

Kartenleser HOST Anbindung

Liebes Praxis-Team,

wir möchten Ihnen die Nutzung des **KV-Vertragsportals** so einfach wie möglich machen. Damit Sie bei einer Einschreibung die Stammdaten Ihres Patienten nicht manuell im Portal eingeben müssen, können Sie die Daten auch über die eGK und Ihr Kartenterminal einlesen. Dafür ist die Installation einer externen Komponente/Kartenleser Host Anwendung notwendig.

Die Installation ist auf jedem Rechner erforderlich, der ein Kartenlesegerät nutzt und auf das KV-Vertragsportal zugreifen möchte.

Wir empfehlen Ihnen diese Installation zusammen mit Ihrem IT-Support durchzuführen.

Bitte folgen Sie der beigefügten Anleitung in den folgenden Schritten:

Schritt 1: Installation der Komponente

Schritt 2: Einstellung des Kartenlesegeräts

Schritt 3: Überprüfung - Karte testweise auslesen

Schritt 4: SSL-Verschlüsselung für Ihren Browser einrichten (nicht immer notwendig)

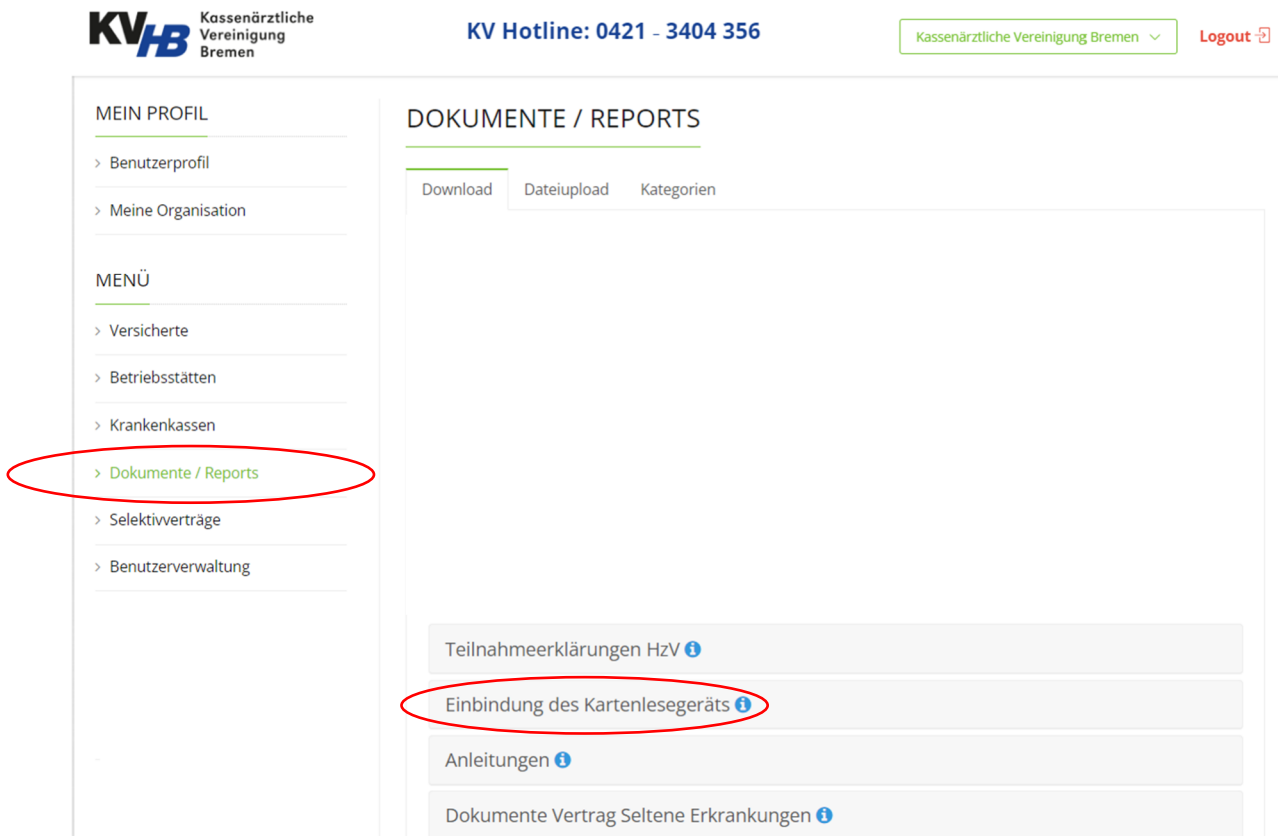
Die technischen Voraussetzungen, die Sie benötigen:

1. Windows-Betriebssystem
 - Windows 7 (x64, x86)
 - Windows 8.1 (x64, x86)
 - Windows 10 (x64, x86)
 - Windows 11
2. Browser
 - Mozilla Firefox
 - Microsoft Edge
 - Google Chrome

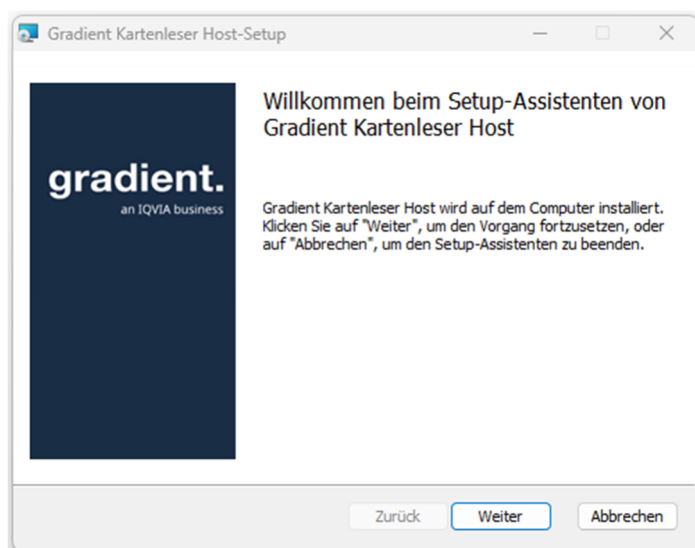
Der Microsoft Internet Explorer wird nicht unterstützt. Bitte nutzen Sie im Zusammenhang mit dem Kartenleser Host einen der unterstützten Browser und stellen Sie sicher, dass dieser auf einem aktuellen Stand ist.

Schritt 1: Installation der Komponente

Bitte laden Sie die Datei **Kartenleser Host Setup** aus dem Downloadbereich des KVHB-Vertragsportals runter.



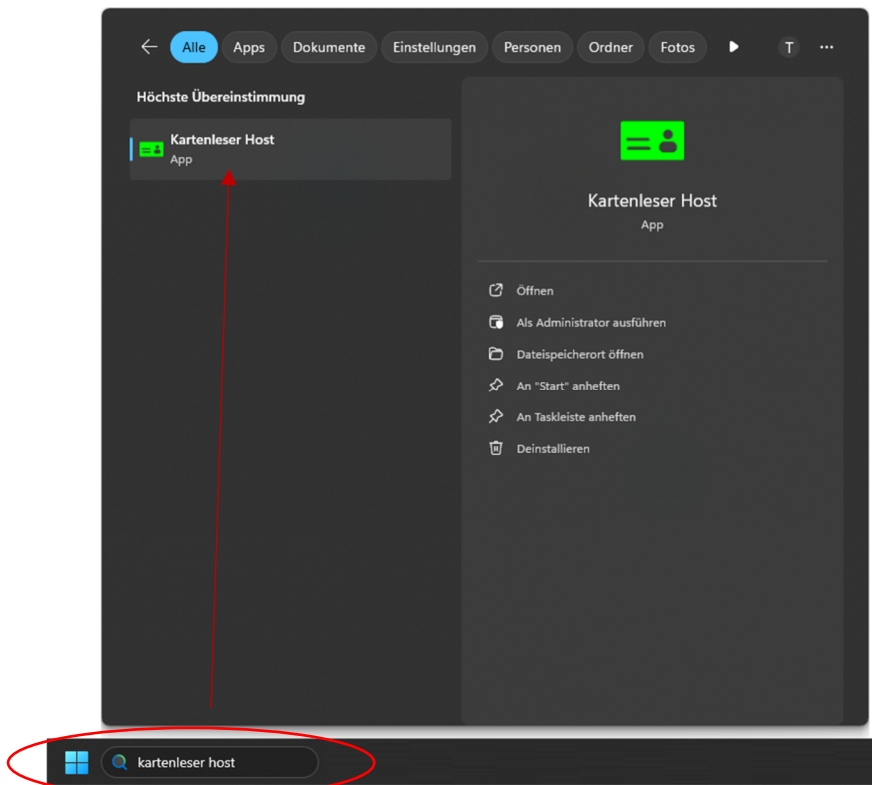
Starten Sie das Kartenleser Host Installationsprogramm und folgen Sie der Installationsanweisung.



