Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature: Laufzeitverlängerung gSMC-K

ENTWURF

Version:	1.0.0 CC
Revision:	371997
Stand:	07.06.2021
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemF_Laufzeitverlängerung_gSMC-K

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
0.9.0	20.05.21		Vorabversion zur Prüfung	gematik
1.0.0 CC	07.06.21		zur Abstimmung freigegeben	gematik

ENTWURF

Inhaltsverzeichnis

1 Einordnung des Dokuments 5

1.1 Zielsetzung 5

1.2 Zielgruppe 5

1.3 Abgrenzungen 5

1.4 Methodik 6

1.4.1 Anforderungen 6

1.4.2 Hinweise auf offene Punkte 6

2 Technisches Konzept Laufzeitverlängerung gSMC-K 7

2.1 Zusammenfassung 7

2.1.1 Betroffene Komponenten und Zertifikate 7

2.1.2 Lösung 8

2.1.3 Wiederholbarkeit der Aktion 9

2.1.4 Zusammenspiel mit der ECC-Migration der Konnektoren 9

2.1.5 Bedeutung der Laufzeitverlängerung der gSMC-K für Robustheit, Akzeptanz und Zukunftsfähigkeit der TI 10

2.2 Identität ID.NK.VPN relevant für Konnektor - VPN-Zugangsdienst 10

2.3 Identität ID.AK.AUT relevant für Konnektor - PS 10

2.3.1 Lösungsalternative: Export von im Konnektor generierten TI-fremden Zertifikaten 11

2.3.2 Lösungsalternative: Import von extern generierten TI-fremden Zertifikaten 11

2.4 Identität SAK.AUTD_CVC relevant für C2C mit HBA 11

2.5 Identität ID.SAK.AUT relevant für eHealth-Kartenterminal 12

3 Operative Umsetzung 13

3.1 Bereitstellung der Zertifikatssenke 13

3.2 Bereitstellung der Zertifikate 13

3.3 Sperrprozesse 13

3.4 Offline Konnektoren 14

4 Spezifikation 15

4.1 Änderungen in gemSpec_Kon 15

4.1.1 (3.1) Konnektoridentität und gSMC-K 15

4.1.2 (3.1.1) Erneuerung der Zertifikate der gSMC-K 15

4.1.3 (3.3) Betriebszustand 18

4.1.4 (4.3.5) Neustart und Werksreset 30

4.1.5 Identität ID.NK.VPN relevant für Konnektor - VPN-Zugangsdienst 31

4.1.5.1 (4.3.7) Re-Registrierung des Konnektors mit neuem NK-Zertifikat 31

4.1.6 (3.4.1) Identität ID.AK.AUT relevant für Konnektor - PS 34

4.1.7 (7 Anhang F) Events 36

4.2 (4.1.1.2) Änderungen in gemILF_PS 36

ENTWURF

4.3 Änderungen in gemSpec_VPN_ZugD 39
4.3.1 (5.3) Schnittstelle I_Registration_Service 39
4.4 Änderungen in gemSpec_X.509_TSP 39
4.4.1 (6.6) Erneuerung von Zertifikaten der gSMC-K 39
4.5 Änderungen in gemSpec_CVC_TSP 40
4.5.1 (5.2) Erneuerung von CV-Zertifikaten der gSMC-K 40
4.6 Änderungen in gemRL_TSL_SP_CP 41
4.6.1 (Kap. 10) Anhang A – Certificate Policy für Komponentenzertifikate 41
4.7 Änderungen in gemSpec_KT 41
4.7.1 Änderung 1, Besonderheiten zur Gültigkeit.....42
4.7.2 Änderung 2, Anmerkung zur Systemuhr.....42
4.7.3 Änderung 3, Datums- und Zeitinformation 42
4.7.4 Änderung 4, Pairing-Block.....43
4.7.5 Änderung 5, Erläuterung zum Pairing Block 43
5 Anhang A – Verzeichnisse 44
5.1 Abkürzungen 44
5.2 Referenzierte Dokumente 44
5.2.1 Dokumente der gematik.....44
5.2.2 Weitere Dokumente.....44
6 Anhang C – Offene Punkte, Fragen 45

ENTWURF

1 Einordnung des Dokuments

Dieses Dokument beschreibt das Feature "Laufzeitverlängerung gSMC-K" mit dem die spezifikatorische Grundlage für eine sichere verlängerte Nutzung von Konnektor-Identitäten der gSMC-K gelegt wird.
Mit diesem Dokument soll die Abstimmung und Freigabe des Features mit den betroffenen Herstellern, dem BSI und den Gesellschaftern der gematik erfolgen.
Nach Abstimmung und Freigabe des Features werden die Spezifikationsanteile in die jeweiligen Spezifikationen übernommen und veröffentlicht.

1.1 Zielsetzung

Die in Konnektoren verbauten gSMC-K werden zum Zeitpunkt der Hardware-Produktion mit TI-Zertifikaten personalisiert. Gemäß gematik- und BSI-Vorgaben dürfen die Komponentenzertifikate ab dem Zeitpunkt des Abrufs maximal 5 Jahre gültig sein. Dadurch haben die Konnektoren eine maximal mögliche Lebensdauer von 5 Jahren. Unter Berücksichtigung der Lager- und Lieferzeiten fordert die gematik, dass die Konnektoren zum Zeitpunkt der Installation beim Leistungserbringer eine Restlaufzeit von mindestens 4 Jahren aufweisen müssen.
Die ersten Konnektoren für den Online Produktiv-Betrieb wurden in der zweiten Jahreshälfte 2017 produziert. Somit laufen deren Zertifikate bis Ende 2022 ab und werden dadurch ungültig.
Nach Ablauf der Zertifikate im Konnektor stehen die Funktionen des Konnektors nicht mehr zur Verfügung. Stand heute muss das Gerät rechtzeitig vor Ablauf der Zertifikate getauscht werden, um eine unterbrechungsfreie TI-Nutzung für die Leistungserbringer zu gewährleisten.

Das Feature "Laufzeitverlängerung gSMC-K" beschreibt eine technische Alternative zu einem Austausch der betroffenen Geräte.

1.2 Zielgruppe

Das Dokument richtet sich an Konnektor-Hersteller sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen, die im Rahmen des Features "Laufzeitverlängerung gSMC-K" relevant ist (betroffene Produkttypen: Konnektor PTV5, TSP X.509 Komponenten, TSP CVC Komponenten, VPN-Zugangsdienst, eHealth-Kartenterminal).

1.3 Abgrenzungen

In diesem Dokument sind nur die Festlegungen und Erläuterungen zum Feature "Laufzeitverlängerung gSMC-K" enthalten.
Die vollständige Anforderungslage für die Produkttypen ergibt sich aus den bekannten Konzept- und Spezifikationsdokumenten; diese sind in den Produkttypsteckbriefen der Produkttypen Konnektor PTV5, TSP X.509 Komponenten, TSP CVC Komponenten, VPN-Zugangsdienst und eHealth-Kartenterminal verzeichnet.

ENTWURF

1.4 Methodik

1.4.1 Anforderungen

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie 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 Afo-ID und Textmarke [<=] angeführten Inhalte.

1.4.2 Hinweise auf offene Punkte

Themen, die noch intern geklärt werden müssen oder eine Entscheidung seitens der Gesellschafter erfordern, sind wie folgt im Dokument gekennzeichnet:

Beispiel für einen offenen Punkt.

ENTWURF

2 Technisches Konzept Laufzeitverlängerung gSMC-K

2.1 Zusammenfassung

Die Abbildung 1 zeigt die vom Laufzeitende der gSMC-K-Zertifikate betroffenen Handlungsfelder im Überblick.

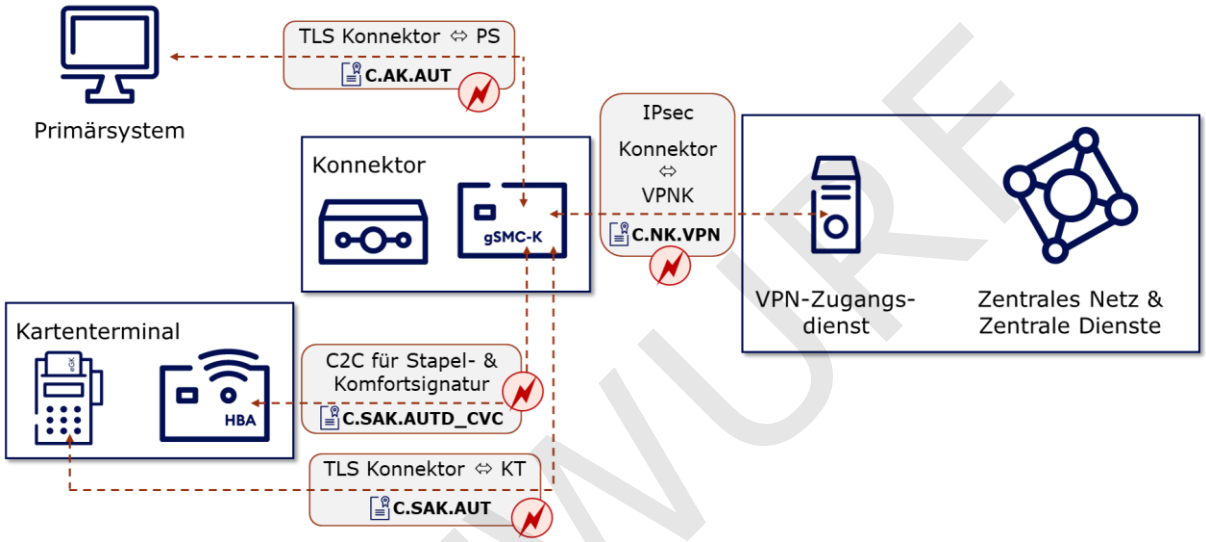

Abbildung 1 Betroffene Konnektor-Funktionalitäten und Zertifikate

Für die Lösung gelten übergreifende Rahmenbedingungen:

- Eine Verlängerung der Laufzeit darf nur während der Gültigkeit der ursprünglichen Karten-Zertifikate erfolgen.
- Die Verlängerung muss ein automatisierter Prozess mit einem Fallback bei Fehlern sein.
- Die Weiternutzung der bestehenden, zertifizierten Umsetzung kryptographischer Verfahren auf der gSMC-K wird angestrebt.
- Die Umsetzungs- und Zertifizierungsaufwände der Konnektor-Hersteller sollen möglichst klein sein.
- Eine implizite ECC-Migration soll nicht erfolgen.

Im folgenden wird der Lösungsansatz der gematik vorgestellt und in einen größeren Kontext eingeordnet.

2.1.1 Betroffene Komponenten und Zertifikate

Die gSMC-K enthält Schlüsselmaterial und Zertifikate für verschiedene Identitäten. Ein Teil davon sind die Geräteidentitäten des Konnektors, die von der gematik spezifiziert und im TI-Kontext gefordert sind; nur diese werden vom gematik-Konzept zur Laufzeitverlängerung der gSMC-K erfasst.
Darüber hinaus gibt es herstellerspezifisch genutzte Identitäten, die hier nicht

ENTWURF

Gegenstand der Betrachtung sind. Ob und wie herstellerspezifische Anteile der gSMC-K betroffen sind, und die Entscheidung, ob und welche Maßnahmen hierbei ergriffen werden, obliegt dem Konnektor-Hersteller.

