware führen Sie bitte folgende Schritte aus:

1. Den Mini-USB-Stecker vom Gerät entfernen, falls verbunden.
2. Alle Chipkarten aus dem Gerät entfernen
3. Eine Batterie entfernen
4. Einschalttaste drücken
5. Batterie wieder einlegen

Nun wird die Firmware auf Integrität geprüft, im Display sehen Sie kurz die Meldung



Sollte die Prüfung einen Fehler ergeben, erscheint die Fehlermeldung: „Fehler Selbsttest“. In diesem Fall müssen Sie das Gerät zum Hersteller einschicken.

25) Alternativer Werksreset

Der „Alternative Werksreset“ bietet die Möglichkeit das VML-GK2 wieder auf den Auslieferungszustand zurückzusetzen, falls die Admin-PIN verloren gegangen ist. Der „Alternative Werksreset“ ist durch eine von Ihnen vergebene Werksreset-PUK oder mit der VML-Security-Card möglich. Die Voraussetzung für die Nutzung des „Alternativen

Werksreset“, ist dessen Aktivierung durch den Admin. Im Auslieferungszustand ist der „Alternative Werksreset“ deaktiviert. Bei der Erstbenutzung des VML-GK2 werden sie nach Vergabe der Admin-PIN gefragt, ob Sie die VML-Security-Card als Karte für den „Alternativen Werksreset“ verwenden möchten.

Aktivierung / Konfiguration des „Alternativen Werksreset“

Ziel:

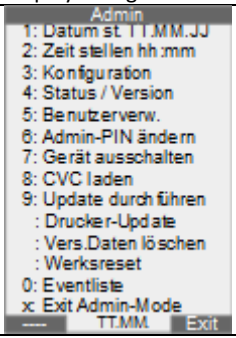
- Konfiguration des „Alternativen Werksreset“

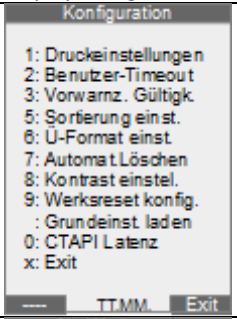
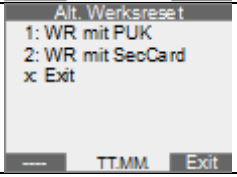
Ausgangssituation:

- Sie befinden sich im Admin-Menü [s. Seite 60]

So gelangen Sie zum Menüpunkt Werksreset konfigurieren:

- Folgende Schritte ausführen:

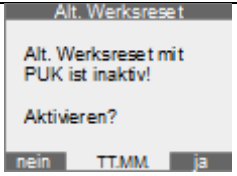
Displayanzeige	Tastatur-Eingabe
	3

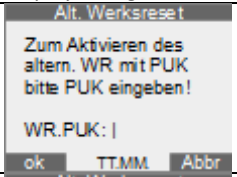
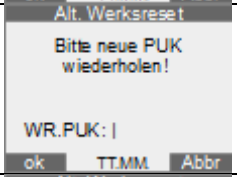
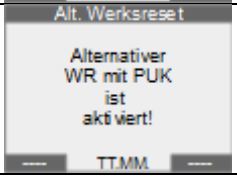
Displayanzeige	Tastatur-Eingabe
	9
	Bitte Menüpunkt auswählen

Je nach gewähltem Menüpunkt geht es wie folgt weiter:

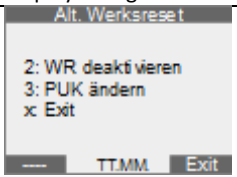
1: WR mit PUK konfigurieren:

- Bei inaktiver Werksreset-PUK:

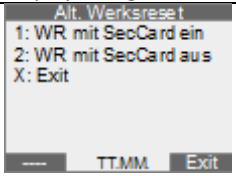
Displayanzeige	Tastatur-Eingabe
	Zum Aktivieren bitte Funktionstaste 2 Drücken

Displayanzeige	Tastatur-Eingabe
	Bitte vergeben Sie eine Werksreset-PUK (8-12 Ziffern)
	Werksreset-PUK Eingabe wiederholen
	

- Bei aktiver Werksreset-PUK:

Displayanzeige	Tastatur-Eingabe
	2 :für Deaktivieren der WR-PUK 3 :WR-PUK ändern X :Menü verlassen

2: WR mit VML-Security-Card konfigurieren:

Displayanzeige	Tastatur-Eingabe
	1: WR mit VML-Security-Card ein 2: WR mit VML-Security-Card aus

