Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation eHealth-CardLink (eH-CL)

Version:	1.0.0
Revision:	867472
Stand:	19.03.2024
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_eHealth-CardLink

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	19.03.2024		Initiale Erstellung	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die gematik möchte mobile Online-Einsatzszenarien in der TI ermöglichen. Es wird eine Lösung von der gematik spezifiziert und zugelassen, die es Versicherten ermöglicht, mit der eGK ohne PIN mit einer Leistungserbringerinstitution (LEI) zu interagieren und einen VSDM-Prüfungsnachweis auszustellen. Dabei verwenden Versicherte oder ihre Vertreter sogenannte Clients des Nutzers; das sind eigene Smartgeräte mit Kartenleser und Internetzugang (beispielsweise ein Smartphone).
Der Produkttyp eHealth-CardLink (eH-CL) stellt eine sichere Verbindung zwischen einem Client des Nutzers und einem Konnektor her und fungiert als ein Gateway, der diese zwei Komponenten mit ihren unterschiedlichen Übertragungsprotokollen miteinander verbindet.

Die vorliegende Spezifikation definiert die Anforderungen zu Funktion, Test und Betrieb des eH-CL.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von eH-CL Lösungen sowie Hersteller von Produkttypen, die hierzu eine Schnittstelle besitzen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekanntgegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

In diesem Dokument werden die von dem Produkttyp eH-CL bereitgestellten (angebotenen) Schnittstellen „IF Karten-Interpreter“ und „IF Konnektor-Interpreter“ spezifiziert. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang 10).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief und im Anbietertypsteckbrief des Produkttyps eH-CL verzeichnet.

Nicht Bestandteil sind die Prozesse zu den Fachdiensten VSDM und E-Rezept.

1.5 Methodik

Anwendungsfälle und Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID,
Anforderungen zusätzlich durch die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen.“ verwendet. Die Schlüsselworte werden außerdem um Pronomen in Großbuchstaben ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anforderungen werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

Dabei umfasst die Anforderung sämtliche zwischen ID und Textmarke [<=] angeführten Inhalte.

In diesem Dokument werden auch Anforderungen aus dem Dokument Spezifikation eHealth-Kartenterminal [gemSpec_KT] referenziert. **Diese Anforderungen gelten sowohl für das eHealth-Kartenterminal als auch für das eHealth-CardLink.** Anforderungen, die sich nur auf die eHealth-CardLink beziehen, werden im Titel der Anforderungen mit eHealth-CardLink bezeichnet.

2 Anwendungskontext

Der Produkttyp eHealth-CardLink ermöglicht mobile TI-Szenarien mit einer eGK ohne die Nutzung der dazugehörigen PIN. Die Kernaufgabe des eH-CL ist die Vermittlung zwischen der eGK des Versicherten und dem Konnektor einer Leistungserbringerinstitution zur Erstellung eines VSDM-Prüfnachweises „VSDM+“. Dieser Prüfnachweis dient zur Autorisierung von Leistungserbringerinstitutionen an TI-Fachdiensten.

2.1 Anwendungsszenario: Mobiles Erstellen eines VSDM-Prüfungsnachweises mit eGK ohne PIN

Der Patient erzeugt mit seiner eGK und Smartphone über den eH-CL einen VSDM-Prüfungsnachweis, der von der angeschlossenen LEI verwendet werden kann, um E-Rezepte des Patienten vom Fachdienst abzurufen.
Die Apotheke bzw. der Apotheker kann dem Patienten anschließend alle aus seiner Sicht zum Zweck der Beratung und Verkauf erforderlichen Informationen beispielsweise über eine Applikation zur Verfügung stellen. Sofern der Nutzer der eGK eine kontaktlose Schnittstelle zum Einlesen seiner Karte verwendet, ist die Eingabe der auf der Karte aufgedruckten CAN erforderlich.

2.1.1 Ablauf mit eHealth-CardLink

Voraussetzung:
Der Versicherte hat eine Applikation (App) auf seinem Smartphone installiert und ist technisch in der Lage, seine eGK mittels kontaktloser Kommunikation zu verwenden.
Die App stellt für diesen Anwendungsfall via eHealth-CardLink eine Verbindung zur einer LEI bereit.

Ablauf:

1. Der Versicherte „Nutzer“ startet die App und hält seine eGK an sein NFC-fähiges Smartphone ("Client des Nutzers").
   Damit übergibt der Versicherte seine eGK an die über die App und den eH-CL angebundene LEI und autorisiert diese damit für den nachfolgenden Ablauf zum VSDM-Prüfungsnachweis.
2. Die für den Prüfablauf relevanten Daten der eGK werden von der App an den eHealth-CardLink übermittelt.
3. Das Primärsystem (PS) ruft die Operation ReadVSD am Konnektor auf.
4. Das Fachmodul VSDM startet die Onlineprüfung und Gültigkeitsprüfung der eGK.
5. Der Fachdienst VSDM (UFS oder VSDD) verwendet als fachliche Information für die Prüfziffer u.a. die KVNR und den aktuellen Zeitpunkt als Zeitstempel. Es wird mit dem betreiberspezifischen Geheimnis ein Hashwert über die fachlichen Informationen gebildet. Die fachlichen Informationen bilden zusammen mit dem Hashwert die Prüfziffer.
6. Das Fachmodul VSDM erstellt den Prüfungsnachweis und fügt die vom Fachdienst VSDM erhaltene Prüfziffer ein.

7. Das Fachmodul VSDM liefert im Response die Versichertenstammdaten und den Prüfungsnachweis an das PS.

3 Systemüberblick

Diese Spezifikation beschreibt den Produkttyp eHealth-CardLink (eH-CL). Abbildung 1 zeigt diesen und seine Schnittstellen zu anderen Komponenten. Der Produkttyp kommuniziert direkt mit Konnektoren und mit Smartcards der TI über Clients der Nutzer. Instanzen des eH-CL haben möglicherweise weitere Schnittstellen zu anderen Komponenten.

Der Produkttyp eH-CL verhält sich gegenüber einem Konnektor wie ein eHealth-Kartenterminal (eH-KT) gemäß [gemSpec_KT], allerdings mit limitiertem Funktionsumfang, siehe A_24769*. Der wesentliche Unterschied zwischen einem eH-KT und dem Produkttypen eH-CL besteht darin, dass ein eH-CL nicht selbst über Kartenslots verfügt, sondern über das Internet auf Kartenleser (Client des Nutzers) zugreift, in denen relevante Smartcards stecken. Beispielsweise sei hier ein Smartphone eines Versicherten mit NFC Funktionalität genannt, dass mit einer eGK kommuniziert. Eine App auf so einem Smartphone ermöglicht die Verbindung vom Smartphone zum eH-CL und damit von der eGK über den eH-CL zum Konnektor. Zwischen der App und den eH-CL kann es weitere Komponenten geben, beispielsweise ein App-Backend.

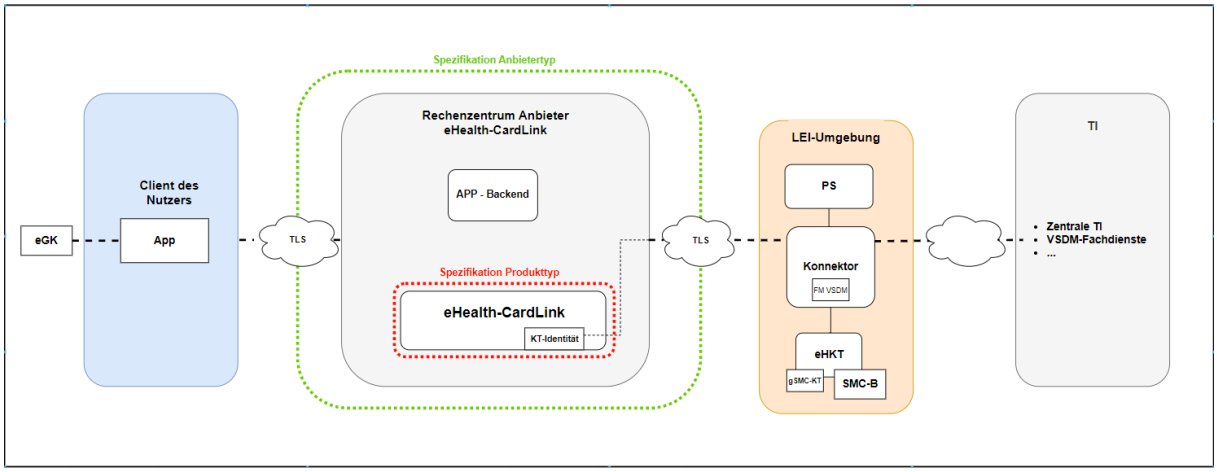

Abbildung 1: Systemüberblick

Ohne im Folgenden auf alle denkbaren Implementierungsvarianten des Produkttyps eH-CL einzugehen, lässt sich der Produkttyp eH-CL wie folgt beschreiben:

1. Der Produkttyp eH-CL verhält sich gegenüber einem Konnektor wie ein eH-KT, auch wenn er mit einem limitierten Funktionsumfang ausgestattet ist.
2. Dass der Produkttyp eH-CL gegenüber einem Produkttypen eH-KT nur einen eingeschränkten Funktionsumfang aufweist, ist für einen Konnektor irrelevant, sofern im Konnektor nur solche TUCs ausgeführt werden, die der Produkttyp eH-CL unterstützt.
3. Der Produkttyp eH-CL offeriert dem Konnektor einen oder mehrere logische Kartenslots zu Smartcards.
4. Der Produkttyp eH-CL ermöglicht es dem Konnektor, beispielsweise die relevanten Versicherten-Daten aus einer eGK auszulesen und einen VSDM-Prüfnachweis zu erzeugen.
5. Der Produkttyp eH-CL umfasst:

a. eine SICCT-konforme Schnittstelle in Richtung Konnektor (mit einem gegenüber einem eH-KT limitierten Funktionsumfang),
b. eine SM-KT-Identität zwecks Pairing und Aufbau der TLS-Verbindung zum Konnektor,
c. eine Schnittstelle zu einer App oder einem App-Backend (nutzendes System) zum Senden und Empfangen von für den „ReadVSD“-Fall relevanter eGK-Daten und Kommandos.

4 Systemkontext

Der eH-CL wird in einem Rechenzentrum betrieben. Die Anbieterzulassung für einen eH-CL setzt eine Produktzulassung für einen eH-CL voraus.
Der eH-CL ist über eine TLS-Verbindung mit einem Konnektor verbunden und reicht kartenrelevante SICCT-Anfragen an einen Client des Nutzers mit Zugriff auf eine Smartcard weiter sowie passende Antworten auf die SICCT-Anfragen an den Konnektor zurück. Der eH-CL implementiert einen SICCT-Kommandointerpreter mit der Einschränkung, dass nur ausgewählte SICCT-Kommandos unterstützt werden.
Der eH-CL ist mit dem Client des Nutzers ebenfalls über eine TLS-Verbindung verbunden. Je nach Produktausprägung endet die TLS-Verbindung im eH-CL oder einer im Rechenzentrum des Anbieters eH-CL vorgelagerten Komponente.

4.1 Rollen und Akteure beim eHealth-CardLink (eH-CL)

Der Anbieter des eH-CL erbringt Betriebsleistung und Service unter Verwendung zugelassener Produkte.
Der Anbieter kann dazu Unterauftragnehmer beauftragen (siehe auch gemKPT_Betr). Die Beziehungen der Firmen untereinander werden hier nicht betrachtet.
Folgende Akteure und Rollen sind für das beispielhafte Anwendungsszenario aus Kapitel 2.1 vorgesehen:

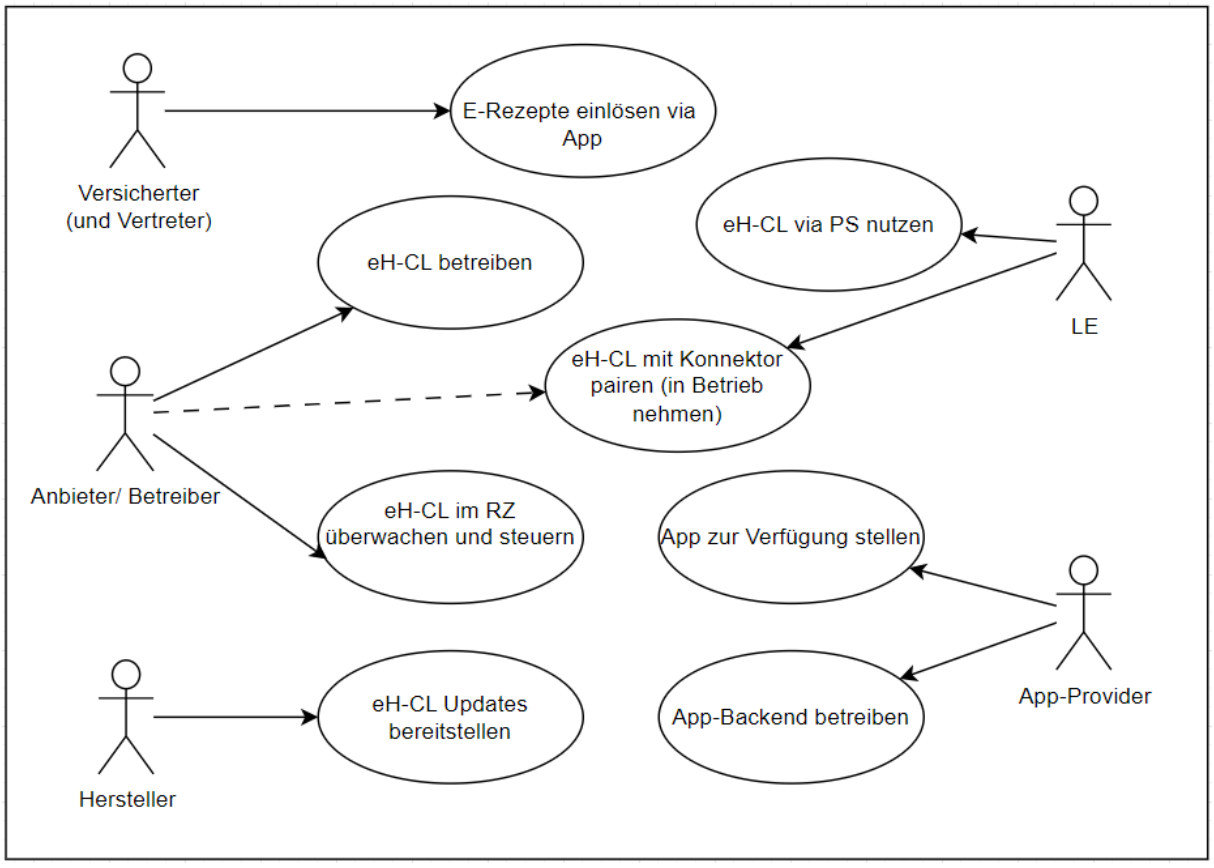

Abbildung 2: Akteure und technische Use Cases

4.1.1 Anbieter/ Betreiber

Der Betreiber überwacht und steuert technische Komponenten des eH-CL inkl. der Rechenzentrum (RZ)-Infrastruktur, in die der eH-CL integriert ist. Er administriert die dem eH-CL zugrundeliegenden und umgebenden Systeme. Zu den Aufgaben des Betreibers gehört die Installation von Softwareupdates und das Erzeugen und Wiederherstellen von Backups der eH-CL-Instanzen (Snapshots).
Weiterhin gehören die Initialisierung und Grundkonfiguration des eH-CL - damit Nutzer ihren eH-CL erreichen können - zu den Aufgaben, die vom Betreiber durchgeführt werden (dazu kann ggf. die Unterstützung des Leistungserbringers beim Pairing gehören).
Der Betreiber überwacht technische Parameter wie die Ressourcenauslastung und ändert technische Parameter wie die Ressourcenzuweisung für eH-CL-Instanzen.

4.1.2 Hersteller

Der Hersteller des eH-CL stellt Softwareupdates bereit und wird für 3rd-Level-Support/Debugging hinzugezogen.
Er hat keinen Zugriff auf Logs aus den eH-CL-Instanzen. Wenn diese für den Support notwendig sind, werden diese vom Administrator pseudonymisiert bereitgestellt.

4.1.3 Fachliche Nutzer

4.1.3.1 Leistungserbringer

Der Leistungserbringer, ist der Nutzer der fachlichen Schnittstelle (SICCT) einer konkreten eH-CL-Instanz und Inhaber einer SMB-Identität. Er verantwortet die fachliche Administration des eH-CL in der Rolle "Admin". Er kann dafür ggf. einen Dienstleister beauftragen.
Bei Nutzung des eH-CL schließt der Leistungserbringer einen Vertrag mit dem Betreiber/ Anbieter des eH-CL.