Die Geräteidentität des Konnektors (Konnektoridentität) teilt sich in drei Identitäten auf:

1. **ID.NK.VPN** für den Netzkonnektor
   Die Identität des Netzkonnektors dient der Authentisierung gegenüber dem VPN-Konzentrator und zur Registrierung beim VPN-Zugangsdienst.
2. **ID.AK.AUT** für den Anwendungskonnektor
   Die Identität des Anwendungskonnektors dient der Authentisierung gegenüber den Clientsystemen im Rahmen von TLS-Verbindungen.
3. **ID.SAK.AUT** für die im Anwendungskonnektor enthaltene Signaturanwendungskomponente
   Die Identität des Signaturdienstes dient zur Authentisierung gegenüber den Kartenterminals.
4. Darüber hinaus muss sich der Signaturdienst des Konnektors gegenüber dem Heilberufsausweis mittels eines kartenverifizierbaren Zertifikats (**C.SAK.AUTD_CVC)** mit entsprechendem Profil ausweisen, um einen Trusted Channel für die Stapel- und Komfortsignaturen aufbauen zu können.

Nach Ablauf der gSMC-K-Zertifikate im Konnektor stehen wichtige Funktionen des Konnektors nicht mehr zur Verfügung:

- der IPsec-Verbindungsaufbau zum VPN-ZugD - C.NK.VPN
- der Aufbau von TSL gesicherten Verbindungen zu Clientsystemen (Primärsystemen) - C.AK.AUT
- die Use Cases Stapelsignatur und Komfortsignatur, für die C2C mit einem HBA benötigt wird - C.SAK.AUTD_CVC

2.1.2 Lösung

Die im Feld befindlichen Konnektoren werden per Firmware Update in die Lage versetzt, frische TI-Zertifikate für ihre alten Schlüssel der gSMC-K zu erhalten und zu verwenden. Der TSP X.509 nonQES für Komponenten stellt Zertifikate in der TI für den Abruf durch die Konnektoren bereit.

- Dazu werden die TSP-Komponenten für X.509 und CVC (beides Arvato) im Auftrag der Konnektor-Hersteller, die die Kartenherausgeber für die gSMC-K sind, frische Zertifikate für alle nicht gesperrten Zertifikate auf Basis der alten CSR Anträge oder der beim TSP vorliegenden Zertifikatsdaten erzeugen. Die Laufzeit der frischen Zertifikate endet am 31.12.2024.
- Die operative Umsetzung dieses Schritts soll zentral gesteuert per Auftrag der gematik an Arvato erfolgen.
- Die frischen Zertifikate werden dem TSP in einer eigens eingerichteten „Zertifikatssenke" innerhalb der TI für die Konnektoren zum Download via http bereitgestellt.
- Die Konnektoren werden so angepasst, dass sie frische Zertifikate für das auf der gSMC-K bestehende Schlüsselmaterial abrufen können, diese neuen Zertifikate in

ENTWURF

ihrem sicheren Speicher ablegen und es ab diesem Zeitpunkt statt der alten Zertifikate von der gSMC-K verwenden.

- Für die Verwendung gegenüber dem VPN-Zugangsdienst ist dafür eine Re-Registrierung mit dem frischen NK.VPN-Zertifikat notwendig.
- Für die neuen Zertifikate muss es ebenso Sperrprozesse geben wie für die alten Zertifikate. Solange beide Zertifikate zeitlich gültig sind, müssen auch beide Zertifikate gesperrt werden, wenn bspw. ein Konnektor als gestohlen gemeldet wird.

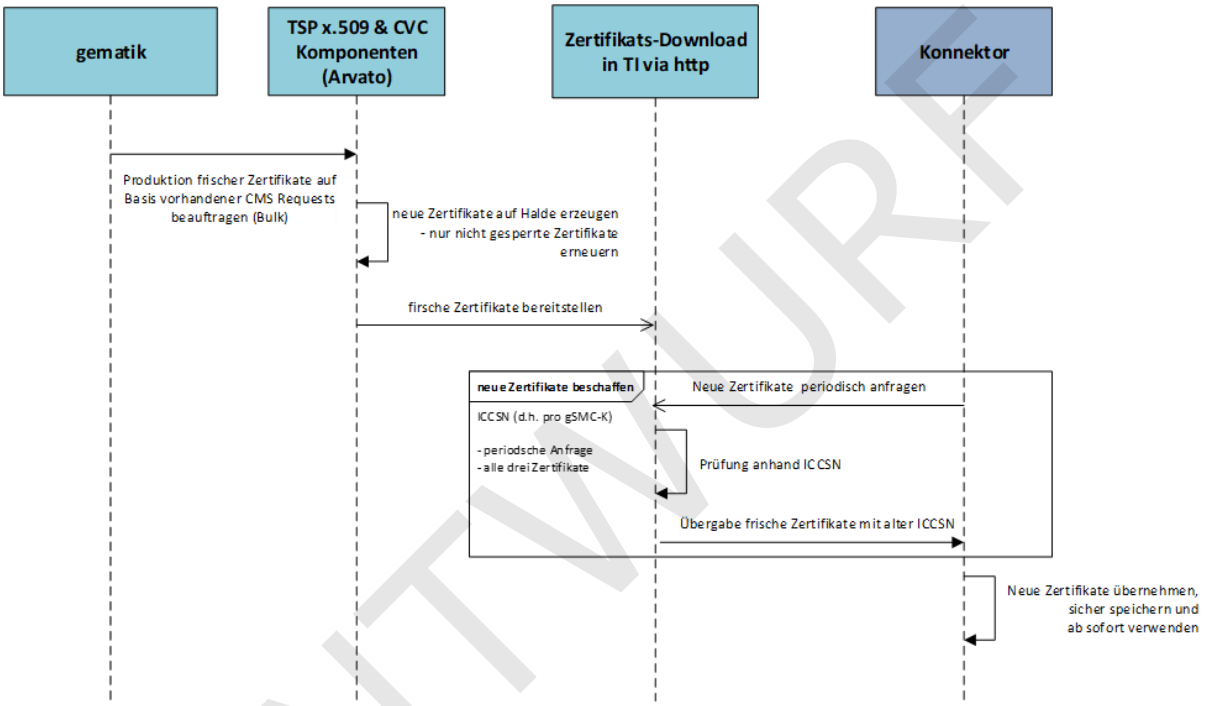

Abbildung 2 Überblick der Abfolge der Schritte zur Laufzeitverlängerung gSMC-K

2.1.3 Wiederholbarkeit der Aktion

Die Spezifikationen und die Implementierungen der Hersteller werden so gestaltet, dass die Aktion der Laufzeitverlängerung auch wiederholt werden kann.
Eine weitere Verlängerung ist nicht vorgesehen, soll jedoch rein technisch als "Notfall-Option" zur Verfügung stehen, falls der geplante Zeitraum bis Ende 2024 nicht ausreicht.
Eine zweite Laufzeitverlängerung darf nur nach Befürwortung durch das BSI erfolgen.

2.1.4 Zusammenspiel mit der ECC-Migration der Konnektoren

Die ECC-Migration der Konnektoren erfolgt unabhängig von der Laufzeitverlängerung der gSMC-K:

- ECC-Support für ePA steht ab Konnektor PTV4 zur Verfügung.

ENTWURF

- ECC-Support für alle kartenbasierten Anwendungsfälle ist ebenso ab PTV4 vorhanden.
- ECC für TLS und IPsec wird ab PTV5 vorhanden sein. (Anmerkung: Es ist geplant, diese Verpflichtung für PTV5 vor dem Hintergrund der rechtzeitigen Bereitstellung von ePA 2.0 entfallen zu lassen. Ein Änderungsantrag ist zur Zeit in der Freigabe)
- Eine vollständige ECC-Fähigkeit alter, insbesondere nicht-dual-personalisierter Konnektoren kann mit der erarbeiteten Lösung nicht erreicht werden, so dass diese Geräte vor Ende 2024 abgelöst werden müssen.

2.1.5 Bedeutung der Laufzeitverlängerung der gSMC-K für Robustheit, Akzeptanz und Zukunftsfähigkeit der TI

Mit dem Feature "Laufzeitverlängerung der gSMC-K" sollein großflächiger Konnektortausch vor der Verfügbarkeit einer Zukunftskonnektorlösung vermieden werden.
Die Lösung wurde so gestaltet, dass möglichst geringe Aufwände für die Umsetzung und Zertifizierung anfallen.

Im folgenden werden erst die jeweiligen Detailkonzepte der betroffenen Handlungsfelder beschrieben, bevor in Kapitel 4 die Spezifikations-Änderungen ausformuliert werden.

2.2 Identität ID.NK.VPN relevant für Konnektor - VPN-Zugangsdienst

Entsprechend der Lösungsbeschreibung in Kapitel 3.1 werden frische C.NK.VPN-Zertifikate vom TSP X.509 Komponenten erzeugt und gemeinsam mit den anderen zur gleichen ICCSN gehörigen Zertifikaten abgelegt.
Der Konnektor beginnt ab einem definierten Zeitpunkt vor Ablauf der gSMC-K-Zertifikate mit der Prüfung, ob frische Zertifikate für die ICCSN seiner gSMC-Ks vorhanden sind. Der Konnektor lädt die bereitgestellten frischen Zertifikate herunter und legt sie in seinem sicheren Speicher ab. Die frischen Zertifikate müssen ab diesem Zeitpunkt verwendet werden. Dazu muss die Registrierung mit dem frischen C.NK.VPN-Zertifikat erfolgen.

2.3 Identität ID.AK.AUT relevant für Konnektor - PS

Beim Verbindungsaufbau zwischen PS und Konnektor präsentiert der Konnektor dem PS das Zertifikat der Identität ID.AK.AUT von der gSMC-K. Dieses Zertifikat ist 5 Jahre gültig und wird nach den 5 Jahren von Primärsystemen nicht mehr akzeptiert. Ein PS wird dann keine gesicherte Verbindung zu solch einem Konnektor aufbauen können.

Bei einer erfolgreichen zentralen Erneuerung der Zertifikate der gSMC-K wird automatisch das erneuerte C.AK.AUT wie bisher verwendet (siehe A_21736). Bei Bedarf kann der Administrator alternativ jedoch nicht-TI-Zertifikate am Konnektor generieren und exportieren bzw. extern generieren und in den Konnektor importieren, so wie deren Verwendungsstartzeitpunkt definieren.

ENTWURF

2.3.1 Lösungsalternative: Export von im Konnektor generierten TI-fremden Zertifikaten

Um die Kommunikationsstrecke mit dem PS abzusichern, generiert ein Administrator über den Konnektor Schlüsselmaterial und Zertifikate. Das Zertifikat für den Konnektor kann dann aus dem Konnektor exportiert und dem PS-Client bekannt gemacht bzw. bei der ersten Kommunikation vom Nutzer des PS akzeptiert werden. Ab wann die neuen Zertifikate und Schlüssel vom Konnektor verwendet werden sollen, bestimmt der Administrator. Dieser Zeitpunkt ist losgelöst vom Generierungszeitpunkt.

2.3.2 Lösungsalternative: Import von extern generierten TI-fremden Zertifikaten

Um die Kommunikationsstrecke mit dem PS abzusichern, generiert ein Administrator Schlüsselmaterial und Zertifikate konnektorextern. In allen LE-Umgebungen, in denen z.B. eine KI betrieben wird, können Schlüsselmaterial und Zertifikate für den Konnektor über diese PKI generiert werden.