Alternativen Werksreset durchführen

Ziel:

- Rücksetzung des Gerätes auf den Auslieferungszustand (z.B. bei vergessener Admin-PIN)

Ausgangssituation:

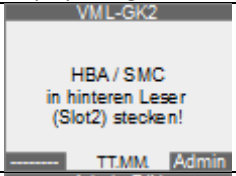
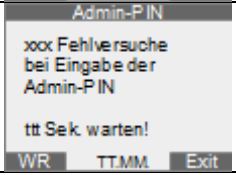
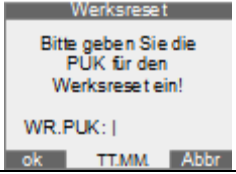
- VML-GK2 ist ausgeschaltet
- es befinden sich keine Chipkarten im Gerät
- die Admin-PIN ist bereits vergeben
- Sie haben bereits mindestens 3 x die Admin-Pin falsch eingegeben
- Der „alternative Werksreset“ ist mindestens für die VML-Security-Card oder die „PUK für Werksreset“ im Admin-Menü aktiviert

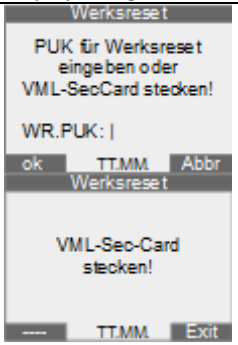
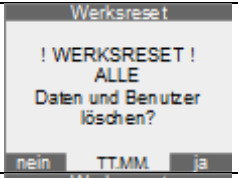
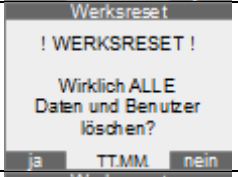
Sicherheitshinweise:

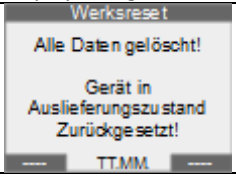
- Der Admin stellt sicher, dass er das Kapitel „Sicherheitshinweise“ auf S. 10 vollständig liest und die Hinweise beachtet.
- Bei einem Werksreset werden sämtliche im Gerät gespeicherten VSD gelöscht
- Alle angelegten Benutzer werden gelöscht
- Der Admin stellt sicher, dass die Benutzer über einen durchgeführten Werksreset umgehend informiert werden.

Aktion:

- Einschalttaste drücken
- Folgende Schritte ausführen:

Displayanzeige	Tastatur-Eingabe
	Funktionstaste „2“ drücken
	WR mittels Funktionstaste1 auswählen
Je nachdem welche Alternative Werksreset-Variante aktiviert wurde, kommt folgende Meldung: 	Je nach Meldung entweder PUK für Werksreset eingeben, oder die VML-Security-Card stecken

Displayanzeige	Tastatur-Eingabe
	
	Falls Werksreset gewünscht, „Ja“ mit Funktionstaste 2 auswählen
	Falls Werksreset gewünscht, „Ja“ mit Funktionstaste 1 auswählen
	

Displayanzeige	Tastatur-Eingabe
	

Aktionen nach dem Werksreset:

- Siehe Kapitel „Erste Schritte [s. S. 21]“

26) Manuelles Abschalten des VML-GK2

Das VML-GK2 kann wie folgt manuell abgeschaltet werden (ein evtl. autorisierter Modus wird durch das Abschalten sicher beendet):

- Drücken der Ausschalttaste für mehr als 1 Sekunde (und anschließendem Loslassen der Taste).
- Durch Betätigen der Funktionstaste, wenn diese mit „AUS“ belegt ist.
- Durch Auswahl der Funktion „Gerät ausschalten“ im Optionsmenü über die Cursor-Tasten (Pfeil-Hoch / Pfeil-Runter) nach Bestätigung durch die OK-Taste
- Entnahme der Batterien, wenn nicht über USB angeschlossen

27) Batteriebetrieb – Stromsparmodus

Das VML-GK2 ist als portables, stromsparendes Gerät entwickelt worden. Um einen Kompromiss zwischen langer Betriebsdauer und optimaler Benutzbarkeit zu gewährleisten, schaltet das VML-GK2 bei Inaktivität nach folgenden Zeiten ab:

Abschalten bei Batteriebetrieb:

- Halten der Ausschalttaste: sofort
- Mit Autorisierung (HPC freigeschaltet):

  Das VML-GK2 schaltet 10 Sekunden nach Ablauf der eingestellten Inaktivitätszeit ab. Folgende Events starten die Inaktivitätszeit neu:
  - Stecken / Ziehen einer eGK
  - Tastendruck
  - Übertragung von Daten (VSD)
- Ohne Autorisierung (HPC nicht freigeschaltet):

  Das VML-GK2 wartet 30 Sekunden auf die Eingabe der HPC-PIN, anschließend schaltet das Gerät nach kurzer Zeit aus.