4.1.3.2 Versicherte

Versicherte oder deren Vertreter nutzen den eH-CL über ein Smartphone (einen Client des Nutzers) mit einer an den eH-CL angebundenen App.

4.1.4 App-Provider

Der App-Provider ist Betreiber einer App und stellt diese seinen Nutzern zur Verfügung. Mit dieser App und mit der Unterstützung des eH-CL und einer angebundenen Leistungserbringerinstitution kann ein VSDM-Prüfungsnachweis ausgestellt werden. Zudem betreibt der App-Provider ein für die App notwendige Backend, welches mit der App, dem eH-CL und dem PS kommunizieren kann. Je nach Umsetzungsvariante wird die Kommunikation zwischen App-Backend und eH-CL oder zwischen App und eH-CL im Kapitel 7.2 beschrieben.

Der App-Provider ist nicht Zulassungsnehmer für das Produkt oder den Anbieter eH-CL, kann aber Anforderungen für die betriebliche Nutzung des eH-CL zur Unterstützung des Anbieters erfüllen.

5 Zerlegung des Produkttyps

Der Produkttyp eHealth-CardLink (eH-CL) umfasst einen limitierten Funktionsumfang des Produkttyps eHealth-Kartenterminal (eH-KT) sowie die funktionalen Komponenten Karten-Interpreter und Konnektor-Interpreter, die im Kapitel "Funktionsmerkmale" beschrieben sind.

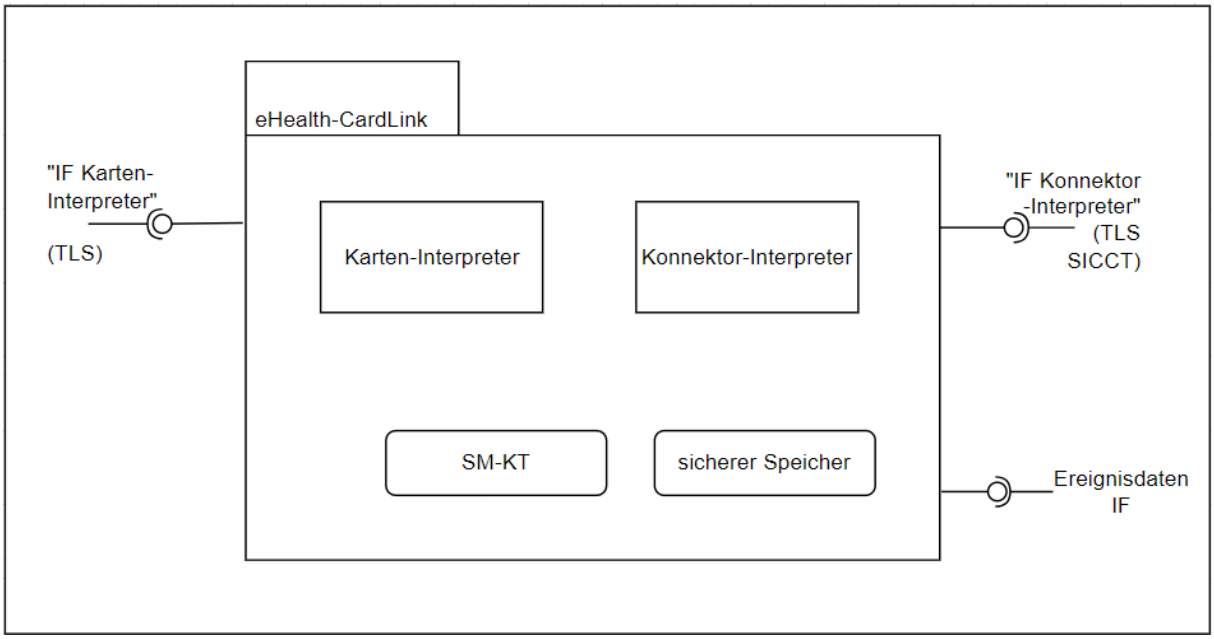

Abbildung 3: Produktzerlegung eHealth-CardLink

6 Übergreifende Festlegungen

6.1 Aufbau von sicheren Verbindungen

Der eHealth-CardLink (eH-CL) verbindet sich nach innen mit einem Konnektor und nach außen mit einem Kartenlesegerät des Nutzers, der eine Karte anbinden möchte. In beiden Richtungen kommt das TLS-Protokoll zur Absicherung der Verbindung zum Einsatz, wobei jedoch unterschiedliche Vertrauensräume Anwendung finden. Nach innen Richtung Konnektor wird der TI-Vertrauensraum genutzt, während nach außen Richtung Client des Nutzers der Vertrauensraum Internet verwendet wird.

Da sich der eH-CL gegenüber dem Konnektor wie ein eHealth-Kartenterminal (eH-KT) verhält, gelten für den eH-CL alle Anforderungen bezüglich TLS aus [gemSpec_KT]. Diese werden entsprechend im Produkttypsteckbrief des eH-CL aufgeführt.

Im Folgenden werden Vorgaben für die Absicherung der Verbindung nach außen zum Client des Nutzers getroffen.

A_24595 - eHealth-CardLink - Kryptographisch geschützte Anbindung des Clients des Nutzers
Der eHealth-CardLink MUSS durchsetzen, dass die Kommunikation mit den Clients der Nutzer, mit denen die Karte verbunden ist, ausschließlich über einen TLS-Kanal erfolgt.
[<=]

Auch bezüglich dieser TLS-Verbindung gelten für den eH-CL die entsprechenden übergreifenden Anforderungen aus gemSpec_Krypt zu TLS (GS-A_4385*, A_18467*, A_18464*, GS-A_4387*, GS-A_5035*, A_21275-01*, GS-A_5322*), Schlüsselerzeugung (GS-A_4368*) und Zufallszahlen (GS-A_4367*), die entsprechend im Produkttypsteckbrief aufgeführt sind. Abweichend zur Strecke nach innen zum Konnektor kann der eH-CL Richtung Client des Nutzers alle TLS-Cipher-Suiten aus [TR-02102-2, Abschnitt 3.3.1 Tabelle 1] mit den dort vorgegebenen Domainparametern (Schlüssellänge, ECC-Kurven-Parameter etc.) verwenden. Die Anforderung wird im Produkttypsteckbrief aufgeführt (A_24779*).

A_24601 - eHealth-CardLink - EV-TLS-Zertifikat
Der eH-CL MUSS sich beim TLS-Verbindungsaufbau gegenüber dem Client des Nutzers mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB Forum] authentisieren.**[<=]**

Dies ermöglicht den Clients der Nutzer Authentifizierung des eH-CL im Rahmen des TLS-Handshake mit "Bordmitteln" durchführen können.

A_24602 - eHealth-CardLink - OCSP-Stapling
Der eHealth-CardLink (eH-CL) MUSS an der HTTPS-Schnittstelle zum Internet OCSP-Stapling [RFC-6066] unterstützen, damit Clients den Sperrstatus des Server-Zertifikats des eH-CL prüfen und bei gesperrten Zertifikaten oder fehlenden OCSP-Responses die Verbindung ablehnen können.
[<=]

Dies ermöglicht den Clients der Nutzer eine leichte Prüfung des Sperrstatus des Zertifikats des eH-CL.

6.2 Übergreifende Sicherheitsanforderungen

Das Produkt eH-CL bietet einen gegenüber einem eH-KT eingeschränkten Funktionsumfang, wobei er aber im Gegensatz zum eH-KT gerade eine Anbindung von Karten über ungeprüfte Clients der Nutzer ermöglicht. Deshalb ist es wichtig, bestimmte Kommandos des Konnektors Richtung Karte durch den eH-CL zu unterbinden. Konkret wird verhindert, dass eine angeschlossene eGK durch PIN oder eine Leistungserbringerkarte freigeschaltet wird.

A_24593 - eHealth-CardLink - Keine PIN-Verifikation
Der eHealth-CardLink DARF KEINE Kommandos an die angebundene Karte senden, welche mit einem Passwortobjekt arbeitet - weder durchgereicht vom Konnektor, noch selbst erzeugt. Das betrifft gemäß [gemSpec_COS#14.6] folgende Kommandos:

1. CHANGE REFERENCE DATA,
2. DISABLE VERIFICATION REQUIREMENT,
3. ENABLE VERIFICATION REQUIREMENT,
4. GET PIN STATUS,
5. RESET RETRY COUNTER,
6. VERIFY.