Der Konnektor importiert extern generiertes Schlüsselmaterial und Zertifikate. Das dem PS vom Konnektor präsentierte Zertifikat ist dem PS-Client entweder bereits bekannt (z.B. über die gemeinsame PKI) bzw. wird bei der ersten Kommunikation vom Nutzer des PS akzeptiert. Ab wann die neuen Zertifikate und Schlüssel vom Konnektor verwendet werden sollen, bestimmt der Administrator. Dieser Zeitpunkt ist losgelöst vom Generierungszeitpunkt.

2.4 Identität SAK.AUTD_CVC relevant für C2C mit HBA

Für die Verwendung von Stapel- und Komfortsignatur (SUK) bei der QES wird im Rahmen der CardToCard-Authentisierung (C2C) zwischen HBA und dem Konnektor die Identität **SAK.AUTD_CVC** der gSMC-K verwendet. Die vom HBA verwendete Identität ist HPC.AUTD_SUK_CVC.

Bei HBA-G2.0-Karten wird für die mehrfache QES-Signatur mit einer einzigen PIN-Eingabe (also SUK) eine Freischaltung des HBA mittels C2C und Aufbau eines Trusted Channel (SE#2) zwischen gSMC-K und HBA für die Übertragung der zu signierenden Daten gefordert.
Die technische Notwendigkeit der C2C und des Trusted Channel für die SUK entfällt bei HBA G2.1. Um das Sicherheitsniveau für QES zu erfüllen, wird jedoch weiterhin ein Trusted Channel für die QES-Stapel- und Komfortsignatur gefordert werden.

Durch die „Innere Uhr" der Karten (Parameter *pointInTime* des COS) ergibt sich bei einer längeren Nutzung von CV-Zertifikaten über deren Gültigkeitszeitraum hinaus das Risiko, dass in bestimmten Szenarien das C2C fehlschlägt. Im konkreten Szenario könnte ein HBA ein zu altes gSMC-K-Zertifikat ablehnen und somit wäre dann keine Stapel- und Komfortsignatur mehr möglich. Daher muss das Zertifikat nach 5 Jahren ersetzt werden.

Entsprechend der Lösungsbeschreibung in Kapitel 3.1 werden frische SAK.AUTD_CVC-Zertifikate vom TSP CVC Komponenten erzeugt und gemeinsam mit den anderen zur gleichen ICCSN gehörigen Zertifikaten abgelegt. Der Konnektor beginnt ab einem definierten Zeitpunkt vor Ablauf der gSMC-K-Zertifikate mit der Prüfung, ob frische Zertifikate für die ICCSN seiner gSMC-Ks vorhanden sind.

ENTWURF

Der Konnektor lädt die bereitgestellten frischen Zertifikate herunter und legt sie in seinem sicheren Speicher ab. Die frischen Zertifikate müssen ab diesem Zeitpunkt verwendet werden.

2.5 Identität ID.SAK.AUT relevant für eHealth-Kartenterminal

Die Identität ID.SAK.AUT auf der gSMC-K ist die im Anwendungskonnektor (AK) genutzte Identität für die Signaturanwendungskomponente (SAK) des Konnektors. Sie dient zur Authentisierung gegenüber den Kartenterminals.
Bisher haben die eHealth-Kartenterminals keine Uhr, gegen die ein Zertifikats-Ende-Datum geprüft werden könnte. Daher wird für das Kartenterminal beim Verifizieren des Konnektor-SAK-Zertifikats momentan auch keine Prüfung des Laufzeit-Endes gefordert.

Das Zertifikat C.SAK.AUT der gSMC-K wird dennoch erneuert und verwendet. Dies soll zur Absicherung der Robustheit dienen, falls Kartenterminals mit Uhren zukünftig zugelassen werden. (Zukunftsfähigkeit). Da die Kartenterminals für die Pairing-Informationen genau nur den öffentlichen Schlüssel des Konnektor-Zertifikats speichern und sich dieser nicht unterscheidet zwischen alten und erneuertem C.SAK.AUT, ist die automatisch Nutzung des neuen Zertifikats im Feld problemlos möglich.

ENTWURF

3 Operative Umsetzung

3.1 Bereitstellung der Zertifikatssenke

Arvato als TSP Komponenten (für x.509 und CVC) wird von der gematik beauftragt, die Zertifikatssenke zur Benutzung durch die Konnektoren, bereitzustellen.
Neben der Bereitstellung des Downloadpunkts mit den Zertifikatspaketen, müssen auch alle operativen Bedingungen gegeben sein, wie beispielsweise Firewall-Freischaltungen.

Datum	Meilenstein	Anmerkungen/ weitere Bedingungen
01.07.2021	Start Beauftragung Arvato	
15.11.2021	Zertifikatssenke und Zertifikate in RU und TU verfügbar	(ggf. Termin staffeln: 01.11. Senke + 15.11. Zertifikatspakete) Die Paketierung und Addressierung muss genauso wie für die PU gestaltet sein. Zusätzlich soll sichergestellt werden, dass der gematik für Testzwecke zeitnah (2-3 Tage) frische Zertifikate wiederholt zur Verfügung gestellt werden (Downloadpunkt und OCSP).
15.02.2022	Zertifikatssenke und Zertifikate in PU verfügbar	auch hier ggf. Termin staffeln (01.02.2022 Senke + 15.02. Zertifikatspakete)

3.2 Bereitstellung der Zertifikate

Die gematik wird Arvato als TSP Komponenten (für x.509 und CVC) beauftragen, die frischen Zertifikate für alle bis dato ausgeführten CSRs für gSMC-K-Zertifikate auf Kosten der gematik zu erzeugen.

3.3 Sperrprozesse

Für alle ausgestellten Zertifikate (auch für die erneuerten) werden Sperr-Informationen vom OCSP-Responder der Komponenten-PKI bereitgestellt. Dies ist in TIP1-A_3627 für

ENTWURF

die Zertifikats-Typen der gSMC-K festgelegt und gilt somit auch für die erneuerten Zertifikate.

Offener Punkt: Zur Zeit erfolgt der Sperrprozess über die Zertifikats-Seriennummer, daher benötigen die Konnektor-Hersteller die Info zur Seriennummer.
OI: Wie bekommen die Hersteller die Information über die neuen Seriennummern?

3.4 Offline Konnektoren

Es kann vorkommen, dass Konnektoren dauerhaft offline sind (z.B. Reserve insbesondere in Krankenhäusern). Für diese Konnektoren ist die skizzierte Lösung nur geeignet, wenn sie rechtzeitig vor Ablauf der Zertifikate online genommen werden.

Offener Punkt: Zusätzlich wird erwogen, ob die Möglichkeit geschaffen werden kann, dass ein Admin manuell frische gSMC-K-Zertifikate einbringt, ggf. auch nach Ablauf der ursprünglichen Zertifikate.

ENTWURF

4 Spezifikation

4.1 Änderungen in gemSpec_Kon

4.1.1 (3.1) Konnektoridentität und gSMC-K

4.1.2 (3.1.1) Erneuerung der Zertifikate der gSMC-K

A_21736 - Verwendung erneuerter Zertifikate
Nach erfolgreicher Zertifikatserneuerung MUSS der Konnektor vor Ablauf der alten Zertifikate an allen Stellen, wo er die Zertifikate C.NK.VPN, C.AK.AUT, C.SAK.AUT, C.SAK.AUTD_CVC und C.CA_SAK.CS verarbeitet, die neuen Zertifikate verwenden, es sei denn die Spezifikation trifft andere Festlegungen. **[<=]**

A_21744 - Zertifikate regelmäßig erneuern
Der Konnektor MUSS die Zertifikate C.NK.VPN, C.AK.AUT, C.SAK.AUT, C.SAK.AUTD_CVC und C.CA_SAK.CS regelmäßig erneuern. Der Konnektor MUSS 180 Tage vor Ablauf des aktuell verwendeten C.NK.VPN-Zertifikats den Zertifikatserneuerungsprozess anstoßen. Solange die Zertifikate noch nicht vollständig erfolgreich erneuert wurden, MUSS der Konnektor genau einmal täglich durch Aufruf von TUC_KON_410 neue Zertifikate beziehen.

[<=]

A_21749 - TUC_KON_410 „gSMC-K-Zertifikate aktualisieren"
Der Konnektor MUSS den technischen Use Case TUC_KON_410 „gSMC-K-Zertifikate aktualisieren" umsetzen.

Tabelle 1: TAB_KON_930 – TUC_KON_410 „Zertifikate aktualisieren"

Element	Beschreibung
Name	TUC_KON_410 "gSMC-K-Zertifikate aktualisieren"
Beschreibung	Dieser TUC bezieht neue gSMC-K-Zertifikate vom Downloadpunkt des TSP X.509 nonQES für Komponenten.
Auslöser	A_21744, Administrator
Vorbedingungen	MGM_LU_ONLINE=Enabled Verbindung zum VPN-Konzentrator TI ist aufgebaut.
Eingangsdaten	Keine
Komponenten	Konnektor, TSP Komponenten

ENTWURF

Ausgangsdaten	Keine

Standardablauf	1. Für jede verbaute gSMC-K wird die zip-Datei mit neuen Zertifikaten per HTTP vom Downloadpunkt TSP Komponenten bezogen ([gemSpec_X.509_TSP#A_21770]).
	2. Die zip-Dateien werden entpackt.
	3. Für jedes bezogene Zertifikat führt der Konnektor folgende Prüfungen durch:
	a. ICCSN des neuen und alten Zertifikats sind gleich
	b. Ablaufdatum des neuen Zertifikats liegt nach Ablaufdatum des alten Zertifikats
	c. Kryptografische Prüfung, dass öffentlicher Schlüssel zum privaten Schlüssel passt
	d. Neue Zertifikatsseriennummer ungleich alter Zertifikatsseriennummer
	e. Für C.NK.VPN-Zertifikat: OCSP-Abfrage gemäß GS-A_4657-03
	4. Erfolgreich geprüfte Zertifikate werden im sicheren Speicher abgelegt und zur Verwendung vorgemerkt.
	Alte Zertifikate im sicheren Speicher werden dabei überschrieben (falls vorhanden).
	5. TUC_KON_256 {
	topic = „SMC_K/UPDATE/SUCCESS“;
	eventType = Op;
	severity = Info;
	parameters = „$Parameters“;
	doLog = true;
	doDisp = true }

Varianten/Alternativen	Keine

ENTWURF

Fehlerfälle	(->1) Fehler beim Download:
	TUC_KON_256 {
	topic = „SMC_K/DOWNLOAD/ERROR";
	eventType = Op;
	severity = Error;
	parameters = „$Parameters";
	doLog = true;
	doDisp = true }
	(->3) Wenn eine der folgenden Prüfungen fehlschlägt, wird das bezogene Zertifikat verworfen und mit dem nächsten fortgesetzt:
	(-> 3a) ICCSN nicht gleich: Fail=Iccsn
	(-> 3b) Neues Ablaufdatum nicht später als altes Ablaufdatum: Fail=Date
	(-> 3c) Öffentlicher Schlüssel passt nicht zum privaten Schlüssel: Fail=Crypt
	(-> 3e) Zertifikat gesperrt oder unknown: Fail=Ocsp
	TUC_KON_256 {
	topic = „SMC_K/UPDATE/ERROR";
	eventType = Op;
	severity = Error;
	parameters = „$Parameters";
	doLog = true;
	doDisp = true }
	(->3) Wenn eine der folgenden Prüfungen fehlschlägt, wird das bezogene Zertifikat trotzdem zur Verwendung vorgemerkt:
	(-> 3d) Zertifikatsseriennummer identisch: Fail=Serial
	Warnung wird protokolliert

Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 2: Tab_Kon_931 Fehlercodes TUC_KON_410 „gSMC-K-Zertifikate aktualisieren"