Nach der Installation wird empfohlen Windows neu zu starten. Der Kartenleser Host wird automatisch mit jedem Start des Betriebssystems ausgeführt.

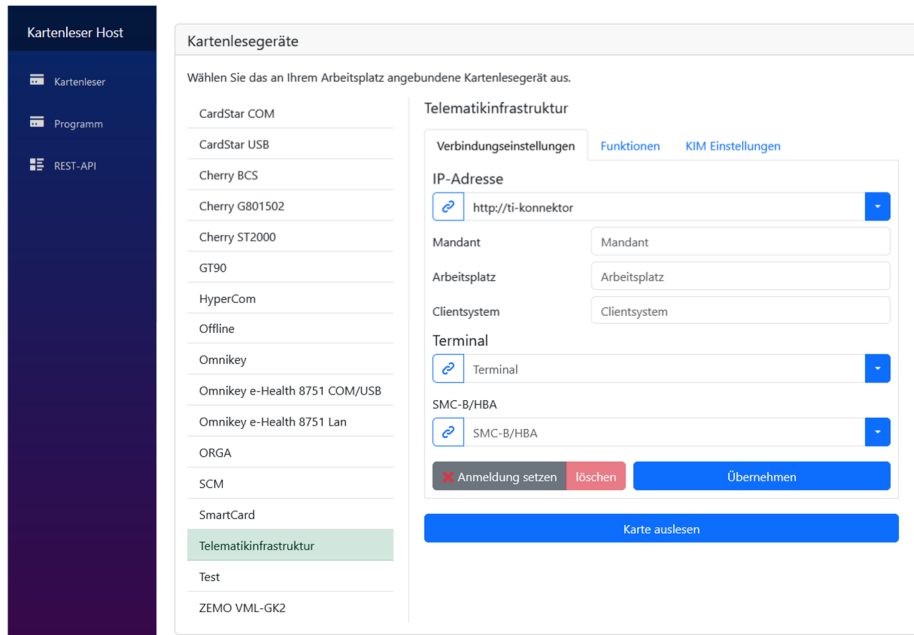
Anwendung starten

Um die Anwendung nach der Installation zu starten, geben Sie in der Programmsuchleiste folgendes ein **Kartenleser Host**.



Danach finden Sie das Programm auch in der Taskleiste.

Mit einem Klick auf folgendes Symbol  öffnet sich der Standardbrowser mit der folgenden Adresse: <https://localhost:8832/> und in der angezeigten Oberfläche können Sie nun die Einstellungen des Kartenlesegeräts konfigurieren.



Hier könnte unter Umständen Schritt 4 notwendig sein, falls Sie einen Warnhinweis erhalten.

Schritt 2: Einstellung des Kartenlesegeräts

Bitte halten Sie zur Anbindung des Kartenlesegeräts folgende Informationen bereit:

1. IP-Adresse des Konnektors
2. Mandanten-ID
3. Arbeitsplatz (das ist der Rechner, der mit dem Kartenlesegerät verbunden ist)
4. Clientsystem (das ist Ihr PVS System)
5. Zertifikat vom Clientsystem und das dazugehörige Passwort

Es ist notwendig, dass Sie einmalig die Einstellung zur Einbindung des Kartenlesegeräts vornehmen. Bei der Einbindung des Kartenlesegeräts gibt es 2 Varianten. Diese sind von der technischen Situation in Ihrer Praxis abhängig:

Variante 1:

Das Kartenlesegerät ist per LAN mit dem TI-Konnektor verbunden: Um die TI zu konfigurieren, wählen Sie als Kartenlesegerät die **Telematikinfrastruktur** aus.

Kartenlesegeräte

Wählen Sie das an Ihrem Arbeitsplatz angebundene Kartenlesegerät aus.