[<=]

Wegen A_24593* ist das Setzen eines Passwortstatus in einer angebundenen Karte nicht möglich.

A_24594 - eHealth-CardLink - Keine Card-to-Card-Freischaltung
Der eHealth-CardLink DARF KEINE Kommandos an die angebundene Karte senden - weder durchgereicht, noch selbst erzeugt - welche zur Folge hat, dass ein Sicherheitsstatus gemäß [gemSpec_COS#(N030.400)] gesetzt wird CHAT.OID = oid_cvc_fl_ti = {1.2.276.0.76.4.152}, sodass geschützte Objekte oder Aktionen dadurch freigeschaltet werden.**[<=]**

A_24594* unterbindet unter anderem, dass Leistungserbringer über eH-CL Objekte in einer eGK freischalten. Zulässig gemäß A_24594* sind

1. symmetrische Authentisierungen mit den Rollen CMS oder VSD (Card-to-Server),
2. asymmetrische Authentisierungen mit den Rollen CMS oder VSD, oder
3. asymmetrische Authentisierungen gegenüber einer Karte mit Flaglisten, welche für die Karte bedeutungslos ist (etwa "Null-Flaglisten").

Unzulässig gemäß A_24594* ist das Importieren und Authentisieren von CV-Zertifikaten mit Flaglisten aus dem Bereich der TI, welche den Sicherheitszustand der angebundenen Karte verändern.

Entsprechend Kapitel 2 ist der eH-CL eine Lösung zur Anbindung der eGK. Der eH-CL soll keine kryptographisch abgesicherte Prüfung des Kartentyps vornehmen, sondern aus den über ihn übertragenen Information auf den Kartentyp schließen.

A_25182 - eHealth-CardLink - Ausschließliche Anbindung von Karten des Typs eGK
Der eHealth-CardLink MUSS technisch durchsetzen, dass ausschließlich Karten des Typs eGK angebunden werden und dazu:

- bei der initialen Anbindung der Karte vor dem Senden der SICCT-Ereignisnachrichten „Slot-Ereignis – Karte eingesteckt“ an den Konnektor anhand der übertragenen Informationen prüfen um welchen Kartentyp es sich handelt und

- das SICCT-Ereignis ausschließlich im Falle einer eGK an den Konnektor senden bzw.
- in allen anderen Fällen einen Fehler an den Client des Nutzers senden, über den die Karte angebunden ist

- bei jedem vom Konnektor angeforderten Lesen von X.509-Zertifikaten von angebundenen Karten prüfen, dass es sich um ein X.509-Zertifikat einer eGK handelt und in allen anderen Fällen
  - einen SICCT-konformen Lesefehler an den Konnektor melden sowie
  - einen Fehler an den Client des Nutzers senden, über den die Karte angebunden ist

[<=]

Da der eH-CL muss im Rahmen seiner Funktionalität personenbezogene Daten von Versicherten temporär verarbeiten. Wichtig ist jedoch, dass solche Daten nicht dauerhaft persistiert werden.

A_25199 - eHealth-CardLink - Keine Speicherung von Versicherten- und eGK-Daten
Der eHealth-CardLink DARF NICHT Daten des Versicherten und Daten der eGK persistent speichern oder protokollieren. Wird ein Vorhalten solcher Daten für spätere Prüfungen gefordert, werden diese ausschließlich im flüchtigen Speicher gehalten und nach Ablauf der in der jeweiligen Forderung genannten Frist gelöscht. <=**[<=]**

Das Produkt eH-CL fungiert als Proxy zwischen dem Client des Nutzers mit Kartenleser, der die Karte anbindet, auf der einen Seite und dem Konnektor auf der anderen Seite. Dabei agiert er als Application Layer Gateway. Es ist nicht möglich über die angeschlossenen Clients der Nutzer Aussagen zu treffen, weshalb davon auszugehen ist, dass auch über den TLS-Kanal Angriffe zu erwarten sind.

A_24596 - eHealth-CardLink - Erkennung und Abwehr von Angriffen über den TLS-Kanal
Der eHealth-CardLink MUSS Maßnahmen zum Erkennen und zur Abwehr unberechtigter Zugriffe und Angriffe über den TLS-Kanal umsetzen (bspw. ALG) und darf keine von Clients der Nutzer erhaltene Pakete oder Inhalte ungeprüft an den angeschlossenen Konnektor weiterleiten. **[<=]**

6.2.1 Maßnahmen gegen Manipulation der Kartenkommunikation

Da die Anbindung der Karte entfernt vom eH-CL und unbeobachtet stattfindet, ergeben sich andere Angriffsmöglichkeiten als im Falle des Steckens der eGK vor Ort in einer Leistungserbringerumgebung. Im Remote-Fall hat der Angreifer volle Kontrolle über die Kommunikation zur Karte, was im vor-Ort-Fall, wo die eGK in ein zertifiziertes eH-KT gesteckt wird, ausgeschlossen werden kann. Daher kann der Angreifer im Remote-Fall Karten während des Vorgangs tauschen, von der Karte gelesene Daten manipulieren oder selbst erzeugte Daten senden, die gar nicht von einer eGK gelesen wurden. Dadurch können die für den Anwendungsfall in der Leistungserbringerumgebung konzipierten Sicherheitsmaßnahmen bspw. im VSDM potentiell von einem Angreifer umgangen werden. Entsprechend ist es erforderlich - über eine allgemeine Robustheit gegen Angriffe (entsprechend A_24596*) hinaus - Maßnahmen zu ergreifen, die gewährleisten, dass die von einer entfernt angebundenen eGK empfangenen Daten auch tatsächlich von ein und derselben Karte stammen. Damit wird im konkreten Anwendungsfall VSDM sichergestellt, dass ein Prüfungsnachweis für eine Versicherten-Identität nur verwendet wird, wenn auch der eGK-Sperrstatus genau dieser Identität

positiv geprüft wurde. Wie erwähnt spielen die Angriffsszenarien im vor-Ort-Fall keine Rolle, weshalb die folgenden Maßnahmen exklusiv für eine entfernte Anbindung der eGK mit dem eH-CL umzusetzen sind.

A_24929 - eHealth-CardLink - Anwendungsfall VSDM - Prüfung ICCSN
Der eHealth-CardLink MUSS für den Anwendungsfall VSDM prüfen, dass die ICCSN im für die Echtheitsprüfung der eGK gelesenen Zertifikat C.eGK.AUT_CVC identisch ist mit der beim Lesen von EF.GDO erhaltene ICCSN. Sind die ICCSN nicht identisch MUSS der eHealth-CardLink so gegenüber dem Konnektor agieren, dass der VSDM-Anwendungsfall am Konnektor mit Fehler abgebrochen wird, sodass seitens Konnektor keine Daten an das aufrufende Primärsystem zurückgegeben werden und keine Daten auf die eGK geschrieben werden.**[<=]**

A_25193 - eHealth-CardLink - Abgleich Ablaufdatum C.CH.AUT und C.eGK.AUT_CVC
Der eHealth-CardLink MUSS prüfen, dass die innerhalb eines VSDM-Ablaufs vom Client des Nutzers präsentierten Zertifikate C.CH.AUT und C.eGK.AUT_CVC Gültigkeitsenddaten aufweisen, die innerhalb einer Woche liegen. Weichen die Gültigkeitsenddaten weiter voneinander ab, MUSS sich der eHealth-CardLink gegenüber dem Konnektor so verhalten, dass das VSDM mit Fehler abgebrochen wird und kein Prüfnachweis vom Fachmodul VSDM erzeugt wird.**[<=]**

Hinweis zu A_25193: Entsprechend A_19073 und A_19173 haben das X.509-Zertifikat C.CH.AUT und das CV-Zertifikat C.eGK.AUT_CVC das selbe Ablaufdatum, sofern im Falle der G2.1 eGK das ECC-X.509-Zertifikat betrachtet wird. Letzteres ist im Anwendungsfall VSDM gegeben, da dort bei G2.1 eGK immer die ECC-X.509-Identität von der eGK gelesen wird.*

6.2.2 Pairing mit Konnektor

Das Pairing mit einem Konnektor ist ein sicherheitskritischer Schritt. Es ist wichtig, dass es dem am Konnektor agierenden Administrator möglich ist festzustellen, ob das Pairing für einen eH-CL oder für ein eH-KT durchgeführt wird. Die Unterscheidung wird dadurch ermöglicht, dass sowohl eH-CL, als auch eH-KT das Kommando SICCT GET STATUS für das Card Terminal Manufacturer Data Object (CTM DO) unterstützen. Im CTM DO finden sich gemäß [gemSpec_KT#3.7.7] unter anderem ein von der gematik vergebenes Herstellerkürzel. Die Unterscheidung zwischen eH-CL und eH-KT ist durch das Herstellerkürzel, oder durch weitere, verpflichtende Informationen im CTM DO möglich.