Abschalten bei Betrieb über USB-Versorgung:

(die Batterie wird nicht belastet)
Betrieb am USB-Port: nach 45 Minuten

Die automatische Abschaltung des VML-GK2 setzt auch die autorisierten Modi für den Admin und den Benutzer zurück. D.h. nach dem Abschalten,

egal ob manuell oder automatisch, ist der autorisierte Modus gelöscht.

Die Hintergrundbeleuchtung der Anzeige verbraucht viel Strom und wird deswegen immer nur kurzzeitig eingeschaltet, kann aber jederzeit durch Drücken einer Taste (außer Einschalttaste) neu aktiviert werden. Bei Betrieb über USB-Versorgung ist die Hintergrundbeleuchtung permanent eingeschaltet.
Durch kurzes Drücken der Einschalttaste im Betrieb wird die Beleuchtung permanent (bis zum Abschalten) ein-/ausgeschaltet.

Batteriewechsel und Hinweise zu Batterien:

Das Batteriesymbol befindet sich bei eingeschaltetem Gerät in der untersten Zeile immer an der gleichen Stelle:

Batterie: leer

Batterie: voll

Auch bei leerer Batterie bleiben die gespeicherten Daten und Einstellungen erhalten.
Wenn im Display das Symbol „Batterie: leer“ angezeigt wird, wechseln Sie bitte die Batterien im Batteriefach auf der Rückseite unter Beachtung der korrekten Polarität (+ und – Pol). Verwenden Sie ausschließlich 1,5V Mignon AA Alkaline Batterien. Verwenden Sie keine wieder aufladbaren Batterien (Akkus) oder Longlife-Batterien. Bitte beachten Sie die Hinweise zur Entsorgung der alten Batterien auf Seite 93.

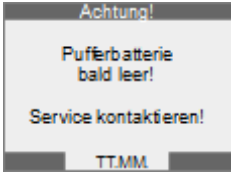
Sicherheitshinweise zu Batterien:

- Batterien können bei Verschlucken lebensgefährlich sein. Bewahren Sie deshalb die Batterien außerhalb der Reichweite von Kindern auf.
- Sollte eine Batterie ausgelaufen sein, vermeiden Sie den Kontakt mit Haut, Augen und Schleimhäuten. Die betroffenen Stellen sofort mit viel klarem Wasser spülen.
- Batterien dürfen nicht geladen, nicht auseinander genommen, ins Feuer geworfen oder kurzgeschlossen werden.
- Nehmen Sie die Batterien umgehend aus dem Gerät heraus, wenn sie erschöpft sind. So vermeiden Sie Schäden, die durch Auslaufen entstehen können.

Pufferbatterie

Der Datumsbaustein wird gemäß Gematik-Spezifikation zusätzlich durch eine Pufferbatterie gestützt. Falls die Hauptbatterien leer sind, wird der Datumsbaustein durch die interne Pufferbatterie mit Strom versorgt. Dadurch ist sichergestellt, dass bei einem Batteriewechsel oder für Überbrückungszeiten die interne Uhr bzw. das Datum korrekt weiterlaufen. Dies ist besonders wichtig, da das Einlesedatum der Versichertenkarte gemeinsam mit der Karte an das Primärsystem übertragen wird. Im Falle eines falsch eingestellten Datums ist es möglich, dass das Primärsystem die Karte ablehnt und einfach löscht.

Ca. 4 Wochen bevor die Pufferbatterie erschöpft ist, wird folgende Warnmeldung angezeigt:



Wenn diese Meldung angezeigt wird übertragen Sie alle gespeicherten Daten umgehend an ihr Primärsystem und senden Sie das Gerät zum Wechsel der Pufferbatterie an den Hersteller ein. Die Pufferbatterie kann nicht von Ihnen selbst gewechselt werden, da hierzu die BSI-Siegel vom Gerät entfernt werden müssen und das Gerät neu versiegelt werden muss. Dies ist notwendig um die BSI-Zertifizierung und Gematik-Zulassung aufrecht zu erhalten.