- CardStar COM
- CardStar USB
- Cherry BCS
- Cherry G801502
- Cherry ST2000
- GT90
- HyperCom
- Offline
- Omnikey
- Omnikey e-Health 8751 COM/USB
- Omnikey e-Health 8751 Lan
- ORGA
- SCM
- SmartCard
- Telematikinfrastruktur**
- Test
- ZEMO VML-GK2

Telematikinfrastruktur

Verbindungseinstellungen
Funktionen
KIM Einstellungen

IP-Adresse

[⌋](#) http://ti-konnektor [⌵](#)

Mandant

Arbeitsplatz

Clientsystem

Terminal

[⌋](#) Terminal [⌵](#)

SMC-B/HBA

[⌋](#) SMC-B/HBA [⌵](#)

Anmeldung setzen
löschen
Übernehmen

Karte auslesen

1. Verbindungseinstellungen:

- Geben Sie zunächst die **IP-Adresse** Ihres TI-Konnektors an.
- Als nächstes folgt die **Mandanten-ID**. Dies kann z.B. Ihre Betriebsstätten Nummer sein.
- Bei **Arbeitsplatz** geben Sie den Namen Ihres Praxisrechners ein, an dem Sie die Installation vornehmen. Dieser kann auch in der Praxisverwaltungssoftware stehen.
- Hier geben Sie den Namen Ihres **Clientsystem** an.

Nachdem Sie die Daten eingetragen haben, können Sie überprüfen, ob die Verbindung zum Konnektor hergestellt werden kann. Dafür klicken Sie auf das

Symbol [⌋](#).

Wenn im Anschluss dieses Symbol [✅](#) erscheint, konnte die Verbindung erfolgreich hergestellt werden. Erscheint jedoch dieses Symbol [❌](#), überprüfen Sie Ihre Angaben und versuchen es erneut.

2. Terminal:

Sind alle Verbindungseinstellungen korrekt getätigt, kann über die Terminalauswahl das entsprechende Kartenlesegerät und über SMC-B/HBA die passende Kartennummer ausgewählt werden. Mit Klick auf das Symbol [⌵](#) können Sie die verfügbaren Terminals und SMC-B/HBA sehen, die im TI-Konnektor

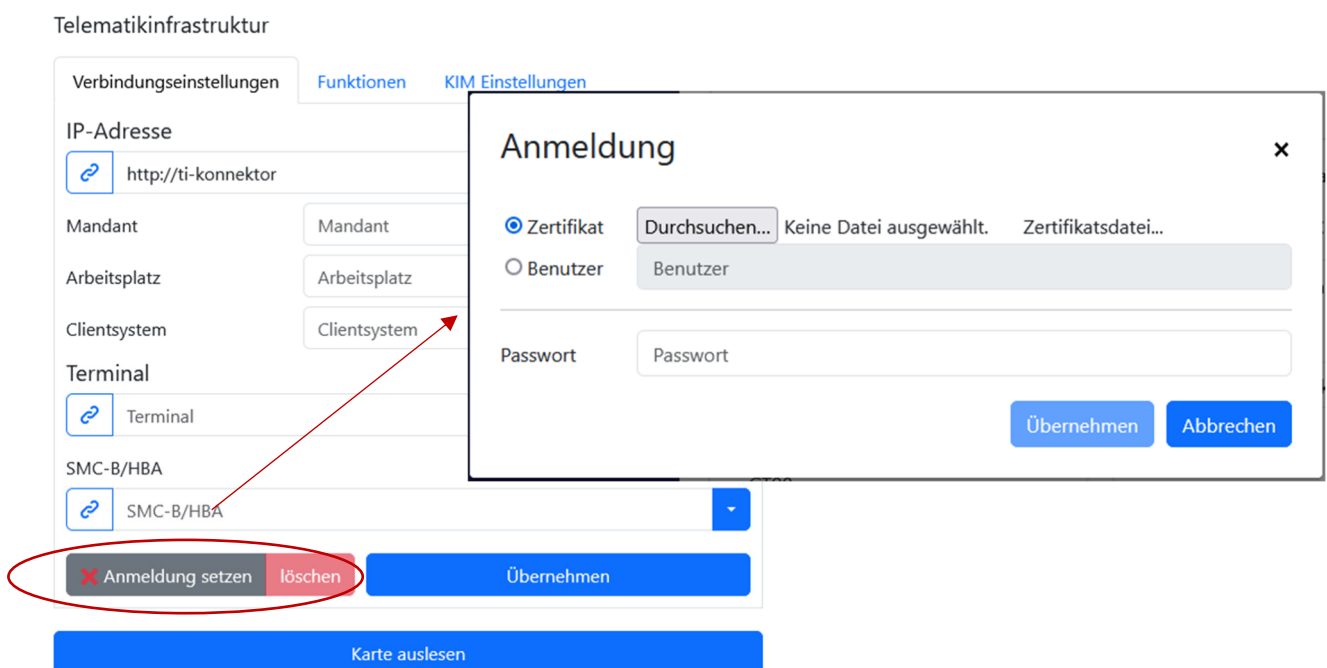
für den zuvor eingetragenen Arbeitsplatz eingerichtet sind.