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
herstellerspezifisch			

[<=]

A_21780 - Nutzerhinweis bezüglich Fehler bei Zertifikatserneuerung
Der Hersteller des Konnektors MUSS in seinem Handbuch den Nutzer/Administrator darauf hinweisen, dass die Ereignisse mit dem Topic=SMC_K/UPDATE/ERROR und dem Topic=SMC_K/DOWNLOAD/ERROR dringend durch das Primärsystem abonniert werden sollten und dass der Nutzer/Administrator sich bei Auftreten des Fehlers unverzüglich mit

ENTWURF

dem Hersteller in Verbindung setzen muss.
[<=]

4.1.3 (3.3) Betriebszustand

TIP1-A_4512-03 - Ereignis bei Änderung des Betriebszustandes
Der Konnektor MUSS per Ereignisdienst TUC_KON_256 über Änderungen des Betriebszustandes (Tabelle TAB_KON_503 Betriebszustand_Fehlerzustandsliste) informieren.
Der Konnektor muss dazu für jeden Fehlerzustand $EC mit Error Condition $EC.errorcondition mit verändertem Wert $EC.value den technischen Anwendungsfall TUC_KON_256 „Systemereignis absetzen" mit folgenden Parametern aufrufen:

```
TUC_KON_256 {
   topic = "OPERATIONAL_STATE/$EC.errorcondition";
   eventType = $EC.type;
   severity = $EC.severity;
   parameters = („Value=$EC.value, $EC.parameterlist")
}
```

Tabelle 3: TAB_KON_503 Betriebszustand_Fehlerzustandsliste

ErrorCondition (siehe Hinweis 1)	Beschreibung	Type	Severity	max. Feststellungs-zeit	Parameterlist (siehe Hinweis 2)
EC_CardTerminal_ Software_Out_Of_ Date ($ctId)	Software auf Kartenterminal($ctId) ist nicht aktuell	Op	Info	1 day	CtID=$ctId; Bedeutung= $EC.description
EC_CardTerminal_ gSMC-KT_Certificate_ Expires_Soon ($ctId)	Das Zertifikat der gSMC-KT im Kartenterminal($ctId) läuft in weniger als 5 Wochen ab	Op	Info	7 days	CtID=$ctId; Bedeutung= $EC.description
EC_Connector_ Software_Out_ Of_Date	I_KSRS_Download::list_ Updates liefert mindestens eine UpdateInformation mit einer UpdateInformation/Firmware/ FWVersion > aktuelle Version der Konnektorsoftware, deren UpdateInformation/Firmwa	Op	Info	1 day	Bedeutung= $EC.description

ENTWURF

	re/ FWPriority = „Kritisch“				
EC_FW_Update_Available	I_KSRS_Download::list_Updates liefert mindestens eine UpdateInformation mit einer UpdateInformation/Firmware/ FWVersion > aktuelle Version der Konnektor- oder Kartenterminalsoftware	Op	Info	1 day	Bedeutung= $EC.description
EC_FW_Not_Valid_Status_Blocked	Konnektor Firmware muss aktualisiert werden. Zugang zur TI momentan nicht erlaubt.	Sec	Fatal	1 day	Bedeutung= $EC.description
EC_Time_Sync_Not_Successful	der letzte Synchronisationsversuch der Systemzeit war nicht erfolgreich.	Op	Info	1 sec	LastSyncAttempt= $lastSyncAttempt Timestamp; LastSyncSuccess =$lastSyncSuccess Timestamp; Bedeutung= $EC.description
EC_TSL_Update_Not_Successful	das letzte Update der TSL war nicht erfolgreich.	Op	Info	1 sec	Bedeutung= $EC.description; LastUpdateTSL= $lastUpdateTSL Timestamp
EC_TSL_Expiring	Systemzeit t mit t > NextUpdate-Element der TSL – 7 Tage und t <= NextUpdate-Element der TSL	Sec	Info	1 day	NextUpdateTSL =$NextUpdate-Element der TSL; Bedeutung= $EC.description
EC_BNetzA_VL_Update_Not_Successful	Das letzte Update der BNetzA-VL war nicht erfolgreich	Op	Info	1 sec	LastUpdateBNetzAVL= $lastUpdateBNetzAVLTimestamp; Bedeutung= $EC.description

ENTWURF

EC_ BNetzA_VL_ not_valid	Systemzeit t mit t > NextUpdate-Element der BNetzA-VL	Sec	Warning	1 day	NextUpdateBNetzAVL =$NextUpdate-Element der BNetzA-VL; Bedeutung= $EC.description
EC_TSL_Trust_ Anchor_Expiring	Gültigkeit des Vertrauensankers ist noch nicht abgelaufen, läuft aber innerhalb von 30 Tagen ab.	Sec	Info	1 day	ExpiringDateTrustAnchor= Ablaufdatum der Vertrauensanker gültigkeit; Bedeutung= $EC.description
EC_LOG_ OVERFLOW	Wenn im Rahmen der Regeln für die rollierende Speicherung von Logging-Einträgen Einträge gelöscht werden, die nicht älter als SECURITY_LOG_DAYS, LOG_DAYS bzw. FM_<fmName>_LOG_DAYS sind, tritt der Fehlerzustand ein. Der Fehlerzustand kann nur durch einen Administrator wieder zurückgesetzt werden. Unter Protokoll wird die Liste der auslösenden Protokolle angegeben.	Op	Warning	1 sec	Protokoll=$Protokoll; Bedeutung= $EC.description
EC_CRL_Expiring	Systemzeit t > NextUpdate der CRL – 3 Tage	Sec	Warning	1 day	ExpiringDateCRL= NextUpdate der CRL; Bedeutung= $EC.description

ENTWURF

EC_Time_Sync_ Pending_Warning	MGM_LU_ONLINE=Enabled und keine erfolgreiche Synchronisation der Systemzeit seit d Tagen und d > NTP_WARN_PERIOD und d <= NTP_GRACE_PERIOD. Nach einer Korrektur oder Bestätigung der Systemzeit durch einen Administrator muss der Konnektor wie nach einer erfolgreichen Zeitsynchronisation verfahren, d.h., der Tagezähler wird auf 0 zurückgesetzt.	Sec	Warning	1 day	LastSyncSuccess=$lastSyncSuccessTimestamp; Bedeutung=$EC.description
EC_TSL_Out_ Of_Date_Within_ Grace_Period	Systemzeit t mit t > NextUpdate-Element der TSL und t <= NextUpdate-Element der TSL + CERT_TSL_ DEFAULT_GRACE_ PERIOD_DAYS und eine neue TSL ist nicht verfügbar	Sec	Warning	1 day	NextUpdateTSL =$NextUpdate-Element der TSL; GracePeriodTSL =CERT_TSL_ DEFAULT_ GRACE_PERIOD_ DAYS; Bedeutung=$EC.description
EC_CardTerminal_ Not_Available ($ctId)	Kartenterminal($ctId) ist nicht verfügbar. Dieser Betriebszustand bezieht sich auf die als „aktiv" gekennzeichneten KTs.	Op	Error	1 sec	CtID=$ctId; Bedeutung=$EC.description
EC_No_VPN_TI_ Connection	Kein sicherer Kanal (VPN) in die Telematikinfrastruktur aufgebaut. Der Wert 300 sec ist abgeleitet aus der maximalen Verbindungsaufbauzeit bei einem Standortausfall des VPN-Zugangsdienstes.	Op	Error	300 sec	Bedeutung=$EC.description

ENTWURF

EC_No_VPN_ SIS_Connection	Kein sicherer Kanal (VPN) zu den Sicheren Internet Services aufgebaut. Der Wert 300 sec ist abgeleitet aus der maximalen Verbindungsaufbauzeit bei einem Standortausfall des VPN-Zugangsdienstes.	Op	Error	300 sec	Bedeutung= $EC.description
EC_No_Online_ Connection	Konnektor kann Dienste im Transportnetz nicht erreichen.	Op	Error	10 sec	Bedeutung= $EC.description
EC_IP_Adresses_ Not_Available	Die IP-Adressen des Netzkonnektors sind nicht oder falsch gesetzt.	Sec	Error	1 sec	Bedeutung= $EC.description
EC_CRL_Out_Of_ Date	Systemzeit t > Next Update der CRL	Sec	Fatal	1 day	NextUpdateCRL= $NextUpdate der CRL; Bedeutung= $EC.description
EC_Firewall_Not_ Reliable	Firewall-Regeln konnten nicht fehlerfrei generiert werden oder beim Laden der Firewall-Regeln ist ein Fehler aufgetreten.	Sec	Fatal	1 sec	Bedeutung= $EC.description
EC_Random_ Generator_ Not_Reliable	Der Zufallszahlengenerator kann die Anforderungen an die zu erzeugende Entropie nicht erfüllen.	Sec	Fatal	1 sec	Bedeutung= $EC.description
EC_Secure_ KeyStore_ Not_Available	Sicherer Zertifikats- und Schlüsselspeicher des Konnektors (gSMC-K oder Truststore) nicht verfügbar	Sec	Fatal	1 sec	Bedeutung= $EC.description

ENTWURF

EC_Security_ Log_ Not_Writable	Das Sicherheitslog kann nicht geschrieben werden.	Op	Fatal	1 sec	Bedeutung= $EC.description
EC_Software_ Integrity_ Check_Failed	Eine oder mehrere konnektorinterne Integritätsprüfungen der aktiven Konnektorbestandteile sind fehlgeschlagen.	Sec	Fatal	1 day	Bedeutung= $EC.description
EC_Time_ Difference_ Intolerable	Abweichung zwischen der lokalen Zeit und der per NTP empfangenen Zeit bei der Zeitsynchronisation größer als NTP_MAX_ TIMEDIFFERENCE. Nach einer Korrektur oder Bestätigung der Systemzeit durch einen Administrator muss der Konnektor den Fehlerzustand zurücksetzen.	Sec	Fatal	1 sec	NtpTimedifference= Zeitabweichung; NtpMaxAllowed Timedifference =NTP_MAX_ TIMEDIFFERENCE; Bedeutung= $EC.description
EC_Time_Sync_ Pending_Critical	MGM_LU_ONLINE= Enabled und keine erfolgreiche Synchronisation der Systemzeit seit d Tagen und d > NTP_GRACE_PERIOD Nach einer Korrektur oder Bestätigung der Systemzeit durch einen Administrator muss der Konnektor wie nach einer erfolgreichen Zeitsynchronisation verfahren, d.h., der Tagezähler wird auf 0 zurückgesetzt.	Sec	Fatal	1 day	LastSyncSuccess =$lastSync SuccessTimestamp; NtpGracePeriod= NTP_GRACE_ PERIOD; Bedeutung= $EC.description
EC_TSL_Trust_ Anchor_ Out_Of_Date	Gültigkeit des Vertrauensankers ist abgelaufen	Sec	Fatal	1 day	ExpiringDateTrust Anchor= Ablaufdatum der Vertrauensanker gültigkeit; Bedeutung= $EC.description