Wenn folgende Meldung angezeigt wird, können Sie aus Sicherheitsgründen das Gerät nicht mehr verwenden:

Senden sie in diesem Fall das Gerät umgehend zum Hersteller, da ansonsten die Gefahr besteht, dass die Pufferbatterie ausläuft und dadurch die Elektronik beschädigt wird. Ein Wechsel der Pufferbatterie vom Anwender ist aufgrund der Sicherheitsvorgaben nicht möglich. Daher lässt sich der Wechsel der Pufferbatterie mit Rücksetzung dieser Meldung und anschließender Neuversiegelung nur im Werk durchführen.

28) Event-/Fehlercodes

Event	Anzeigetext	Auslöser/Maßnahme
1002	Zeitüberschreitung (Timeout)	HPC-PIN schneller eingeben
1005	Kommunikationsfehler mit Karte	Kartenfehler
1006	Kartenapplikation ist deaktiviert	Kartenfehler
1007	Fehler beim Zugriff auf die Karte	evtl. Autorisierung HPC fehlt
1008	Kartenapplikation existiert nicht	Kartenfehler
1008	Objekt existiert nicht	Kartenfehler
1011	Fehler bei C2C-Authentisierung	Kartenfehler
1012	Korruptes Datenformat auf der Karte	Kartenfehler
1013	Abbruch durch den Benutzer	keine
1019	Kartenzugriff verweigert	evtl. Autorisierung HPC fehlt
1019	Zertifikat nicht lesbar	Kartenfehler
1024	Fehler bei der C2C-Authentisierung, Quellkarte	HPC nicht für eGK zugelassen
1025	Fehler bei der C2C-Authentisierung, Zielkarte	eGK nicht gültig für HPC
1028	Quellkarte für Card-to-Card fehlt	HPC fehlt
1060	PIN gesperrt oder Änderung erforderlich	HPC mit PUK freischalten
1060	PUK falsch oder gesperrt	PUK ist falsch
1061	PIN blockiert	HPC-PIN falsch
1061	PUK gesperrt	PUK ist falsch
1064	Neue PIN nicht identisch	Eingaben wiederholen
1065	Neue PIN zu kurz / zu lang	Falsche PIN Länge, Anleitung beachten
1070	Kryptografischer Algorithmus nicht unterstützt	Kartenfehler

1072	Korruptes Chiffrat bei symmetrischer Entschlüsselung	HPC neu anlegen oder defekt
1073	Korruptes Chiffrat bei asymetrischer Entschlüsselung	HPC neu anlegen oder defekt
1083	Rolle oid_versicherter stimmt nicht überein	eGK fehlerhaft
1084	Rolle oid_versichert. im X509 CA eGK nicht gefunden	eGK fehlerhaft
1088	Zertifikat ist zeitlich nicht gültig	eGK abgelaufen / ungültig
1120	Karte gesperrt	eGK fehlerhaft
1501	Karte ungültig	eGK fehlerhaft
3001	Daten inkonsistent	HPC neu anlegen oder Gerätefehler
3021	Daten inkonsistent (Prüfsumme falsch oder Daten korrupt)	HPC neu anlegen oder Gerätefehler
8001	Datum wurde gestellt	Das Datum wurde gestellt
8002	Auf Sommerzeit umgestellt	Wechsel von Winter- auf Sommerzeit
8003	Auf Winterzeit umgestellt	Wechsel von Sommer- auf Winterzeit
8004	Werksreset durchgeführt	Es wurde ein Werksreset durchgeführt
8005	Update durchgeführt	Es wurde ein Update durchgeführt
8006	Gespeicherter Key ist korrupt	HPC neu anlegen oder Gerätefehler
8007	Version HPC ist ungültig	Fehler HPC
8008	Version der eGK ist ungültig	Fehler eGK
8009	CVCs wurden geladen	Update der CVC´s wurde durchgeführt

8010	Druckerkonfiguration wurde geladen	Update der Druckerkonfiguration wurde durchgeführt
8011	Update-/Ladefehler	Fehler beim Update

29) Reinigung / Pflege / Desinfektion

Reinigen Sie das Kartenterminal nur mit einem weichen, leicht feuchten Tuch.
Durch die Reinigung mit einem trockenen Tuch kann das Kunststoffgehäuse elektrostatisch aufgeladen werden. Putz- und Scheuermittel, sowie lösungsmittelhaltige Stoffe dürfen für die Reinigung nicht verwendet werden.