Wenn Sie eine Auswahl getroffen haben, kann diese mit einem Klick auf  überprüft werden. Wenn im Anschluss dieses Symbol  erscheint, konnte die Verbindung erfolgreich hergestellt werden. Erscheint jedoch dieses Symbol , überprüfen Sie Ihre Angaben und versuchen Sie es erneut.

3. Zertifikat:

Ob Ihr Zertifikat verschlüsselt ist, können Sie in der TI-Konnektor Konfiguration einsehen.

Sollten die Kartenleser Dienste per Zertifikat verschlüsselt sein, müssen Sie diese Verschlüsselung konfigurieren. Hierzu klicken Sie auf **Anmeldung setzen** und es öffnet sich ein Pop-up Fenster. In der Oberfläche können Sie die Art der Verschlüsselung zwischen **Zertifikat** oder **Benutzer** auswählen.



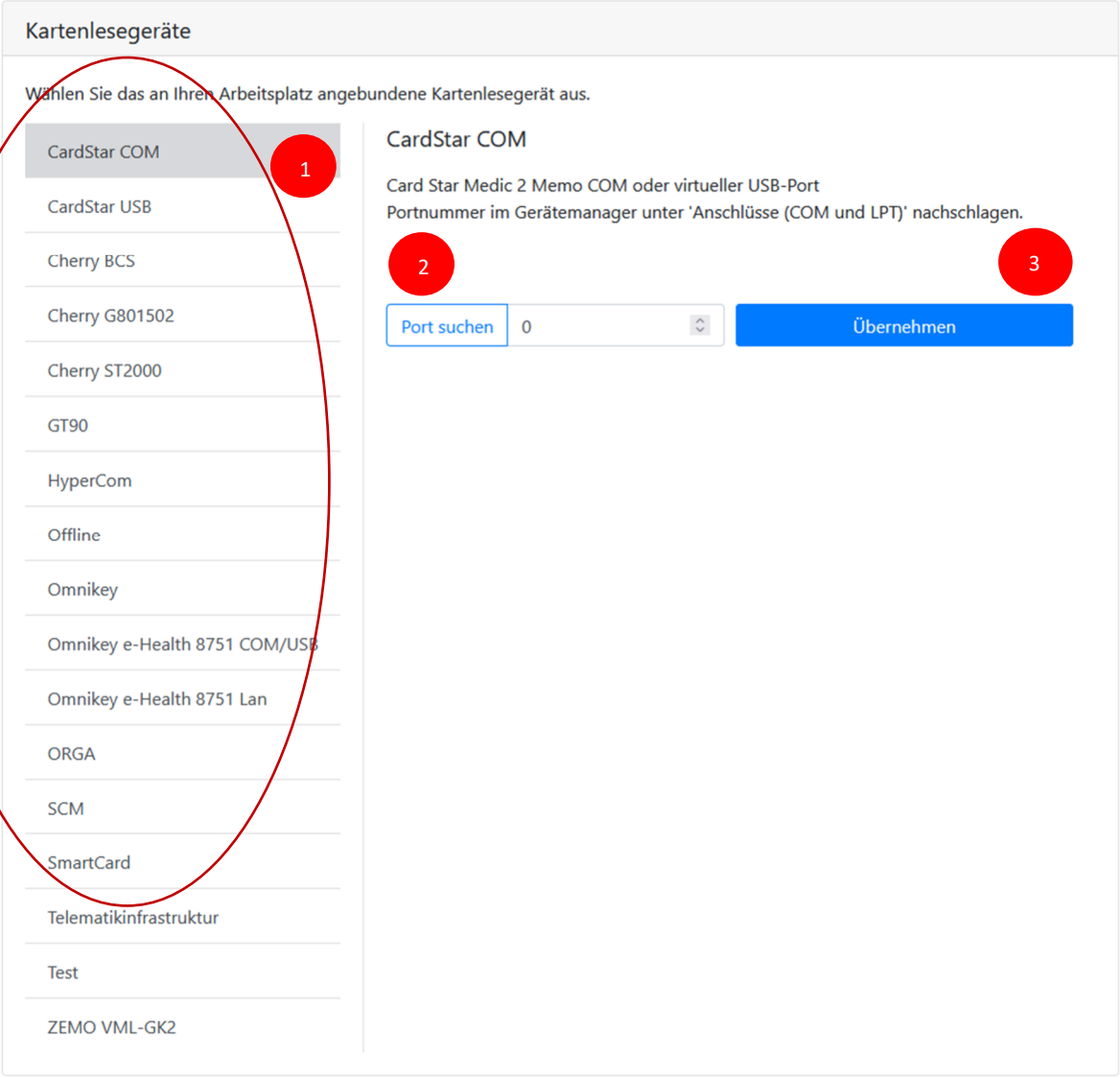
Die Verschlüsselung des Zertifikats kann auf unterschiedliche Weise konfiguriert sein:

1. **Verschlüsselung per Zertifikat:** Generieren Sie im TI-Konnektor das Zertifikat. Laden Sie dieses herunter, wählen es über die Zertifikatsdatei aus und geben das zugehörige Passwort an.
2. **Verschlüsselung per Benutzername und Passwort:** Geben Sie den Benutzernamen und das Passwort der Verschlüsselung an. Diese Angaben wurden bei der Installation des TI-Konnektors vergeben und sollten Ihnen ausgehändigt worden sein.

4. Mit Klick auf **Übernehmen** werden die Einstellungen gespeichert.

Variante 2:

Das Kartenlesegerät ist seriell mit dem PC (über USB) verbunden.



Kartenlesegeräte

Wählen Sie das an Ihrem Arbeitsplatz angebundene Kartenlesegerät aus.

- CardStar COM **1**
- CardStar USB
- Cherry BCS
- Cherry G801502
- Cherry ST2000
- GT90
- HyperCom
- Offline
- Omnikey
- Omnikey e-Health 8751 COM/USB
- Omnikey e-Health 8751 Lan
- ORGA
- SCM
- SmartCard
- Telematikinfrastruktur
- Test
- ZEMO VML-GK2

CardStar COM

Card Star Medic 2 Memo COM oder virtueller USB-Port
Portnummer im Gerätemanager unter 'Anschlüsse (COM und LPT)' nachschlagen.

2 Port suchen 0 **3** Übernehmen

1. Hier kann das Seriell über USB oder COM angebundene Kartenlesegerät gewählt werden.
2. Im Falle eines Seriellen Kartenlesegeräts kann hier der Port manuell oder automatisch über Port suchen eingestellt werden.
3. Mit **Übernehmen** wird dann das eingestellte Kartenlesegerät mit dem entsprechenden Port gespeichert.

Schritt 3: Karte testweise auslesen

Nach der erfolgreichen Konfiguration des Kartenlesegeräts über eine der oben beschriebenen Varianten, kann abschließend **Testweise** eine Karte ausgelesen werden.

Kartenlesegeräte
 Wählen Sie das an Ihrem Arbeitsplatz angebundene Kartenlesegerät aus.

- CardStar COM
- CardStar USB
- Cherry BCS
- Cherry G801502
- Cherry ST2000
- GT90
- HyperCom
- Offline
- Omnikkey
- Omnikkey e-Health 8751 COM/USB
- Omnikkey e-Health 8751 Lan
- ORGA
- SCM
- SmartCard
- Telematikinfrastruktur**
- Test
- ZEMO VML-GK2

Telematikinfrastruktur
 Verbindungseinstellungen Funktionen KIM Einstellungen
 IP-Adresse

 Mandant
 Arbeitsplatz
 Clientsystem
 Terminal

 SMC-B/HBA

Die Installation war erfolgreich, wenn sich bei Klick auf **Karte auslesen** folgende Maske mit den ausgelesenen Stammdaten öffnet:

Versichertendaten
×
 Kartenlesegerät: Cherry BCS

Krankenkasse bzw. Kostenträger

WOP

Name, Vorname des Versicherten

geb.am.