ENTWURF

EC_TSL_Out_ Of_Date_ Beyond_Grace_ Period	Systemzeit t mit t > NextUpdate-Element der TSL + CERT_TSL_DEFAULT_ GRACE_ PERIOD_DAYS und eine neue TSL ist nicht verfügbar	Sec	Fatal	1 day	NextUpdateTSL =$NextUpdate-Element der TSL; GracePeriodTSL =CERT_TSL_ DEFAULT_ GRACE_PERIOD_ DAYS; Bedeutung= $EC.description
EC_ CRYPTOP ERATION_ ALARM	Gemäß TIP1-A_4597 wurde ein potentieller Missbrauch einer Kryptooperation erkannt. Nur der Administrator kann die Alarmmeldung zurücksetzen.	Sec	War ning	1 min	Operation= $Operationsname; Count=$Summenwe rt; Arbeitsplatz= $<Liste operationsaufrufend en workplaceIDs>; Meldung= 'Auffällige Häufung von Operationsaufrufen in den letzten 10 Minuten'
EC_OTHER_ ERROR_ STATE($no)	Herstellerspezifische Fehlerzustände, die per $no (von 1 aufsteigend nummeriert) identifiziert werden. $Type, $Severity und $ParameterList legt der Hersteller nach Bedarf fest.	$Typ e	$Sev erity	<= 1 day	Bedeutung= $EC.description
EC_NK_Certificate_Ex piring	Das C.NK.VPN-Zertifikat läuft bald ab. Systemzeit t > (Ablaufdatum von C.NK.VPN – 180 Tage)	Sec	Warni ng	1 day	Iccsn=$Iccsn; Serial=$Serialnu mber; Bedeutung= $EC.description

ENTWURF

EC_NK_Certificate_Expired	Das C.NK.VPN-Zertifikat ist abgelaufen. Systemzeit t > Ablaufdatum von C.NK.VPN	Sec	Fatal	1 day	Iccsn=$Iccsn; Serial=$Serialnumber; Bedeutung= $EC.description

Erläuterungen zu TAB_KON_503:

Hinweis 1:
Jeder Fehlerzustand wird durch einen eindeutigen ErrorCondition identifiziert. Dieser kann einen Parameter enthalten. Sind etwa die Kartenterminals mit ctId=47 und das mit ctId=93 nicht erreichbar, so lauten die ErrorCondition „EC_CardTerminal_Not_Available(47)" und „EC_CardTerminal_Not_Available(93)".

Hinweis 2:
EC.description referenziert den Text, der in der Spalte „Beschreibung" des Zustandes spezifiziert wurde.

[<=]

TIP1-A_4510-04 - Sicherheitskritische Fehlerzustände
Der Konnektor MUSS bei eingetretenem Fehlerzustand aus Tabelle Tab_ Kon_503 Betriebszustand_Fehlerzustandsliste mit Severity=Fatal dafür sorgen, dass von den Operationen der Basisdienste und Technische Use Cases (TUCs) der Basisdienste, die relevant für Fachanwendungen sind, nur erlaubte Operationen und TUCs gestartet und ausgeführt werden.
Welche Operationen und TUCs je eingetretenem Fehlerzustand ausgeführt werden dürfen, legt Tabelle „TAB_KON_504 Ausführungserlaubnis für Dienste in kritischen Fehlerzuständen" fest: Jede Erlaubnis ist dort durch ein „x" definiert.
Abweichend zu Angaben in der Tabelle TAB_KON_504 DÜRFEN folgende Operationen und TUCs NICHT im Zustand EC_Firewall_Not_Reliable ausgeführt werden:

- TUC_KON_000 PrüfeAufrufkontext
- TUC_KON_041 Einbringen der Endpunktinformationen während der Bootup-Phase
- GetCardTerminals
- GetCards
- GetResourceInformation
- Subscribe
- RenewSubscription
- Unsubscribe
- GetSubscription
- ReadCardCertificate
- CheckCertificateExpiration
- VerifyCertificate

Sind mehrere Fehlerzustände gleichzeitig eingetreten, dürfen nur die Operationen und TUCs ausgeführt werden, die für alle eingetretenen Fehlerzustände erlaubt sind. Der Konnektor MUSS Anfragen, die auf Grund eines kritischen Fehlerzustandes nicht

ENTWURF

ausgeführt oder abgebrochen werden, mit einem Fehler (Fehlercode 4002) beantworten.

Tabelle 4: TAB_KON_502 Fehlercodes „Betriebszustand"

Fehlercode	ErrorType	Severity	Fehlertext
4002	Security	Fatal	Der Konnektor befindet sich in einem kritischen Betriebszustand

[<=]

Tabelle 5: TAB_KON_504 Ausführungserlaubnis für Dienste in kritischen Fehlerzuständen

	EC_Software_Integrity_Check_Failed	EC_Random_Generator_Not_Reliable	EC_Security_Log_Not_Writable	EC_Time_Sync_Pending_Critical	EC_Time_Difference_Intolerable	EC_CRL_Out_Of_Date	EC_TSL_Out_Of_Date_Beyond_Grace_Period	EC_TSL_Trust_Anchor_Out_Of_Date	EC_Secure_Key_Store_Not_Available	EC_FW_Not_Valid_Status_Blocked	EC_gSMC_K_Expired
Technische Use Cases (TUCs) der Basisdienste relevant für Fachanwendung und die Kommunikation mit Weiteren Anwendungen und SIS											
Zugriffsberechtigungsdienst											
TUC_KON_000 Prüfe Zugriffsberechtigung	-	x	x	x	x	x	x	x	x	x	x
Dienstverzeichnisdienst											
TUC_KON_041 Einbringen der Endpunktnformationen während der Bootup-Phase	-	-	-	x	x	x	x	x	x	x	x

ENTWURF

Kartenterminaldienst											
TUC_KON_051 Mit Anwender über Kartenterminal interagieren	-	-	-	-	-	x	x	x	-	x	-
Kartendienst											
TUC_KON_005 Card-to-Card authentisieren	-	-	-	-	-	x	x	x	-	x	-
TUC_KON_006 Datenzugriffsaudit eGK schreiben	-	-	-	-	-	x	x	x	-	x	-
TUC_KON_018 eGK-Sperrung prüfen	-	-	-	-	-	x	x	x	-	x	-
TUC_KON_024 Karte zurücksetzen	-	-	-	-	-	x	x	x	-	x	-
TUC_kON_026 Liefere CardSession	-	-	-	-	-	x	-	x	-	-	-
TUC_KON_200 SendeAPDU	-	-	-	-	-	x	x	x	-	x	-
TUC_KON_202 LeseDatei	-	-	-	-	-	x	x	x	-	x	-
TUC_KON_203 SchreibeDatei	-	-	-	-	-	x	x	x	-	x	-
TUC_KON_209 LeseRecord	-	-	-	-	-	x	x	x	-	x	-
Systeminformationsdienst											
TUC_KON_256 Systemereignis absetzen	-	x	x	x	x	x	x	x	x	x	x
Verschlüsselungsdienst											

ENTWURF

TUC_KON_072 Daten symmetrisch verschlüsseln	-	-	-	x	x	x	x	x	-	x	-
TUC_KON_073 Daten symmetrisch entschlüsseln	-	-	-	x	x	x	x	x	-	x	-
Zertifikatsdienst											
TUC_KON_034 Zertifikatsinformationen extrahieren	-	-	-	x	x	x	x	x	-	x	x
Protokollierungsdienst											
TUC_KON_271 Schreibe Protokolleintrag	-	x	x	x	x	x	x	x	x	x	x
TLS-Dienst											
TUC_KON_110 Kartenbasierte TLS-Verbindung aufbauen	-	-	-	-	-	-	-	-	-	-	-
Verbindung zum VPN-Konzentrator											
TUC_VPN-ZD_0001 „IPsec Tunnel TI aufbauen”	-	-	-	-	-	-	-	-	-	-	-
TUC_VPN-ZD_0002 „IPsec Tunnel SIS aufbauen”	-	-	-	-	-	-	-	-	-	-	-
Operationen der Basisdienste											
Kartendienst											
VerifyPin	-	-	-	-	-	x	x	x	-	x	-
UnblockPin	-	-	-	-	-	x	x	x	-	x	-
ChangePin	-	-	-	-	-	x	x	x	-	x	-

ENTWURF

	GetPinStatus	-	-	-	-	-	x	x	x	-	x	-
Systeminformationsdienst												
	Schnittstelle der Ereignissenke	-	x	x	x	x	x	x	x	x	x	x
	GetCardTerminals	-	x	x	x	x	x	x	x	x	x	-
	GetCards	-	x	x	x	x	x	x	x	x	x	-
	GetResourceInformation	-	x	x	x	x	x	x	x	x	x	-
	Subscribe	-	x	x	x	x	x	x	x	x	x	-
	RenewSubscription	-	x	x	x	x	x	x	x	x	x	-
	Unsubscribe	-	x	x	x	x	x	x	x	x	x	-
	GetSubscription	-	x	x	x	x	x	x	x	x	x	-
Verschlüsselungsdienst												
	EncryptDocument	-	-	-	-	-	x	x	x	-	x	-
	DecryptDocument	-	-	-	-	-	x	x	x	-	x	-
Signaturdienst												
	SignDocument	-	-	-	-	-	x	x	x	-	x	-
	VerifyDocument	-	-	-	-	-	x	x	x	-	x	-
	GetJobNumber	-	-	-	-	-	x	x	x	-	x	-
	StopSignature	-	-	-	-	-	x	x	x	-	x	-
	ActivateComfortSignature	-	-	-	-	-	x	x	x	-	x	-
	DeactivateComfortSignature	-	-	-	-	-	x	x	x	-	x	-
	GetSignatureMode	-	-	-	-	-	x	x	x	-	x	-

ENTWURF

Authentifizierungsdienst											
	ExternalAuthenticate	-	-	-	-	-	x	x	x	-	x	-
Zertifikatsdienst											
	ReadCardCertificate	-	-	-	-	-	x	x	x	x	x	-
	CheckCertificateExpiration	-	-	-	-	-	x	x	x	x	x	-
	VerifyCertificate	-	-	-	-	-	x	-	x	x	x	-
Zeitdienst											
	I_NTP_Time_Information	-	-	-	-	-	x	x	x	x	-	-
Konnektormanagement											
	Softwareaktualisierung	x	x	x	x	x	x	x	x	x	x	x
	Protokolleinsicht	x	x	x	x	x	x	x	x	x	x	x
	Werksreset	x	x	x	x	x	x	x	x	x	x	x
	Sonstiges	-	x	x	x	x	x	x	x	x	x	x

ENTWURF

4.1.4 (4.3.5) Neustart und Werksreset

folgende Anforderung wird im Kapitel 4.3.5 ergänzt

A_21743 - Laufzeitverlängerung gSMC-K: Erneuerte Zertifikate nach Werksreset verwenden
Der Konnektor, dessen gSMC-K-Zertifikate erneuert wurden, MUSS auch nach einem Werksreset die erneuerten Zertifikate verwenden.**[<=]**

4.1.5 Identität ID.NK.VPN relevant für Konnektor - VPN-Zugangsdienst

4.1.5.1 (4.3.7) Re-Registrierung des Konnektors mit neuem NK-Zertifikat

A_21745 - Re-Registrierung mit neuem NK-Zertifikat durchführen
Nach einer vollständigen erfolgreichen Zertifikatserneuerung über TUC_KON_410 MUSS der Konnektor eine Re-Registrierung mit dem neuen Zertifikat beim Registrierungsdienst des VPN-Zugangsdienstes durchführen. Solange nach Bezug eines neuen C.NK.VPN-Zertifikats noch keine erfolgreiche Re-Registrierung durchgeführt wurde, MUSS der Konnektor genau einmal täglich TUC_KON_411 aufrufen.**[<=]**

A_21758 - TUC_KON_411 „Konnektor mit neuem NK-Zertifikat registrieren“
Der Konnektor MUSS den technischen Use Case TUC_KON_411 "Konnektor mit neuem NK-Zertifikat registrieren" umsetzen.