Desinfektionsmittel dürfen nicht direkt auf das Gerät gesprüht/gespritzt werden, es kann sonst Flüssigkeit in das Gerät gelangen und dieses zerstören. Verwenden Sie deshalb leicht feuchte Desinfektionstücher. Die Siegel und die Bedruckung können eventuell empfindlich auf zu intensiven Kontakt mit chemischen Flüssigkeiten reagieren, was im Laufe der Zeit zum Ablösen bzw. zur Zerstörung der Siegel führen kann.

30) Außerbetriebnahme

Das ZEMO VML-GK2 ist ein sicherheitsrelevanter Bestandteil der Telematikinfrastruktur im Gesundheitswesen. Bei der Außerbetriebnahme müssen Sie folgende Sicherheitshinweise beachten:

Sicherheitshinweise:

- Übertragen Sie alle noch im Gerät gespeicherten Versichertenkarten zu Ihrem Primärsystem (S. 40)
- Führen Sie einen „Werksreset“ durch (S. 81)
  Anmerkung: Hierbei werden alle Benutzer, gespeicherten Daten gelöscht, sowie die Admin-PIN und die Parameter auf den Auslieferungszustand gesetzt.
- Wenn Sie das Gerät endgültig außer Betrieb setzten, müssen Sie die BSI-Siegel von den Stirnseiten des Gerätes (Siegel siehe S.15) entfernen, bevor Sie das Gerät entsorgen.

Hinweise zur Entsorgung:

Zur Vermeidung von Umweltbelastungen darf das ZEMO VML-GK2 nicht über den Hausmüll entsorgt werden, sondern muss einer gesetzeskonformen Entsorgung/Verwertung zugeführt werden.
Nehmen Sie hierzu bitte Kontakt zu Ihrem Zulieferanten oder direkt zu einem zertifizierten Entsorgungsunternehmen auf.

- Da es sich bei dem ZEMO-Lesegerät im Sinne des Elektro- und Elektronikgerätegesetzes (ElektroG) um ein professionell genutztes Gerät handelt, ist die Entsorgung über kommunale Sammelstellen nicht zulässig.
- Entsorgung der Batterien:
  Verbrauchte Batterien gehören nicht in den Hausmüll! Entsorgen Sie diese über Ihren Elektrofachhändler oder Ihre öffentliche Wertstoff-Sammelstelle. Als Verbraucher sind sie gesetzlich verpflichtet, gebrauchte Batterien ordnungsgemäß zu entsorgen. Batterien dürfen nicht geladen, nicht auseinander genommen, ins Feuer geworfen oder kurzgeschlossen werden.

31) Konformitätserklärung

CE EG-KONFORMITÄTSERKLÄRUNG
DECLARATION OF EG-CONFORMITY

Wir/We

ZEMO GmbH
Franz-Mader-Str. 9, 94036 Passau

erklären in alleiniger Verantwortung, daß das Produkt,
declare under our sole responsibility that the product,

Chipkartenleser: ZEMO VML-GK2 v 3.1.0
(Bezeichnung, name)

auf das sich diese Erklärung bezieht, mit der/den folgenden Norm(en) oder normativen Dokument(en) übereinstimmt.
to which this declaration relates is in conformity with the following standard(s) or other normative document(s)

EN 50021 - Störaussendung
EN 50024 - Störfestigkeit

Titel und Nummer sowie Ausgabedatum der Norm(en)
Title and number and date of issue of the standard(s)

gemäß den Bestimmungen der Richtlinie
following of the provisions of directive

89 / 336 / EWG
93 / 44 / EWG **Amtsblatt der EG Nr. L 139 S. 19**

Passau, 19.03.2018
Ort, Datum der Ausstellung
place and date of issue

Ralf Saohling
Name + Untersohrift des Befugten
name and signature of authorized person

32) Signatur der Anleitung

Die elektronische Form dieser Anleitung (PDF) ist mit einer digitalen Signatur gemäß Signaturgesetz versehen.
Aussteller der Signatur ist: Ralf Sachling, ZEMO GmbH, 94036 Passau.

Die Echtheit der digitalen Signatur können Sie mit einer dafür vorgesehenen Software oder auch im Internet z.B. auf nachfolgender Website prüfen: www.signature-check.de

signiert
von: Ralf Sachling
am: 18.04.2018
um: 17:19:54 +02
ZEMO GmbH, Passau