Im Rahmen des Pairings wird zwischen Konnektor und eH-CL ein Pairing-Geheimnis etabliert.

A_24606 - eHealth-CardLink - Sichere Speicherung der Pairing-Geheimnisse
Der eHealth-CardLink (eH-CL) MUSS die Pairing-Geheimnisse für die mit ihm gepairten Konnektoren so vor unberechtigtem Zugriff geschützt speichern, dass auch Administratoren des Anbieters eH-CL diese nicht im Klartext auslesen können.**[<=]**

6.3 Übergreifende Anbieteranforderungen

A_24953 - eHealth-CardLink - Änderungen nur durch Berechtigte
Der Anbieter eHealth-CardLink MUSS durchsetzen, dass nur Berechtigte Konfigurationsänderungen und das Einspielen von Updates vornehmen können.**[<=]**

6.3.1 Absicherung der SM-KT

Um sich gegenüber dem Konnektor auszuweisen ist eine SM-KT mit den darauf enthaltene Identitäten notwendig. Die derzeit einzige Ausprägung ist eine gSMC-KT Smartcard. Die konkrete technische Anbindung der gSMC-KT wird nicht vorgeschrieben, jedoch muss ein Zugriffsschutz im Betrieb gewährleistet sein.

A_25214 - eHealth-CardLink - Zugriffsschutz gSMC-KT
Der Anbieter eHealth-CardLink MUSS die gSMC-KT in einem vor Zutritt geschützten Bereich betreiben und unberechtigte physische und logische Zugriffe auf die gSMC-KT unterbinden.**[<=]**

6.3.2 Absicherung Richtung Internet

Das Produkt eH-CL verbindet sich entsprechend 6.1 über einen TLS-Kanal mit seinen Kommunikationspartnern. Die Anbindung und Absicherung auf IP-Ebene ist Aufgabe des Anbieters eH-CL.

A_24597 - eHealth-CardLink - Erkennung und Abwehr unberechtigter Zugriffe aus dem Internet
Der Anbieter eHealth-CardLink MUSS Maßnahmen zum Erkennen und zur Abwehr unberechtigter Zugriffe aus dem Internet umsetzen (bspw. durch Paketfilter, Netflow, IDS/IPS, ALG).**[<=]**

A_24598 - eHealth-CardLink - Sicherung zum Transportnetz Internet durch Paketfilter
Der Anbieter eHealth-CardLink MUSS den Zugang zum Internet durch einen zustandslosen Paketfilter (ACL) absichern, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der Paketfilter MUSS frei konfigurierbar sein auf der Grundlage von Informationen aus OSI Layer 3 und 4, das heißt Quell- und Zieladresse, IP-Protokoll sowie Quell- und Zielport.**[<=]**

A_24599 - eHealth-CardLink - Platzierung Paketfilters Internet
Der Anbieter eHealth-CardLink (eH-CL) DARF den Paketfilter zum Schutz in Richtung Transportnetz Internet NICHT auf der selben physischen Komponente betreiben wie den eH-CL.**[<=]**

A_24600 - eHealth-CardLink - Richtlinien für den Paketfilter zum Internet
Der Anbieter eHealth-CardLink (eH-CL) MUSS im Paketfilter die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf die nachfolgenden Protokolle beschränken:

- HTTPS
- OCSP-Zugriffe für das OCSP-Stapling nach A_24602*
- ggf. notwendige DNS Anfragen (und Antworten)

Ein Verbindungsaufbau vom eH-CL in Richtung Internet MUSS unterbunden werden, mit Ausnahme der Verbindungen bzgl. OCSP-Stapling. Ausnahmen davon sind mit dem Gutachter abzustimmen, von diesem zu bewerten und im Falle der Abnahme (positiven Bewertung) durch den Gutachter nachvollziehbar im Gutachten zu dokumentieren.**[<=]**

6.3.3 Absicherung Richtung Konnektor

A_24604 - eHealth-CardLink - Kein direkter Zugriff auf Konnektoren
Der Anbieter eHealth-CardLink (eH-CL) MUSS einen direkten Zugriff aus dem Internet auf die mit dem eH-CL verbundenen Konnektoren verhindern.**[<=]**

A_24605 - eHealth-CardLink - 4-Augen-Prinzip bei Änderungen
Der Anbieter eHealth-CardLink (eH-CL) MUSS durchsetzen, dass Änderungen an der Software und Hardware des eH-CL nur im 4-Augen-Prinzip möglich sind.**[<=]**

Reine Konfigurationsänderungen über die gesicherte Management-Schnittstelle des eH-CL sind von A_24605* ausgenommen. Änderungen der Software über diese Management-Schnittstelle (Software-Update) erfüllen das 4-Augenprizip, wenn diese eben nur über den angemeldeten Administrator des Anbieters eingespielt werden können und vom Produkt eH-CL vor der Anwendung des Updates eine Signatur des Updates geprüft wird, die nur der Hersteller aufbringen kann.

Das Pairing zwischen eH-CL und den mit diesen verbundenen Konnektoren ist ein sicherheitskritischer Schritt und darf nicht unkontrolliert geschehen. Der Anbieter benötigt entsprechend sichere Prozesse, die gewährleisten, dass nur berechtigte Administratoren auf Seiten des eH-CLs das Pairing ermöglichen können.

A_24845 - eHealth-CardLink - Kontrolliertes Pairing von Konnektoren
Der Anbieter eHealth-CardLink (eH-CL) MUSS durchsetzen, dass nur berechtigtes Personal das Pairing des eH-CL mit Konnektoren bestätigen bzw. umsetzen kann; also keine unkontrollierte Kopplung des eH-CL mit beliebigen Konnektoren stattfindet.**[<=]**

Aus Sicht des Konnektors befindet sich der eH-CL - ebenso wie ein eH-KT - im selben lokalen Netz, wie der Konnektor selbst und der Anbieter eH-CL muss entsprechend für eine sichere Anbindung der Konnektoren sorgen, die das abbildet.

A_24852 - eHealth-CardLink - Sichere Anbindung von Konnektoren
Der Anbieter eHealth-CardLink (eH-CL) MUSS die mit dem eH-CL zu verbindenden Konnektoren bzw. das Netz, indem sich diese befinden, sicher anbinden, sodass diese den eH-CL im selben Netzwerk erreichen. Eine solche Anbindung ist bspw. über eine VPN-Verbindung möglich.**[<=]**

6.3.4 Absicherung über Protokollierungsmaßnahmen

Im folgenden Abschnitt sollen Maßnahmen zur Tatgelegenheitsreduktion möglicher Missbrauchsszenarien beim Einsatz von eH-CL durch den Anbieter umgesetzt werden.

A_25156 - eHealth-CardLink - Anwendung nur mit Telefonnummer
Der Anbieter eHealth-CardLink (eH-CL) MUSS sicherstellen, dass Anwendungsfälle mit dem eH-CL nur für Nutzer möglich sind, die eine Telefonnummer angeben.**[<=]**

A_25157 - eHealth-CardLink - SMS-Code vor Daten-Abruf
Der Anbieter eHealth-CardLink (eH-CL) MUSS, bevor mit Unterstützung des eH-CL ein VSDM-Prüfungsnachweis erzeugt wird,

- dem Nutzer einen SMS-Code an die im Nutzerkonto hinterlegte oder eingegebene Telefonnummer senden
- und den vom Nutzer eingegebenen und von dem Anbieter eH-CL empfangenen Code gegen den zuvor erzeugten Code abgleichen
- und genau nur im Falle der Übereinstimmung den Datenabruf durchführen.