Tabelle 6: TAB_KON_932 – TUC_KON_411 „Konnektor mit neuem NK-Zertifikat registrieren“

Element	Beschreibung
Name	TUC_KON_411 "Konnektor mit neuem NK-Zertifikat registrieren"
Beschreibung	Dieser TUC führt eine Deregistrierung mit dem alten und eine Neuregistrierung mit dem neuen NK-Zertifikat durch.
Auslöser	A_21745, Administrator
Vorbedingungen	Keine
Eingangsdaten	Keine
Komponenten	Konnektor, VPN-ZugD
Ausgangsdaten	Keine

ENTWURF

Standardablauf	1. Der Konnektor ermittelt die URI des Registrierungsservers (MGM_ZGDP_REGSERVER) durch eine DNS-Anfrage nach dem SRV und TXT Resource Record „_regserver._tcp.<DNS_DOMAIN_VPN_ZUGD_INT>".
	2. Der Konnektor MUSS eine deRegisterKonnektorRequest-Struktur gemäß [gemSpec_VPN_ZugD] erstellen und mit den entsprechenden Parametern befüllen (aktuelles Datum/Uhrzeit, bei der letzten erfolgreichen Registrierung verwendetes C.NK.VPN-Zertifikat, MGM_ ZGDP_CONTRACTID).
	Der Konnektor MUSS die Request-Nachricht mittels einer verfügbaren SM-B (ID.HCI.OSIG) im Element deRegisterKonnektorRequest/Signature signieren. (MGM_ ZGDP_SMCB ist zu bevorzugen, es kann aber auch eine andere SM-B verwendet werden).
	3. Der Konnektor ruft unter Verwendung der erzeugten Request-Nachricht die in [gemSpec_VPN_ZugD#Tab_ZD_deregisterKonnektor] definierte Operation I_Registration_Service::deRegisterKonnektor mit der Zieladresse MGM_ZGDP_REGSERVER auf.
	Der Response der Operation wird verarbeitet:
	a. Setze MGM_TI_ACCESS_GRANTED auf
	- Enabled, wenn /RegistrationStatus = „Registriert"
	- Disabled, wenn /RegistrationStatus = „Nicht registriert"
	b. Persistiere diese Zustandsinformation zusammen mit dem Zeitpunkt
	c. Verteile das folgende Ereignis über TUC_KON_256: {
	topic = "MGM/TI_ACCESS_GRANTED";
	eventType = Op;
	severity = Info;
	parameters = „Active=$MGM_TI_ACCESS_GRANTED";
	doLog = true;
	doDisp=true }
	4. Der Konnektor MUSS eine registerKonnektorRequest-Struktur gemäß ProvisioningService.xsd [gemSpec_VPN_ZugD] erstellen und mit den entsprechenden Parametern befüllen (aktuelles Datum/Uhrzeit, erneuertes C.NK.VPN-Zertifikat, MGM_ ZGDP_CONTRACTID). Der Konnektor MUSS die Request-Nachricht mittels der ausgewählten SM-B (ID.HCI.OSIG) im Element

ENTWURF

	registerKonnektorRequest/Signature signieren und das SM-B-Zertifikat im Element X509Data ablegen.
	5. Der Konnektor ruft unter Verwendung der erzeugten Request-Nachricht die in [gemSpec_VPN_ZugD#Tab_ZD_registerKonnektor] definierte Operation I_Registration_Service::registerKonnektor mit der Zieladresse MGM_ZGDP_REGSERVER auf.
	Der Response der Operation wird verarbeitet:
	a. Setze MGM_TI_ACCESS_GRANTED auf
	- Enabled, wenn /RegistrationStatus = „Registriert“
	- Disabled, wenn /RegistrationStatus = „Nicht registriert“
	b. Persistiere diese Zustandsinformation zusammen mit dem VPN:ContractStatus
	c. Verteile das folgende Ereignis über TUC_KON_256
	{
	topic = ”MGM/TI_ACCESS_GRANTED“;
	eventType = Op;
	severity = Info;
	parameters = „Active=$MGM_TI_ACCESS_GRANTED“;
	doLog = true;
	doDisp = true }

Varianten/Alternativen	(->5) Wenn der Konnektor nicht mit dem neuen C.NK.VPN-Zertifikat registriert werden konnte, dann muss sich der Konnektor, beginnend mit Schritt 4, erneut mit dem alten C.NK.VPN-Zertifikat registrieren.

Fehlerfälle	(→ 2,4) Es konnte keine freigeschaltete SM-B ausgewählt werden:
	Fail=No_Smcb
	(->4,5) Im Fehlerfall
	TUC_KON_256 {
	topic = „SMC_K/REGISTER/ERROR“;
	eventType = Op;
	severity = Error;
	parameters = „$Parameters“;
	doLog = true;
	doDisp = true }
	Die Registrierung soll herstellerspezifisch erneut mehrmals versucht werden.
	Bei allen Fehlerfällen, die zum Abbruch führen:
	TUC_KON_256 {
	topic = „SMC_K/REGISTER/ERROR“;
	eventType = Op;
	severity = Error;
	parameters = „$Parameters“;

ENTWURF

	doLog = true; doDisp = true }
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 7: Tab_Kon_933 Fehlercodes TUC_KON_411 „Zertifikate aktualisieren"

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
herstellerspezifisch			

[<=]

A_21781 - Nutzerhinweis bezüglich Fehler bei Re-Registrierung
Der Hersteller des Konnektors MUSS in seinem Handbuch den Nutzer/Administrator darauf hinweisen, dass das Ereignis mit dem Topic=SMC_K/REGISTER/ERROR dringend durch das Primärsystem abonniert werden sollte. Bei Auftreten des Fehlers mit Fail=No_Smcb muss in der Leistungserbringerumgebung dafür gesorgt werden, dass eine freigeschaltete SMC-B verfügbar ist, die der Konnektor beim nächsten Re-Registrierungsversuch verwenden kann.**[<=]**

4.1.6 (3.4.1) Identität ID.AK.AUT relevant für Konnektor - PS

Damit sich der Konnektor mittels X.509 gegenüber Clientsystemen authentisieren kann, muss er über ein entsprechendes Zertifikat und dazu passendes Schlüsselmaterial verfügen. Dieses Zertifikat und Schlüsselmaterial befinden sich auf der gSMC-K (ID.AK.AUT). Der Administrator hat mehrere Möglichkeiten, die ID.AK.AUT von der gSMC-K für die Authentisierung gegenüber den Clientsystemen zu ersetzen:

- er kann ein Zertifikat und das dazugehörige Schlüsselmaterial Konnektor-extern mit seinen lokalen Mitteln erzeugen und in den Konnektor importieren oder
- er kann ein Zertifikat und das dazugehörige Schlüsselmaterial im Konnektor erzeugen und das Zertifikat ggf. aus dem Konnektor exportieren.

Da es sich um eine lokal begrenzte Authentisierung im Verantwortungsbereich des Betreibers des lokalen Netzes handelt, werden keine weiteren Vorgaben zur Erstellung und Handhabung in der LE-Umgebung der außerhalb des Konnektors erzeugten Zertifikate und Schlüssel erhoben. Eine Online-Status-Prüfung dieser Zertifikate ist nicht erforderlich und nicht vorgesehen.

A_21811 - Vorgaben für generierte und importierte Schlüssel und Zertifikate entsprechend gemSpec_Krypt

ENTWURF

Der Konnektor SOLL bezüglich selbst generierter und importierter Schlüssel und Zertifikate für die TLS-Authentisierung gegenüber Primärsystemen die kryptographischen Vorgaben aus gemSpec_Krypt durchsetzen.**[<=]**

Bezüglich der Nutzung von Schlüsseln und Zertifikaten basierend auf elliptischer Kurven Kryptographie, sind für die generierten und importierten Daten für die TLS-Authentisierung gegenüber Primärsystemen neben den in gemSpec_Krypt genannten Brainpoolkurven auch die NIST-Kurven gleicher Stärke gestattet.

A_21697 - Schlüsselpaar und dazugehöriges X.509-Zertifikat für Authentisierung des Konnektors gegenüber Clientsystemen importieren
Der Konnektor MUSS dem Administrator den Import eines extern generierten Schlüsselpaars und des dazugehörigen X.509-Zertifikats für die Authentisierung des Konnektors im Rahmen von TLS-Verbindungen gegenüber Clientsystemen über das Managementinterface ermöglichen. **[<=]**

A_21698 - Importiertes Schlüsselpaar und dazugehöriges X.509-Zertifikat für Authentisierung des Konnektors gegenüber Clientsystemen verwenden
Der Konnektor MUSS dem Administrator das Einschalten der Verwendung von importiertem Schlüsselpaar und dazugehörigem X.509-Zertifikat für die Authentisierung des Konnektors gegenüber Clientsystemen über das Managementinterface ermöglichen. **[<=]**

A_21699 - Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen erzeugen
Der Konnektor MUSS die Erstellung eines Schlüsselpaars und eines dazugehörigen X.509-Zertifikats für die Authentisierung des Konnektors im Rahmen von TLS-Verbindungen gegenüber den Clientsystemen durch den Administrator über das Managementinterface ermöglichen. Hierbei MUSS der Konnektor dem Administrator die Möglichkeit geben, das kryptographische Verfahren RSA-2048 oder ECC-256 auszuwählen. Ferner MUSS der Konnektor dem Administrator die Möglichkeit geben, den Hostnamen des Konnektors im Zertifikat zu vergeben.**[<=]**

A_21701 - Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen exportieren
Der Konnektor MUSS dem Administrator den Export von intern generierten X.509-Zertifikaten für die Authentisierung des Konnektors im Rahmen von TLS-Verbindungen gegenüber den Clientsystemen über das Managementinterface ermöglichen. Als Exportformat MUSS PKCS#12 verwendet werden.**[<=]**

A_21702 - Intern generierte Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen verwenden
Der Konnektor MUSS dem Administrator das Einschalten der Verwendung von intern generierten Schlüsseln und X.509-Zertifikaten für die Authentisierung des Konnektors gegenüber den Clientsystemen über das Managementinterface ermöglichen. **[<=]**

A_21759 - Aufgefrischte ID.AK.AUT für Authentisierung des Konnektors gegenüber Clientsystemen verwenden
Der Konnektor MUSS dem Administrator das Einschalten der Verwendung von aufgefrischter ID.AK.AUT für die Authentisierung des Konnektors gegenüber der Clientsysteme über das Managementinterface ermöglichen. Das erneuerte Zertifikat DARF NICHT automatisch verwendet werden.**[<=]**

A_21760 - ID.AK.AUT auf gSMC-K für Authentisierung des Konnektors gegenüber Clientsystemen verwenden

ENTWURF

Der Konnektor MUSS dem Administrator das Einschalten der Verwendung von ID.AK.AUT auf der gSMC-K für die Authentisierung des Konnektors gegenüber den Clientsystemen über das Managementinterface ermöglichen.**[**<=**]**

4.1.7 (7 Anhang F) Events

Tabelle 8: TAB_KON_777 Events Interne Mechanismen

Topic Ebene1 /Topic Ebene2 /Topic Ebene3	Typ	Schwere	Prot	AnClients	Parameter	Bedeutung	Auslöser (TUC/Op)
SMC_K/UPDATE/SUCCESS	Op	Info	x	x		Zertifikate erfolgreich erneuert	TUC_KON_410
SMC_K/DOWNLOAD/ERROR	Op	Error	x	x		Fehler beim Zertifikatsdownload	TUC_KON_410
SMC_K/UPDATE/ERROR	Op	Error	x	x	Iccsn=$Iccsn; Profile=$CertProfile; Serial=$Serialnumber; Fail=Iccsn | Date | Crypt | Serial | Ocsp	Prüffehler bei Zertifikatsupdate	TUC_KON_410
SMC_K/REGISTER/ERROR	Op	Error	x	x	Iccsn=$Iccsn; SerialOld=$SerialnumberNKOld; SerialNew=$SerialnumberNKNew; Operation=Register | Deregister; Fail=No_Smcb | Other	Fehler bei Reregistrierung	TUC_KON_411

4.2 (4.1.1.2) Änderungen in gemILF_PS

Der Konnektor verwendet als TLS-Server-Zertifikat die auf der gSMC-K gespeicherte **<PTV5>bzw. vom Konnektor über die TI aufgefrischte</PTV5>** Identität ID.AK.AUT. Der CommonName dieses Zertifikats ist mit der ICCSN und dem

ENTWURF

Herausgabedatum befüllt und nicht mit dem Hostnamen des Konnektors. Eine optional durchzuführende Hostnamenprüfung durch das Primärsystem kann daher ggf. nur daraufhin erfolgen, ob der Konnektor in der LEI unter dem in `Subject.AltNames` festgelegten `DNSName`="konnektor.konlan" erreichbar ist.