VK gültig bis

Kassen-Nr.

Versicherten-Nr.

Art

Gruppe

DMP

CDM-Version

Typ

Zulassungsnr.

Einlesedatum

Schritt 4: SSL-Verschlüsselung für Ihren Browser einrichten (nicht immer notwendig)

Warum kann es sein, dass das Zertifikat für „localhost“ als unsicher eingestuft wird?

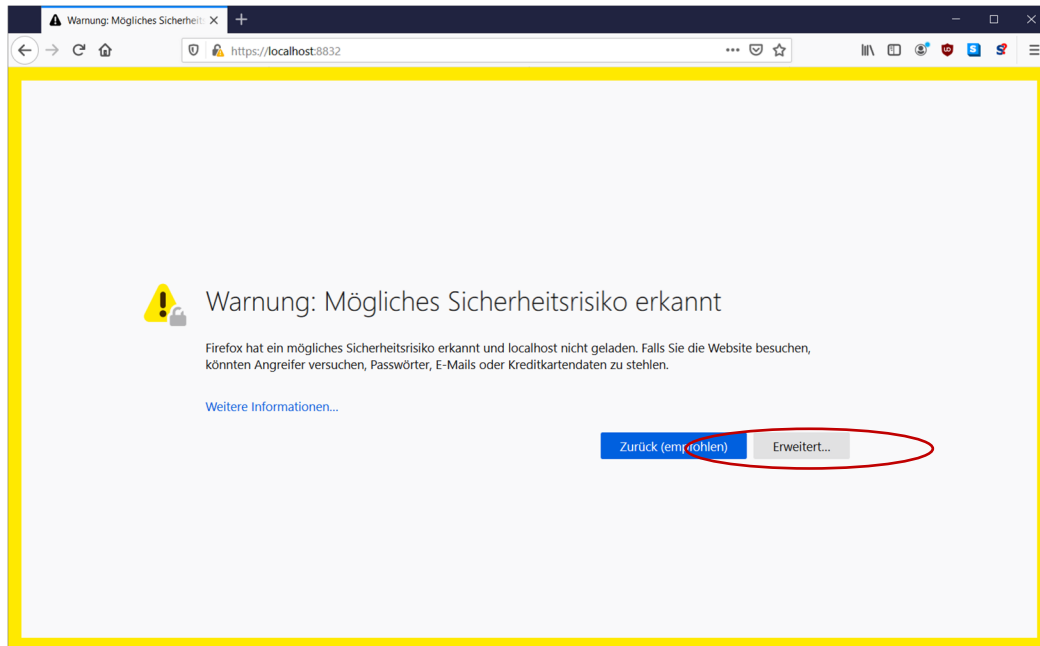
Damit ein Zertifikat allgemein als vertrauenswürdig angesehen wird, muss es von einer (vertrauenswürdigen) Zertifizierungsstelle ausgestellt worden sein. Da der Kartenleser Host auf einem Arbeitsplatzrechner läuft und von diesem aus aufgerufen wird, benötigt man ein Zertifikat für die Domain "localhost". Für diese Domain stellt allerdings keine Zertifizierungsstelle ein Zertifikat aus, da es keinen Inhaber dieser Domain gibt. Damit ist ein Zertifikat für "localhost" per se nicht vertrauenswürdig und erst einmal "unsicher". Ein Benutzer/Administrator muss explizit erklären, dass er dem Zertifikat vertraut. Dies erfolgt in Firefox dadurch, dass der Benutzer beim ersten Aufruf der Seite angibt, dass er dem Zertifikat vertraut. Für andere Browser wird das Problem dadurch gelöst, dass bei der Installation des Kartenleser Hosts das Zertifikat für "localhost" in den Zertifikatsspeicher von Windows importiert wird. Der Hinweis darauf, dass ein "localhost"-Zertifikat nicht vertrauenswürdig ist, ist an sich sinnvoll und vergleichbar mit Warnhinweisen, die man z. B. erhält, wenn man Anwendungen installiert, deren Quelle Windows nicht als vertrauenswürdig einstufen kann.