[<=]

A_25478 - eHealth-CardLink - Anwendung nur mit deutscher Telefonnummer
Der Anbieter eHealth-CardLink (eH-CL) MUSS sicherstellen, dass der in A_25157* geforderte SMS-Code ausschließlich an Telefonnummern von deutschen Anbietern versendet wird.**[<=]**

A_25168 - eHealth-CardLink - SMS-Code Gültigkeit

Der Anbieter eHealth-CardLink (eH-CL) KANN nach dem Abgleich des SMS-Codes (vgl. A_25157*) bei wiederholten Anwendungsfällen innerhalb einer Session und innerhalb von 15 Minuten auf den Abgleich eines SMS-Codes verzichten.**[<=]**

A_25169 - eHealth-CardLink - eGK mit Telefonnummer verknüpfen
Der Anbieter eHealth-CardLink (eH-CL) MUSS bei erstmaliger Verwendung einer eGK durch einen Nutzer, diese eGK mit der Telefonnummer des Nutzers verknüpfen.**[<=]**

A_25212 - eHealth-CardLink - Maximale Anzahl eGKs pro Session
Der Anbieter eHealth-CardLink (eH-CL) MUSS die Verbindungen innerhalb einer nach A_25168* validierten Session höchstens für zehn (10) eGKs aufrecht halten.**[<=]**

A_25170 - eHealth-CardLink - Information durch Backend bei bereits mit Telefonnummer verknüpfter eGK
Der Anbieter eHealth-CardLink (eH-CL) MUSS bei der Verknüpfung einer eGK, die bereits einer anderen Telefonnummer zugewiesen ist:

- an die App des App-Providers in der aktuellen Session einen entsprechenden Status senden, der den Zeitpunkt der Erstellung der bestehenden Verknüpfung enthält,
- die bisherige Verknüpfung der eGK mit der entsprechenden Telefonnummer aufheben und
- den Nutzer, mit dessen Telefonnummer die eGK bisher verknüpft war, über einen verfügbaren Kommunikationsweg informieren, dass die Verknüpfung mit der eGK auf Grund einer neuen Zuordnung aufgehoben wurde und dabei den Zeitpunkt der neuen Verknüpfung angeben.

[<=]

A_25178 - eHealth-CardLink - Protokollierung und Anomalie-Erkennung
Der Anbieter eHealth-CardLink (eH-CL) MUSS die Zugriffe auf den eHealth-CardLink protokollieren und für 90 Tage vorhalten, und dabei:

- mindestens Datum, Uhrzeit, Telefonnummer und ICCSN speichern
- das Protokoll vor unberechtigten Zugriffen schützen
- die Daten mit Ablauf der 90 Tage sicher löschen
- die vorhandenen Daten stetig hinsichtlich Anomalien analysieren und
- pseudonymisierte Daten zur Anomalie-Prüfung der gematik auf Anfrage bereitstellen.

[<=]

Die in A_25178* genannten Fälle, die zur Anomalie-Prüfung einbezogen werden sollen, sind grundsätzlich erlaubte Nutzungsszenarien, weichen aber vom Standardfall ab, bei dem Versicherte ihre eGK nutzen und sich Telefonnummern nur sehr selten ändern. Insbesondere zu Beginn des Betriebs von Lösungen mit entfernter Anbindung einer eGK wird es die Aufgabe der Betreiber der Lösung und der gematik sein, die Anomalie-Erkennung gemeinsam auszuwerten und kontinuierlich zu verbessern. Dazu wird es anfangs auch erforderlich sein, die pseudonymisierten Daten häufig an die gematik zu übermitteln, während dies später in größeren Zeitabständen erfolgen kann. Die Weiterentwicklung der Anomalie-Erkennung kann dann auch zu Anpassungen der A_25178* führen.

7 Funktionsmerkmale

Wie in Kapitel "Systemüberblick" dargelegt, betrachtet diese Spezifikation hinsichtlich des Produkttypen eHealth-CardLink (eH-CL) aus funktionaler Sicht lediglich die folgenden Schnittstellen:

1. "IF Konnektor-Interpreter" als Schnittstelle, welche die Kommunikation zwischen Konnektor und eH-CL beschreibt; der Funktionsumfang dieser Schnittstelle ist eine Teilmenge derjenigen aus [gemSpec_KT].
2. "IF Karten-Interpreter" als logische Schnittstelle zwischen eH-CL und dem Client des Nutzers, bzw. App oder App-Backend.Es können weitere technische Komponenten (bspw. Backend-Systeme oder Load Balancer) beteiligt sein. Diese werden in dieser Spezifikation nicht beschrieben.

7.1 Konnektor-Interpreter

A_24769 - eHealth-CardLink - Schnittstelle Konnektor - eHealth-CardLink
Der eHealth-CardLink (eH-CL) MUSS aus funktionaler Sicht die Anforderungen aus [gemSpec_KT] umsetzen, sofern sie im Produkttypsteckbrief von eH-CL genannt sind. Dabei gelten folgende Besonderheiten:

1. Folgende Functional Units gemäß [SICCT#Abb.2] sind zu unterstützen:
   a. SICCT Kommandointerpreter
   b. Anzahl Slots (im Sinne von Kartenslots) aus dem Intervall eins bis 14
2. Das Vorhandensein der übrigen, im Folgenden genannten, Functional Units gemäß [SICCT] ist nicht erforderlich, aber zulässig: Display, Keypad, RFID-Antenne, Iris-Scann, Face-Recognition, Dynamic Signature Verification, Voiceprint, Fingerprint, Printer, Acoustic Signal, Optical Signal
3. Folgende Kommandos an den SICCT Interpreter bzw. deren Ausprägungen sind zu unterstützen:
   a. SICCT INIT CT SESSION (siehe [SICCT#5.10]),
   b. SICCT CLOSE CT SESSION (siehe [SICCT#5.11]),
   c. SICCT RESET CT / ICC (siehe [SICCT#5.12]),
   d. SICCT REQUEST ICC (siehe [SICCT#5.13],
   e. SICCT EJECT ICC (siehe [SICCT#5.14]),
   f. SICCT GET STATUS (siehe [SICCT#5.15]) mit den Einschränkungen:
      i. Parameter P1 aus der Menge {'00'} (adressiert das Kartenterminal) und P2 aus der Menge:
         A. P2='46': CardTerminal Manufacturer Data Object
         B. P2='63': CardTerminal Status Data Object
         C. P2='80': ICC Status Data Object (all ICC Interfaces)
      ii. Parameter P1 aus dem Intervall ['01', '0E'] (adressiert kontaktbehaftete Kartenslots eins bis 14) und P2 aus der Menge:

   A. P2='66': Interface Capabilities Data Object

g. SICCT OUTPUT (siehe [SICCT#5.18]),

h. EHEALTH TERMINAL AUTHENTICATE (siehe [gemSpec_KT#3.7.2]) mit folgender Einschränkung: In der Ausprägung "P2=´01´ (CREATE)" im Schritt 5 (siehe TIP1-A_3125-*) ist es zulässig, dass eH-CL

   i. keine Displayausgabe durchführt, selbst dann, wenn eH-CL über ein Display verfügt und

   ii. den Druck auf eine Taste simuliert, selbst dann, wenn eH-CL über ein Keypad verfügt.

4. Die Unterstützung der übrigen, im Folgenden genannten, Kommandos an den SICCT Interpreter ist nicht erforderlich, aber zulässig: SICCT CONTROL COMMAND, SICCT GET STATUS für weitere Kombinationen von P1 und P2, SICCT SET STATUS, SICCT INPUT, SICCT PERFORM VERIFICATION, SICCT MODIFY VERIFICATION DATA, SICCT COMFORT AUTHENTICATION, SICCT CONFORM ENROLL, SICCT DOWNLOAD INIT, SICCT DOWNLOAD DATA, SICCT DOWNLOAD FINISH.

5. Die Unterstützung von SICCT SELECT CT MODE ist gemäß [gemSpec_KT#TIP1-A_3012] untersagt.

6. Wenn eH-CL ein Slot-Ereignis "Karte gesteckt" meldet und es handelt sich dabei um eine:

   a. eGK, dann ermöglicht der eH-CL aus Sicht des Konnektors die korrekte Ausführung mindestens der folgenden Kartenkommandos, falls diese nicht durch Secure Messaging geschützt sind:

      i. SELECT gemäß [gemSpec_COS#(N040.800), (N041.300)], selektieren des MF ohne Antwortdaten oder Antwortdaten mit FCP

      ii. SELECT gemäß [gemSpec_COS#(N042.700), (N043.300)], selektieren per AID ohne Antwortdaten oder Antwortdaten mit FCP für die Verzeichnisse DF.ESIGN und DF.HCA

      iii. SELECT gemäß [gemSpec_COS#(N046.700), (N047.300)], selektieren einer Datei ohne Antwortdaten oder Antwortdaten mit FCP für die Dateien:

         A. im MF: EF.ATR, EF.C.CA.CS.E256, EF.C.eGK.AUT_CVC.E256, EF.GDO, EF.Version2

         B. im DF.ESIGN: EF.C.CH.AUT.R2048, EF.C.CH.ENC.R2048, EF.C.CH.AUT.E256, EF.C.CH.ENC.E256,

         C. im DF.HCA: EF.GVD, EF.PD, EF.StatusVD, EF.VD

      iv. READ BINARY gemäß [gemSpec_COS#(N051.100), (N051.500)], ohne und mit *shortFileIdentifier* für die Dateien:

         A. im MF: EF.ATR, EF.C.CA.CS.E256, EF.C.eGK.AUT_CVC.E256, EF.GDO, EF.Version2

         B. im DF.ESIGN: EF.C.CH.AUT.R2048, EF.C.CH.ENC.R2048, EF.C.CH.AUT.E256, EF.C.CH.ENC.E256,

         C. im DF.HCA: EF.GVD, EF.PD, EF.StatusVD, EF.VD

      v. UPDATE BINARY gemäß [gemSpec_COS#(N053.200), (N053.600)] ohne und mit shortFileIdentifier für die Datei EF.Prüfungsnachweis

      vi. APPEND RECORD gemäß [gemSpec_COS#(N058.400), (N058.700)] ohne und mit shortFileIdentifier für die Datei EF.Logging.

      vii. EXTERNAL AUTHENTICATE gemäß [gemSpec_COS#(N083.500)].

viii. INTERNAL AUTHENTICATE gemäß [gemSpec_COS#(N086.400)].

ix. PSO Verify Certificate gemäß [gemSpec_COS#(N095.500)].

x. GET CHALLENGE gemäß [gemSpec_COS#(N098.625)].

xi. LIST PUBLIC KEY gemäß [gemSpec_COS#(99.452)].

xii. MANAGE SECURTITY ENVIRONMENT in den folgenden Ausprägungen:

A. [gemSpec_COS#(N100.900)], Schlüsselauswahl zur internen, asymmetrischen Authentisierung

B. [gemSpec_COS#(N101.900)], Schlüsselauswahl zur externen, asymmetrischen Authentisierung

C. [gemSpec_COS#(N103.300)], Schlüsselauswahl zum Prüfen von CV–Zertifikaten

b. eGK, dann ermöglicht der eH-CL aus Sicht der eGK die korrekte Ausführung mindestens der folgenden Kartenkommandos zum Aufbau eines Trusted Channels:

i. MANAGE SECURTITY ENVIRONMENT in der Ausprägung gemäß [gemSpec_COS#(N102.400)], Schlüsselauswahl zur symmetrischen, gegenseitigen Authentisierung.

ii. GET CHALLENGE gemäß [gemSpec_COS#(N098.625)].

iii. EXTERNAL AUTHENTICATE gemäß [gemSpec_COS#(N083.800)], symmetrische, gegenseitige Authentisierung mit Aufbau eines Trusted Channels.

c. eGK, dann werden Karten APDUs, welche durch Secure Messaging geschützt sind (vergleiche [gemSpec_COS#13]), unverändert weitergeleitet.

d. einen anderen Kartentyp, dann legt diese Version dieser Spezifikation das weitere Verhalten von eH-CL nicht fest.

[<=]

Hinweis: In A_24769- Punkt 6.a wird die Einschränkung "Secure Messaging" vorgenommen. Mit "Secure Messaging" ist eine Transportsicherung von Kartennachrichten gemäß [gemSpec_COS#13] gemeint. Im CLA Byte wird gemäß (N032.500) sichtbar, ob eine Kommandonachricht per "Secure Messaging" gesichert ist oder nicht.*

7.2 Karten-Interpreter

Gemäß dem in Kapitel 2 beschriebenen Anwendungskontext bietet der eHealth-CardLink (eH-CL), in der vorliegenden Version, den nutzenden Systemen eine Webschnittstelle an (Card Communication Interface), über die das nutzende System Daten einer Karte (eGK) an den eH-CL übermitteln kann, der eH-CL Kartenkommandos und Nachrichten an das nutzende System senden und Responses der Karte vom nutzenden System empfangen kann. Je nach Umsetzungsvariante kann das nutzende System ein App-Backend oder direkt eine App sein.

A_25159 - eHealth-CardLink - Card Communication Interface, Websocket-Verbindungen
Der eHealth-CardLink (eH-CL) MUSS eine Webschnittstelle "Card Communication Interface" anbieten, die

1. mindestens Verbindungen per Websocket unterstützt und

2. auf Applikationsebene Nachrichten gemäß dem Schema in folgendem Projekt austauscht:
   https://github.com/gematik/api-ehcl

[<=]

A_25160 - eHealth-CardLink - Card Communication Interface, API-Dokumentation
Falls eHealth-CardLink (eH-CL) für die Kartenkommunikation Schnittstellen anbietet, die nicht gemäß A_25159 arbeiten, dann MUSS der Hersteller des eH-CL zusätzlich eine Referenzimplementierung bereitstellen, der das Interface aus A_25159* unterstützt und die Nachrichten in die herstellerspezifische Kommunikation zu eH-CL und zum nutzenden System weiterleitet.
[<=]

Die Webschnittstelle Card Communication Interface unterstützt den im Diagramm "Ablauf Prüfungsnachweis (PNW) erzeugen" beispielhaft dargestellten Nachrichtenfluss zwischen den Komponenten App bzw. App-Backend (nutzendes System) und eHealth-CardLink.

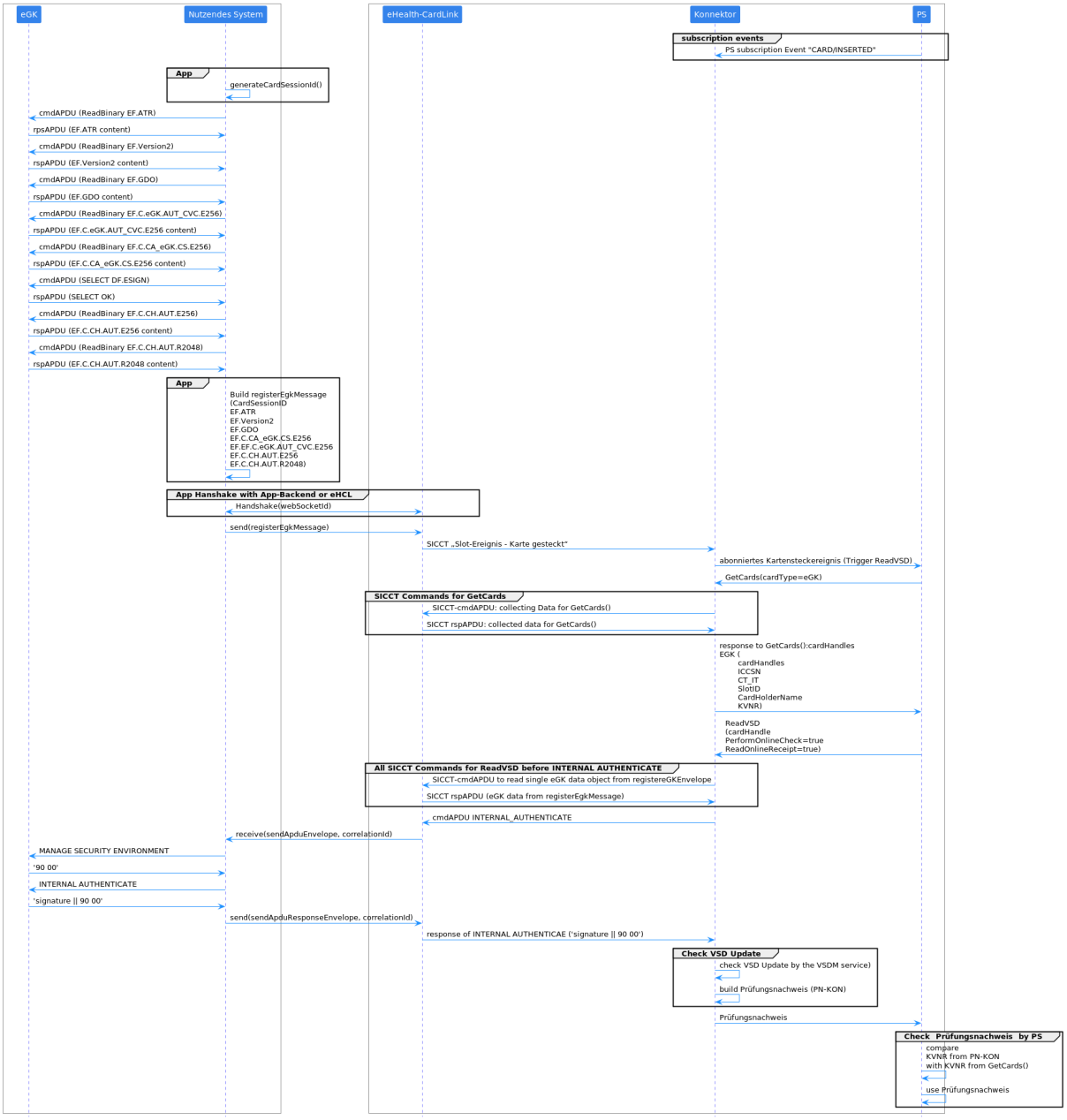

Abbildung 4: Ablauf Prüfungsnachweis (PNW) erzeugen

A_25161 - eHealth-CardLink - SICCT „Slot-Ereignis – Karte eingesteckt“ an Konnektor senden

Der eHealth-CardLink (eH-CL) MUSS nach Empfang einer Nachricht receiveRegisterEgkMessage mit den Kartendaten aus registerEgkMessage ein SICCT „Slot-Ereignis – Karte eingesteckt“ ([SICCT#6.2.4.4], TAG ‚84’) an den Konnektor senden.**[<=]**

A_25189 - eHealth-CardLink - correlationId zur Korrelation von Command- und Response-APDU

Der eHealth-CardLink (eH-CL) MUSS Correlation IDs (correlationId) zur Korrelation von Command- und Response-APDUs erzeugen, auswerten und an das nutzende System übergeben.**[<=]**

A_25162 - eHealth-CardLink - Command APDU INTERNAL AUTHENTICATE an nutzendes System weiterleiten
Der eHealth-CardLink (eH-CL) MUSS ein an der Konnektor-Interpreter-Schnittstelle empfangenes Kommando INTERNAL AUTHENTICATE im Format sendApduEnvelope über die Operation sendApduMessage an das auf die eGK zugreifende nutzende System weiterleiten.**[<=]**

A_25185 - eHealth-CardLink - Response APDU INTERNAL AUTHENTICATE an Konnektor weiterleiten
Der eHealth-CardLink (eH-CL) MUSS nach Empfang einer Nachricht sendApduResponseMessage, die eine INTERNAL AUTHENTICATE Response enthält, diese an den Konnektor weiterleiten.**[<=]**

A_25163 - eHealth-CardLink - Webschnittstelle, Fehlerfälle bei registerEgk
In Fehlerfällen während des Ablaufs von registerEgk MUSS der eHealth-CardLink (eH-CL) über die Operation sendTaskListErrorMessage eine dem Fehlerfall entsprechende taskListErrorMessage an das nutzende System senden.**[<=]**

7.3 Identität und sicherer Speicher

Die Anforderungen an die Identität des eH-CL entsprechen im Wesentlichen denen an ein eH-KT. Diese sind in [gemSpec_KT] im Kapitel "Anforderungen an die Kartenterminalidentität" zusammengefasst.

Ein eH-CL hat eine SM-KT-Identität und nutzt diese Identität zum Aufbau einer TLS-Verbindung zum Konnektor.

Virtualisierung: Wenn es mehrere eH-CL-Instanzen gibt, ist es aus Sicherheitssicht zulässig, dass alle eH-CL-Instanzen sich eine SM-KT-Identität teilen. Aus Sicherheitssicht ist das selbst dann zulässig, wenn jede eH-CL-Instanz eine eigene TLS-Verbindung mit einem Konnektor unterhält. Aus Sicherheitssicht ist es also zulässig, dass ein Konnektor gleichzeitig mit mehreren eH-CL per TLS verbunden ist und alle eH-CL für den TLS-Handshake dieselbe SM-KT-Identität verwenden.

Hinweis: Es ist möglich, dass es Konnektor-Implementierungen gibt, die den Aufbau einer weiteren TLS-Verbindung zu einem Gerät ablehnen, das eine Identität präsentiert, wenn dieselbe Identität bereits zum Aufbau einer bestehenden TLS-Verbindung genutzt wurde. Pro eH-CL-Instanz, die mit so einer Konnektor-Implementierung verbunden wird, ist dann eine eigene SM-KT-Identität erforderlich.

Der eH-CL schützt bestimmte, gespeicherte Daten vor Zugriff. Dies betrifft sowohl die unberechtigte Kenntnisnahme (Vertraulichkeit) als auch die unbemerkte Manipulation (Integrität) von Daten.

A_24855 - eHealth-CardLink - Geschützte Speicherung kritischer persistenter Daten
Der eHealth-CardLink (eH-CL) DARF NICHT den privaten Schlüssel für sein Internet-TLS-Zertifikat (A_24601*) und das Shared Secret im Klartext persistent speichern.**[<=]**

Es ist zulässig, zur Erfüllung von A_24855* Bordmittel des Betriebssystems und der Server-Hardware zu verwenden (bspw. TPM). Ein HSM ist nicht zwingend erforderlich.

8 Informationsmodell

Ein gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten wird nicht benötigt.

9 Verteilungssicht

Ein eH-CL wird als Software-Anwendung in einem Rechenzentrum beim Anbieter eH-CL ausgerollt und betrieben.

10 Anhang A – Verzeichnisse

10.1 Abkürzungen

Kürzel	Erläuterung
ACL	Access List (enthält Zugriffs- und Verbotsregeln für die Filterung von Datenpaketen)
ALG	Application Layer Gateway
eH-CL	eHealth-CardLink
eH-KT	eHealth-Kartenterminal
HSM	Hardware-Sicherheitsmodul
ICCSN	Integrated Circuit. Card Serial Number (Die ICCSN ist die weltweit eindeutige Identifikationsnummer eines Chipmoduls einer Smartcard)
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
LEI	Leistungserbringerinstitution
PS	Primärsystem
RZ	Rechenzentrum
TLS	Transport Layer Security, etwa gemäß RFC 5246
TUC	Technical Use Case

10.2 Glossar

Begriff	Erläuterung
CAB-Forum	CA/Browser Forum - https://cabforum.org/
Client des Nutzers	Mit dem Begriff "Client des Nutzers" werden Smartgeräte eines Versicherten oder seines Vertreters, die mit Kartenleser und

	Internetzugang ausgestattet sind, bezeichnet (beispielsweise ein Smartphone).
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
Internet Vertrauensraum	Der Vertrauensraum für TLS-Zertifikate der durch die Zertifizierungsstellen (Certification Authorities, CAs) aufgespannt wird, die durch die gängigen Web-Browser und Betriebssysteme akzeptiert werden. Siehe dazu auch [CAB-Forum].

Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung gestellt.

10.3 Abbildungsverzeichnis

10.4 Tabellenverzeichnis

No table of figures entries found.

10.5 Referenzierte Dokumente

10.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemSpec_KT]	Spezifikation eHealth-Kartenterminal

10.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[SICCT]	SICCT TeleTrusT, SICCT Secure Interoperable ChipCard Terminal, Version 1.2.3, 30. September 2016 Errata zu SICCT1.2.3, Version 1.0 vom 5. Mai 2021

10.6 Klärungsbedarf

Kapitel	Offener Punkt	Zuständig
	derzeit keine	

10.7 Allgemeine Erläuterungen

10.7.1 Betrachtungen zum Loggen auf einer eGK

Die eGK besitzt mit der Datei EF.Logging einen Speicherbereich, wo der Zugriff auf geschützte Daten protokolliert wird. Von Anfang an und nach wie vor gilt dabei das Prinzip, dass Aktionen der folgenden Rollen nicht geloggt werden, weil diese Rollen nicht die entsprechenden Zugriffsrechte besitzen:

1. Rolle Besitzer der Karte,
2. Rolle CMS,
3. Rolle VSD.

Wegen A_24594* führen aber nur die Rollen Besitzer, CMS oder VSD-Aktionen mit einer Karte durch, welche an einen eHealth-CardLink (eH-CL) angebunden ist. Daraus folgt, dass Aktionen, welche über den eHealth-CardLink erfolgen mangels Zugriffsrechten nicht geloggt werden.