<PTV5>Nach einer erfolgreichen Auffrischung der Identität ID.AK.AUT kann der Zeitpunkt der Verwendung von dieser aufgefrischten Identität vom Administrator frei gewählt werden.

Darüber hinaus kann der Konnektor intern oder extern generierte Identitäten als TLS-Server-Zertifikat verwenden. Der Administrator hat zwei Möglichkeiten, die ID.AK.AUT für die Authentisierung gegenüber den Clientsystemen zu ersetzen:

- **er kann ein Zertifikat und das dazugehörige Schlüsselmaterial konnektorextern mit seinen lokalen Mitteln erzeugen und in den Konnektor importieren oder**
- **er kann ein Zertifikat und das dazugehörige Schlüsselmaterial im Konnektor erzeugen und das Zertifikat ggf. aus dem Konnektor exportieren.**

Der CommonName dieser Zertifikate kann mit einem frei wählbaren Hostnamen des Konnektors befüllt werden. Eine optional durchzuführende Hostnamenprüfung durch das Primärsystem kann dann vollumfänglich erfolgen.

Der Zeitpunkt der Verwendung von generierten oder importierten Zertifikaten kann vom Administrator frei gewählt werden und ist unabhängig vom Zeitpunkt der Generierung oder des Imports. Der Administrator kann jederzeit zwischen der Verwendung von generierten, importierten, aufgefrischten oder ursprünglichen Zertifikaten der gSMC-K hin- und herschalten.</PTV5>

Für eine Prüfung des TLS-Server-Zertifikates des Konnektors durch das Primärsystem sind verschiedene auch kombinierbare Umsetzungsvarianten möglich.

<PTV5>Die Prüfung der generierten oder importierten Zertifikate durch das Primärsystem kann nicht gegen die TI-TSL oder die TI-Komponenten-CA-Zertifikate erfolgen, da es sich um rein lokale Identitäten außerhalb des TI-Vertrauensraums handelt.</PTV5>

Variante Prüfung gegen TI-Komponenten-SubCAs

Im Falle einer Prüfung der TLS-Server-Zertifikate des Konnektors gegen die produktive Komponenten-SubCA der TI (z.B. am PS gespeichert in einer PEM-Datei) ist der Lebenszyklus der in der TSL veröffentlichten TI-Komponenten-SubCA zu beachten. Die SubCA ist 8 Jahre gültig und wird über diesen Zeitraum in der TSL veröffentlicht. Nach spätestens drei Jahren werden jedoch End-Entity-Komponenten-Zertifikate von einer neu hinzugefügten SubCA abgeleitet, damit diese noch 5 Jahre gültig sind. Das PS muss also damit rechnen, TLS-Server-Zertifikate von Konnektoren gegen mindestens drei produktive SubCAs validieren zu können, weil es im Feld End-Entity-Konnektorzertifikate geben kann, die aus unterschiedlichen SubCAs abgeleitet sind. Am Laufzeitende einer TI-Komponenten-SubCA verliert diese ihre Gültigkeit und wird aus der TSL entfernt. Die aktuelle TSL ist unter https://download.tsl.ti-dienste.de/ verfügbar.

Darin befinden sich Zertifikate mit dem Namen GEM.KOMP-CA*, also z.B. GEM.KOMP-CA1, GEM.KOMP-CA3, o.ä. Diese Zertifikate sind auch separat im Verzeichnis https://download.tsl.ti-dienste.de/ verfügbar, um sie als Trusted CA in der LE-Umgebung zu verwalten.

ENTWURF

<PTV4> Parallel dazu wird für die Einführung von elliptischen Kurven eine zweite TSL () sowie entsprechende ECC verwendende Komponenten-CA-Zertifikate () von der gematik zur Verfügung gestellt. Diese neue TSL beruht auf ECC als kryptografisches Verfahren, enthält jedoch zusätzlich alle für den parallelen Einsatz von RSA und ECC erforderlichen RSA-Anteile. </PTV4>

Variante Etablierung Vertrauensbeziehung zwischen Konnektor und PS

Falls ein Administrator am Primärsystem das TLS-Server-Zertifikat des Konnektors im Rahmen der Inbetriebnahme des Konnektors dem Zertifikatsspeicher des lokalen PS-Rechners hinzufügen will (zur Etablierung einer Vertrauensbeziehung zwischen einer Konnektor-Instanz und einer PS-Instanz in einer einzelnen LE-Umgebung), wird an PS-Arbeitsplätzen das Konnektor-TLS-Server-Zertifikat beim ersten TLS-Handshake mit dem Konnektor einmalig akzeptiert und vom Primärsystem-Arbeitsplatz persistent gespeichert, um die gesamte nachfolgende TLS-Kommunikation zwischen PS und Konnektor abzusichern (so wie an einem Browser eine Ausnahmeregelung für CAs einer Webseite gespeichert werden kann).

Das Konnektor-TLS-Server-Zertifikat muss im Falle der Etablierung der Vertrauensbeziehung zwischen Konnektor und Primärsystem-Arbeitsplatz nicht durch das Primärsystem gegen die Komponenten-SubCAs aus der TSL geprüft werden. Im Falle eines Konnektorwechsels muss dieses Pairing mit dem neuen Konnektor erneut durchgeführt werden. Beim Austausch konnektoreigener Zertifikate, z. B. im Zuge eines Wechsels der TLS-Server-Zertifikate des Konnektors <PTV4>aufgrund der Umstellung auf Zertifikate, die ECC verwenden,</PTV4> muss die Vertrauensbeziehung erneut mit den neu erstellten End-Entity-Zertifikaten hergestellt werden.

<PTV5>Falls ein Administrator ein konnektorextern generiertes und in den Konnektor importiertes Zertifikat, ein im Konnektor generiertes Zertifikat oder die aufgefrischte ID.AK.AUT für die Server-Authentisierung verwendet, so ist das Zertifikat am Primärsystem entweder bereits bekannt (z.B. durch die Verwendung einer PKI), oder es wird im Rahmen der Inbetriebnahme des Konnektors dem Zertifikatsspeicher des lokalen PS-Rechners wie oben beschrieben hinzugefügt.</PTV5>

Änderung in Absatz 4.1.4: Neuer Absatz:

<PTV5>

4.1.4.7 Informationen zu Fehlern bei der Zertifikatserneuerung (Laufzeitverlängerung gSMC-K)

Der Konnektor stellt Informationen über ggf. aufgetretene Fehler bei der Erneuerung der Zertifikate der gSMC-K über den Systeminformationsdienst zur Verfügung, insbesondere über den Topic SMC_K/DOWNLOAD/ERROR und SMC_K/UPDATE/ERROR.

Diese Informationen sollten gemäß den Betriebsprozessen des Primärsystems beim Leistungserbringer sorgfältig berücksichtigt werden, da eine fehlerhafte oder unvollständige Erneuerung der Zertifikate der gSMC-K zu einem Ausfall der TI-Anwendungsfälle führen und einen Konnektor-Tausch notwendig machen kann. Das Primärsystem sollte diese Informationen daher beziehen (siehe Kap. 4.1.4.3) und den Anwender geeignet informieren.

Ebenso stellt der Konnektor Informationen über aufgetretene Fehler bei der Reregistrierung mit erneuertem Zertifikat zur Verfügung, insbesondere über den Topic SMC_K/REGISTER/ERROR. Bei Auftreten des Fehlers mit Parameter Fail=No_Smcb muss in der Leistungserbringerumgebung dafür gesorgt werden,

ENTWURF

dass eine freigeschaltete SMC-B verfügbar ist, die der Konnektor für die Reregistrierung verwenden kann.</PTV5>

4.3 Änderungen in gemSpec_VPN_ZugD

4.3.1 (5.3) Schnittstelle I_Registration_Service

Ergänzung von informativem Text:

Im Rahmen der Laufzeitverlängerung der gSMC-K der Konnektoren können sich Konnektoren über die vorhandene Schnittstelle I_Registration_Service automatisiert mit einem erneuerten Zertifikat C.NK.VPN gemäß [gemSpec_Kon#TUC_KON_411] erneut registrieren.

4.4 Änderungen in gemSpec_X.509_TSP

4.4.1 (6.6) Erneuerung von Zertifikaten der gSMC-K

A_21765 - Erneuerung von gSMC-K-Zertifikaten: Zeitliche Vorgabe
Ein TSP-X.509 nonQES für Komponenten MUSS zur Erneuerung von Zertifikaten der gSMC-K (C.NK.VPN, C.AK.AUT und C.SAK.AUT) den Erneuerungsprozess auf Antrag der gematik einleiten und dabei alle gSMC-K Zertifikate erneuern, die bis zum Beantragungszeitpunkt ausgegeben wurden. Das Laufzeitende der erneuerten Zertifikate MUSS jeweils auf 31.12.2024 gesetzt werden. **[<=]**

A_21766 - Erneuerung von gSMC-K-Zertifikaten: Prüfung auf Sperrung
Ein TSP-X.509 nonQES für Komponenten DARF NICHT Zertifikate der gSMC-K erneuern, wenn das zu verlängernde C.NK.VPN-Zertifikat den Status "revoked" hat. Dazu wird vom TSP-X.509 nonQES für Komponenten zuvor eine Statusprüfung durchgeführt.**[<=]**

A_21763 - Erneuerung von gSMC-K-Zertifikaten: CSR
Ein TSP-X.509 nonQES für Komponenten MUSS zur Erneuerung von Zertifikaten der gSMC-K (C.NK.VPN, C.AK.AUT und C.SAK.AUT) die ursprünglich eingereichten CSRs inklusive der ursprünglichen öffentlichen Schlüssel oder die alten Zertifikate verwenden. **[<=]**

A_21767 - Erneuerung von gSMC-K-Zertifikaten: Profile und CommonName
Ein TSP-X.509 nonQES für Komponenten MUSS zur Erneuerung von Zertifikaten der gSMC-K (C.NK.VPN, C.AK.AUT und C.SAK.AUT) denselben commonName verwenden (mit ICCSN und Kartenherausgabedatum), der im ursprünglichen Zertifikat enthalten ist. Zudem MUSS das jeweils in gemSpec_PKI definierte Zertifikatsprofil für C.NK.VPN, C.AK.AUT und C.SAK.AUT verwendet werden.**[<=]**

A_21768 - Erneuerung von gSMC-K-Zertifikaten: Erneuerung aller 3 X.509 Zertifikats-Typen

ENTWURF

Ein TSP-X.509 nonQES für Komponenten MUSS zur Erneuerung von Zertifikaten immer alle einer gSMC-K zugeordneten Zertifikate, also C.NK.VPN, C.AK.AUT und C.SAK.AUT erneuern.**[<=]**

A_21769 - Erneuerung von gSMC-K-Zertifikaten: Datei-Namen für X.509-Zertifikate
Ein TSP-X.509 nonQES für Komponenten MUSS zur Erneuerung von Zertifikaten der gSMC-K die Zertifikate jeweils in einer Zertifikats-Datei des Formats PEM bereitstellen und das folgende Namensformat verwenden - die ICCSN wird dabei als Variable für die Zuordnung der jeweiligen gSMC-K mit angegeben:

- C.NK.VPN_RSA_<ICCSN>.pem
- C.AK.AUT_RSA_<ICCSN>.pem
- C.SAK.AUT_RSA_<ICCSN>.pem

Wenn auch X.509-Zertifikate als ECC vorhanden sind und damit erneuert werden, dann werden diese wie folgt bereitgestellt:

- C.NK.VPN_ECC_<ICCSN>.pem
- C.AK.AUT_ECC_<ICCSN>.pem
- C.SAK.AUT_ECC_<ICCSN>.pem

[<=]

A_21770 - Erneuerung von gSMC-K-Zertifikaten: ZIP-Datei und Ablage
Ein TSP-X.509 nonQES für Komponenten MUSS alle erneuerten Zertifikate einer gSMC-K mit den entsprechenden in **A_21769** und **A_21775** definierten Dateien in einer gepackten Datei als ZIP zur Verfügung stellen. Jede ZIP-Datei enthält im Dateinamen die ICCCN der gSMC-K, exemplarisch mit <ICCSN>.zip
Alle ZIP-Dateien müssen nebeneinander an folgenden Downloadpunkten (getrennt nach Umgebung) bereitgestellt werden.

- PU: http://download.tsl.telematik/gsmck_neu/
- RU: http://download-ref.tsl.telematik-test/gsmck_neu/
- TU: http://download-test.tsl.telematik-test/gsmck_neu/

Dabei handelt es sich jeweils um ein Unterverzeichnis des TSL-Downloadpunktes - definiert in gemSpec_TSL#A_17680-x.

[<=]

A_21771 - Erneuerung von gSMC-K-Zertifikaten: Sperrung aller Zertifikate
Ein TSP-X.509 nonQES für Komponenten MUSS im Falle einer zu erfolgenden Sperrung einer gSMC-K alle mit der ICCSN dieser gSMC-K verknüpften X.509-Zertifikate sperren. Dazu zählen im Falle einer zwischenzeitlichen Zertifikats-Erneuerung die erneuerten als auch die ursprünglich beantragten Zertifikate einer gSMC-K.**[<=]**

4.5 Änderungen in gemSpec_CVC_TSP

4.5.1 (5.2) Erneuerung von CV-Zertifikaten der gSMC-K

A_21772 - Erneuerung von CV-Zertifikaten der gSMC-K

ENTWURF

Ein TSP-CVC für Komponenten MUSS CV-Zertifikate der gSMC-K (C.SMC.AUT_CVC und C.SAK.AUTD_CVC) auf Basis des ursprünglich eingereichten CSR inkl. öffentlichen Schlüsseln erneuern können.**[<=]**

A_21773 - Erneuerung von CV-Zertifikaten der gSMC-K: Auslösung
Ein TSP-CVC für Komponenten MUSS alle CV-Zertifikate der gSMC-K (C.SMC.AUT_CVC und C.SAK.AUTD_CVC) erneuern, sobald die korrespondierenden X.509 Zertifikate (v.a. C.NK.VPN) erneuert wurden.**[<=]**

A_21774 - Erneuerung von CV-Zertifikaten der gSMC-K: Profile, CHR und CXD
Ein TSP-CVC für Komponenten MUSS bei der Erneuerung der CV-Zertifikate der gSMC-K (C.SMC.AUT_CVC und C.SAK.AUTD_CVC) dieselben Zugriffsprofile (0 und 51) und vor allem denselben CHR (inkl. ICCSN-Bezug) verwenden. Als Certificate Expiration Date (CXD) MUSS dabei der 31.12.2024 angesetzt werden.**[<=]**

A_21775 - Erneuerung von CV-Zertifikaten der gSMC-K: Datei-Namen für erneuerte CV-Zertifikate
Ein TSP-CVC für Komponenten MUSS zur Erneuerung von CV-Zertifikaten der gSMC-K die Zertifikate jeweils in einer Zertifikats-Datei des Formats PEM bereitstellen und das folgende Namensformat verwenden - die ICCSN wird dabei als Variable zur Zuordnung der jeweiligen gSMC-K mit angegeben:

- C.SMC.AUT_CVC.E256_<ICCSN>.pem
- C.SMC.AUT_CVC.E384_<ICCSN>.pem
- C.SAK.AUTD_CVC.E256_<ICCSN>.pem
- C.SAK.AUTD_CVC.E384_<ICCSN>.pem

Neben den spezifischen Zertifikaten wird auch das Zertifikat der CVC-CA bereitgestellt, die die erneuerten CV-Zertifikate der gSMC-K signiert hat in der Form:

- <CVC-CA-Name>.pem (z.B. DEZGW830218.pem)

[<=]

4.6 Änderungen in gemRL_TSL_SP_CP

4.6.1 (Kap. 10) Anhang A – Certificate Policy für Komponentenzertifikate

Ergänzend zu Abschnitt 5.6 gelten zusätzlich folgende Anforderungen hinsichtlich der Zertifikatserneuerung bei einem TSP-X.509 nonQES für Komponentenzertifikate (gSMC-K):

A_21764 - Erneuerung von Zertifikaten der gSMC-K
Ein TSP-X.509 nonQES für Komponenten MUSS Zertifikate der gSMC-K (C.NK.VPN, C.AK.AUT und C.SAK.AUT) auf Basis des ursprünglich eingereichten CSR bzw. der zuvor ausgestellten Zertifikate erneuern können.**[<=]**

4.7 Änderungen in gemSpec_KT

Vorbemerkungen zu den im Folgenden dargestellten Änderungen:

ENTWURF

1. So weit bekannt, verfügt derzeit kein eHealth-Kartenterminal über eine Systemuhr oder anderweitige Zeitinformation. Deshalb prüfen eHealth-Kartenterminals die zeitliche Gültigkeit von Zertifikaten nicht.
2. So weit bekannt, verwenden eHealth-Kartenterminals in Pairing-Blöcken keine Zertifikate, sondern öffentliche Schlüssel, die Zertifikaten entnommen werden.
3. Diesbezüglich ist vorgesehen, dass sich die Anforderungslage nicht ändert. Eine Systemuhr (oder ähnliches) ist nach wie vor nicht erforderlich. Allerdings ist es das Ziel deutlicher herauszustreichen, dass
   a. eine zeitliche Prüfung von Zertifikaten erlaubt ist (siehe Änderungen 1 und 2) und
   b. in Pairing-Blöcken eben keine Zertifikate, sondern öffentliche Schlüssel verwendet werden (siehe Änderungen 4 und 5).
4. Falls ein eHealth-Kartenterminal die zeitliche Gültigkeit von Zertifikaten prüft und dabei feststellt, dass ein Zertifikat abgelaufen ist, dann wird so ein Zertifikat gemäß Änderung 3 als "ungültig" betrachtet. Die unveränderte Anforderungslage in [gemSpec_KT#3.11] ist dann so, dass ein TLS-Aufbau zwar möglich, der nutzbare Funktionsumfang allerdings eingeschränkt ist, siehe [gemSpec_KT#TIP1-A_3137].

4.7.1 Änderung 1, Besonderheiten zur Gültigkeit

In [gemSpec_KT#Tabelle 16] wird in der Zeile "Gültigkeit des Zertifikates prüfen" in der letzte Spalte der folgende Passus ersatzlos entfernt: "Wird nicht durchgeführt."

4.7.2 Änderung 2, Anmerkung zur Systemuhr

In [gemSpec_KT#3.11] wird die erste Anmerkung unter Tabelle 16 wie folgt geändert:

Ersetze:
Ein eHealth-Kartenterminal verfügt über keine Systemuhr und keine Datumsangaben. Es kann daher die Gültigkeit des Komponentenzertifikats nicht überprüfen.

Durch:

Die gematik betrachtet es als zulässig, wenn ein eHealth-Kartenterminal keine Systemuhr besitzt und auch anderweitig keine Information zu Datum oder Zeit zur Verfügung hat. Als Konsequenz folgt daraus, dass eHealth-Kartenterminals ohne Datums- und Zeitinformation nicht in der Lage sind die zeitliche Gültigkeit von Zertifikaten zu prüfen.

4.7.3 Änderung 3, Datums- und Zeitinformation

In [gemSpec_KT#3.11] wird unmittelbar hinter TIP1-A_4115 folgende Anforderung neu aufgenommen:

A_21812 - Datums- und Zeitinformation
Das eHealth-Kartenterminal KANN über eine Systemuhr oder anderweitige Datums- und Zeitinformation verfügen. Falls das eHealth-Kartenterminal über eine Datums- und Zeitinformation verfügt, dann wird empfohlen, dass Zertifikate als ungültig eingestuft werden, wenn ihre zeitliche Gültigkeit abgelaufen ist.**[<=]**

ENTWURF

4.7.4 Änderung 4, Pairing-Block

[gemSpec_KT#TIP1-A_3046] wird durch folgende Anforderung ersetzt:

TIP1-A_3046-01 - Pairing-Block
Jeder Pairing-Block besteht aus einem Shared-Secret und aus einer Menge mit öffentlichen Schlüsseln. Das eHealth-Kartenterminal MUSS für die Mächtigkeit der Menge alle Werte aus dem Intervall [1, 3] unterstützen.**[**<=**]**

4.7.5 Änderung 5, Erläuterung zum Pairing Block

In [gemSpec_KT#2.5.2] wird der Absatz unterhalb von TIP1-A_3046 wie folgt ergänzt:
In TIP1-A_3046-01 werden absichtlich die "öffentlichen Schlüssel" verwendet, statt die Zertifikate, mit denen die öffentlichen Schlüssel transportiert werden. Als Konsequenz ist es einem Konnektor möglich zu einem öffentlichen Schlüssel, für den ein gültiger Pairing-Block vorliegt, beliebig viele Zertifikate zu verwenden, ohne dass dies Auswirkungen auf das bestehende Pairing hätte.

ENTWURF

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung

5.2 Referenzierte Dokumente

5.2.1 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: Glossar der Telematikinfrastruktur

5.2.2 Weitere Dokumente

[Quelle]	**Herausgeber (Erscheinungsdatum): Titel**

ENTWURF

6 Anhang C – Offene Punkte, Fragen

Offener Punkt zu Kapitel 3.3: Zur Zeit erfolgt der Sperrprozess über die Zertifikats-Seriennummer, daher benötigen die Konnektor-Hersteller die Info zur Seriennummer.
OI: Wie bekommen die Hersteller die Information über die neuen Seriennummern?

Offener Punkt zu Kapitel 3.4: Zusätzlich wird erwogen, ob die Möglichkeit geschaffen werden kann, dass ein Admin manuell frische gSMC-K-Zertifikate einbringt, ggf. auch nach Ablauf der ursprünglichen Zertifikate.

ENTWURF