Es kann sein, dass Sie nach dem Starten des Kartenleser Hosts, die SSL Verschlüsselung für Ihren Browser einrichten müssen. Dies passiert dann bereits nach Schritt 1:

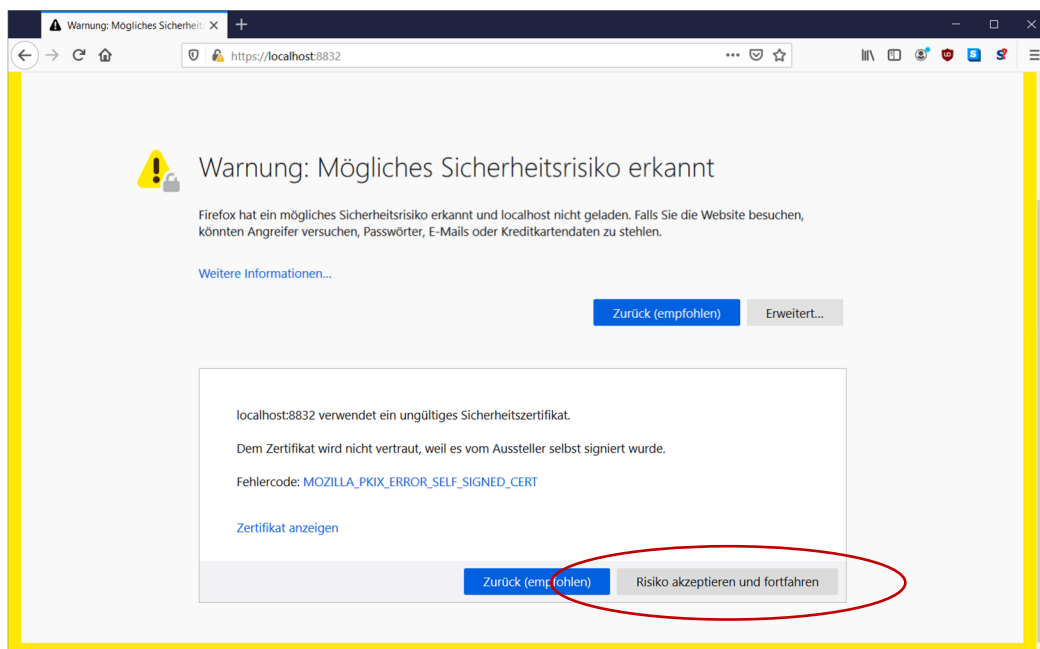
Im Folgenden wird die Einrichtung der SSL-Verschlüsselung anhand des Browsers Mozilla Firefox beispielhaft erklärt. Die Einrichtung kann auch, je nach Einstellung, in anderen Browsern vorkommen und wird oft ähnlich eingerichtet.

Der Kartenleser-Host verwendet für die Verschlüsselung der Kommunikation mit SSL ein selbstsigniertes Zertifikat. Dieses Zertifikat ist für den lokalen Arbeitsplatzrechner ("localhost") ausgestellt. Mozilla Firefox stuft selbstsignierte Zertifikate grundsätzlich als mögliches Sicherheitsrisiko ein. Daher muss ein solches Zertifikat in Firefox als Ausnahme hinzugefügt werden, bevor der Kartenleser-Host in Kombination mit Firefox genutzt werden kann.

Hierzu rufen Sie im Firefox die Adresse <https://localhost:8832/> auf. Es erscheint ein Warnhinweis, dass ein mögliches Sicherheitsrisiko erkannt wurde:



Anschließend klicken Sie auf **Erweitert...** und es erscheint ein Bereich mit weiteren Details:



Klicken Sie auf **Risiko akzeptieren und fortfahren**. Hiernach wurde das Zertifikat als Ausnahme hinzugefügt. Es erscheint die Konfigurationsseite des Kartenleser-Hosts. Anhand des Schlosssymbols mit dem gelben Warndreieck können Sie sehen, dass das Zertifikat erfolgreich als Ausnahme hinzugefügt wurde und die Kommunikation mit SSL-Verschlüsselung erfolgt:

