Einführung der Gesundheitskarte

Errata zu Release 1.6.4 Online-Rollout (Stufe 1) Erprobung und Produktivbetrieb

führt zu

Release 1.6.4-2

Version:	1.0.0
Stand:	23.10.2017
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemErrata_R1.6.4-2]

Betroffene Produkttypen	Neue Produkttypversion
gemProdT_Kon	1.10.2-0
gemProdT_Kon (mit QES)	2.11.2-0
gemProdT_VPN_ZugD	1.7.3-0
gemProdT_eHealth_KT	1.2.1-1
gemProdT_gSMC-KT_ObjSys_G2.1	4.4.1-0
gemProdT_HBA_ObjSys_G2.1	4.4.1-0
gemProdT_eGK_ObjSys_G2.1	4.4.1-0
gemProdT_SMC-B_ObjSys_G2.1	4.4.1-0
gemProdT_HBA_ObjSys	4.3.1-2
gemProdT_X.509_TSP_nonQES_eGK	1.7.0-1
gemProdT_X.509_TSP_nonQES_HBA	1.7.0-1
gemProdT_X.509_TSP_nonQES_Komp	1.8.0-1
gemProdT_X.509_TSP_nonQES_SMC-B	1.9.0-0
gemProdT_gematik-Root-CA	1.4.0-1
gemProdT_TSL	1.7.0-2

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_5569	gemSpec_HBA_ObjSys_G2.1, gemSpec_gSMC-KT_ObjSys_G2.1	Kapitel 'Methodik', Abschnitt 'Nomenklatur', Tabelle 'Beispiele'	**Karten G2.1 – Entfernung irrelevanter G1 Anteile – redaktionell** Die genannte Tabelle erläutert informativ die Nomenklatur zur Verwendung rollenbasierter Authentisierung in Zugriffsregeln gemäß Generation 1. Diese Art der Kodierung ist veraltet und wird in den Dokumenten nicht genutzt. In der SMC-B sind diese Hinweise nicht (mehr) aufgeführt. Die Entfernung der informativen Einträge schafft diesbezüglich einen einheitlichen Stand in allen Objektsystemspezifikationen.	Entfernen der informativen Zeilen aus der Beispieltabelle. Detailliert in C_5569_Anlage dargestellt.	gemSpec_HBA_ObjSys_G2.1, gemSpec_gSMC-KT_ObjSys_G2.1
C_6071	gemSpec_Karten_Fach_TIP	EF.Version2	**Karten G2.1 – Aufnahme Festlegungen zu EF.KeyInfo** Die Version der Befüllvorschrift für EF.KeyInfo muss für die gSMC-K und gSMC_KT der Generation G2.1 angepasst werden, da sich die Struktur des Objekts EF.KeyInfo geändert hat. Die bisherigen Vorgaben für die Befüllung von EF.KeyInfo können entfallen. Es wird ein neues Dokument gemSpec_Karten_Fach_TIP_G2.1 für die in G2.1 notwendigen Vorgaben eingeführt, welches darüber hinaus weitere Anpassungen enthält, um konsistent zu den bereits veröffentlichten Objektsystemspezifikationen zu sein.	Zu den Änderungen von gemSpec_Karten_Fach_TIP_G2.1 gegenüber gemSpec_Karten_Fach_TIP siehe Anlage: C_6071_Anlage.docx Der Produkttypsteckbrief gemProdT_gSMC-KT_ObjSys_G2.1 ändert sich wie folgt: Tabelle 1: Alt: gemSpec_Karten_Fach_TIP Befüllvorschriften für die Plattformanteile der Karten der TI 2.6.0 Neu: gemSpec_Karten_Fach_TIP_G2.1 Befüllvorschriften für die Plattformanteile der Karten der TI 1.0.0 Kapitel 3.1.1 und 3.2.1 Card-G2-A_3483 wird ersetzt durch Card-G2-A_3483-01 Card-G2-A_3499, Card-G2-A_3501, Card-G2-A_3504 und Card-G2-A_3505 entfallen	gemSpec_Karten_Fach_TIP_G2.1 (neu) gemProdT_gSMC-KT_ObjSys_G2.1
C_6099	gemProdT_Kon_PTV1 gemProdT_Kon_PTV2	Tabelle 2 Tabelle 4 Tabelle 5	**Klarstellung von Prüfverfahren für Anforderungen** Diese Anpassung umfasst Änderungen an Prüfverfahren von Anforderungen. Der Anforderungshaushalt der Produkttypen wird dabei nicht verändert. Aus folgenden Gründen ist diese Anpassung notwendig: 1. Anforderungen sind im Funktionsumfang VSDM-Konnektor (PTV1) nicht relevant und daher aus PTV1 zu entfernen. 2. Anforderungen sind im Blackbox-Verfahren nicht testbar und daher nur über Herstellererklärung nachzuweisen. 3. Anforderungen können nur zum Teil durch Blackbox-Tests nachgewiesen werden. Nicht testbare Aspekte der Anforderung sind über eine Herstellererklärung zu belegen. 4. Anforderungen sind weder im Funktionsumfang VSDM-Konnektor (PTV1) noch im QES-Konnektor (PTV2) testbar und sind daher über eine Herstellererklärung nachzuweisen. Hierzu zählen auch TUCs, die nicht aufgerufen werden. 5. Anforderungen beschreiben keine funktionalen Eigenschaften des Produkts und sind daher nicht über Test, sondern über eine Herstellererklärung nachzuweisen. 6. Übergreifende Anforderung wird durch konkrete Anforderungen bereits abgedeckt. 7. Anforderung wurde fälschlicherweise dem Sicherheitsgutachten der gSMC-K-Personalisierung bzw. gSMC-KT-Personalisierung zugeordnet. 8. Korrekturen der Zuordnung zur sicherheitstechnischen Eignung "CC-Evaluierung". 9. Anforderungen müssen allein oder zusätzlich zu anderen Prüfverfahren über eine Herstellererklärung nachgewiesen werden.	siehe C_6099_Anlage	gemProdT_Kon_PTV1 gemProdT_Kon_PTV2 gemProdT_KT
C_6100	gemSpec_eGK_ObjSys_G2.1, gemSpec_HBA_ObjSys_G2.1, gemSpec_SMC-B_ObjSys_G2.1, gemSpec_gSMC-KT_ObjSys_G2.1		**Karten G2.1 – Konsistenzfehler Objektsysteme** In den Objektsystemspezifikationen G2.1 werden einige Inkonsistenzen korrigiert. Im Wesentlichen betrifft dies Zugriffsregeln und Objektattribute von Objekten für Objektsstatus und Anwendungssituationen, die zu keiner Zeit im Lebenszyklus der Karten erreichbar und daher nicht testbar sind und nicht implementiert werden müssen. Darüber hinaus werden einige editorische Inkonsistenzen, etwa die einheitliche Verwendung von Nomenklaturen, korrigiert.	siehe Anlage C_6100	gemSpec_eGK_ObjSys_G2.1 gemSpec_HBA_ObjSys_G2.1 gemSpec_SMC-B_ObjSys_G2.1 gemSpec_gSMC-KT_ObjSys_G2.1 gemProdT_eGK_ObjSys_G2.1 gemProdT_HBA_ObjSys_G2.1 gemProdT_gSMC-KT_ObjSys_G2.1 gemProdT_SMC-B_ObjSys_G2.1

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	**Anpassungen** an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_6131	gemSpec_Net	GS-A_4835 GS-A_5546	**Konsistenzfehler bei Zuordnung der Festlegung der Dienstklassen zur Priorisierung (Konnektor)** Die Anforderung GS-A_4835 muss durch den Produkttypen Konnektor erfüllt werden, war bisher aber nicht in den Produkttypsteckbriefen dieses Produkttyps enthalten. Diese inhaltliche Inkonsistenz muss behoben werden. Der bisher in der Anforderung benannte Produkttyp VPN-Zugangsdienst ist nicht durch diese Anforderung betroffen und wird zukünftig auch nicht mehr in der Anforderung benannt. Um eine Umsetzung im Produkttyp Konnektor zu vereinfachen wird die Möglichkeit geschaffen, dass Konnektoren bei der Kommunikation mit dem KSR eine einheitliche Markierung verwenden können.	Zuordnung der Afo zum Konnektor gemSpec_Net: **alt:** GS-A_4835 Festlegung der Dienstklassen zur Priorisierung Die Produkttypen Konnektor, VPN-Zugangsdienst und Zentrales Netz der TI MÜSSEN die Zuordnung von Dienstklassen zu fachanwendungsspezifischen Diensten und zentralen Diensten gemäß Tabellen Tab_QoS_Dienstklassen, Tab_QoS_Mapping_Dienstklasse_Anwendung und Tab_QoS_Mapping_Dienstklassen_Bandbreite umsetzen. Die Zuordnungen können durch den GBV bei Bedarf geändert werden. **neu:** GS-A_4835 Festlegung der Dienstklassen zur Priorisierung Die Produkttypen Konnektor und Zentrales Netz der TI MÜSSEN die Zuordnung von Dienstklassen zu fachanwendungsspezifischen Diensten und zentralen Diensten gemäß Tabellen Tab_QoS_Dienstklassen, Tab_QoS_Mapping_Dienstklasse_Anwendung und Tab_QoS_Mapping_Dienstklassen_Bandbreite umsetzen. Die Markierung MUSS sowohl bei Requests als auch bei Responses der Dienste umgesetzt werden. Testtyp: funktionaler Test **neue Afo:** GS-A_5546 Der Produkttyp Konnektor KANN Datenverkehr in Richtung KSR mit einer einheitlichen DSCP-Markierung "KSR Update" versehen. Testtyp: funktionaler Test	gemSpec_Net gemProdT_Kon_PTV1 gemProdT_Kon_PTV2
C_6138	gemSpec_Perf	Kapitel 4.2.9 Produkttyp VPN-Zugangsdienst	**Performanceanforderungen für IPSec Tunnel TI und SIS für VPN-Zugansdienst** Als Erkentniss der Erprobung ORS1 fehlt eine Anforderungen, die verhindert, dass der VPN-Zugansdienst eine unnötige Einschränkung des Durchsatzes über das Transportnetz durch die IPsec-Tunnel TI und SIS verursacht.	In Kapitel 4.2.9 werden folgende Anforderungen ergänzt: **GS-A_5510 Performance - VPN-Zugangsdienst - IPSec-Tunnel TI und SIS** Der Produkttyp VPN-Zugangsdienst MUSS eine Anbindung zum Transportnetz von mindestens 1 Gbit/sec pro 10000 Konnektoren besitzen. Die VPN-Konzentratoren für SIS und TI MÜSSEN einen IPSec-Durchsatz unterstützten, der sich aus der Transportnetzanbindung ergibt. **Prüfverfahren:** Herstellererklärung **GS-A_5545 Performance - VPN-Zugangsdienst - IPSec-Tunnel TI und SIS** Konfigurationseinstellungen Der Produkttyp VPN-Zugangsdienst DARF den IPSec-Durchsatz der VPN-Konzentratoren pro Konnektor NICHT durch Konfigurationseinstellungen reduzieren. **Prüfverfahren:** Herstellererklärung	gemSpec_Perf gemProdT_VPN_ZugD
C_6139	gemSpec_Kon	TIP1-A_4714	**Flexibilisierung Format für log-Zeitstempel für Konnektor** Die mit C_5988 eingeführte Vorgabe eines konkreten Formats für die Formatierung des Zeitstempels in Protokolleinträgen hatte die gesetzliche Zeit (§4 EinhZeitG) vorausgesetzt und die Angabe einer Zeitzone nicht vorgesehen. Mit Änderung C_6139 wird im Zeitstempel-Format auch die Angabe der Zeitzone ermöglicht. Die Anforderung wird so geändert, dass vorhandene Implementierungen zulässig sind. Die Mindestanforderungen an einen Zeitstempel bezüglich Genauigkeit und Einheitlichkeit bleiben gewahrt.	In TIP1-A_4714 wird folgender Absatz geändert: **alt:** „timestamp=%d{dd.MM.yyyy HH:mm:ss.SSS}“ MUSS als Zeitstempelformat verwendet werden und als Wert die gesetzliche Zeit (§4 EinhZeitG) angegeben werden. **neu:** Es MUSS durchgängig dasselbe Zeitstempelformat verwendet werden, entweder „timestamp=%d{dd.MM.yyyy HH:mm:ss.SSS}“ (Beispiel „30.08.2017 13:44:12.436“) und als Wert die gesetzliche Zeit (§4 EinhZeitG) oder „timestamp=%d{dd.MM.yyyy HH:mm:ss.SSSZ}“, wobei „Z“ die Zeitzonenangabe nach RFC 822 mit ("+" / "-") 4DIGIT bezeichnet (Beispiel „30.08.2017 13:44:12.436+0200“).	gemSpec_Kon

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_6162	gemSpec_Perf	GS-A_5327	Vereinfachung Nachweis der Performancevorgaben für den Konnektor GS-A_5327 fordert den Nachweis der Skalierbarkeit für einen VSDM-Konnektor auf Basis eines QES-Produktmusters. Im Dokument gemSpec_Perf wird im Anschluss an die Anforderung in zwei Absätzen skizziert, welche Funktionalität das QES-Produktmuster liefern muss und wie die Tests erfolgen. Um den Aufwand bei der Bereitstellung des QES-Produktmusters zu minimieren, ist eine detailliertere Beschreibung im Anhang von gemSpec_Perf zu ergänzen.	siehe C_6162_Anlage	gemSpec_Perf
C_6173	gemSpec_Kon		**Klarstellung Sicherheitsanforderungen gSMC-K für Konnektor** Es kann vorkommen, dass ein Konnektorhersteller im Rahmen der gSMC-K-Herausgabe selber Schlüssel für die gSMC-K erzeugt, statt diese vom Personalisierer erzeugen zu lassen. Dieser Fall wurde bisher nicht berücksichtigt. Um sicherzustellen, dass die Schlüssel sicher erzeugt und gespeichert werden und anschließend sicher an den Personalisierer übertragen werden, müssen zwei entsprechende Anforderungen an den Konnektorhersteller in die Konnektor-Spezifikation aufgenommen werden. Die Umsetzung der Anforderung ist über eine Herstellererklärung nachzuweisen	Die folgenden neuen Anforderungen werden in Kap. 3.1.1 der Konnektorspezifikation aufgenommen: TIP1-A_5702 - Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung Der Hersteller des Konnektors, der Schlüssel für die gSMC-K erzeugt, MUSS diese Schlüssel in einem HSM erzeugen, welches a) über einen Zugriffsschutz verfügt, sodass nur Berechtigte den Schlüssel nutzen können, b) in einem zutrittsgeschützten Bereich aufbewahrt wird und c) mindestens nach FIPS 140-2 Level 3 zertifiziert ist. TIP1-A_5703 - Geschützte Übertragung von Daten zum Kartenpersonalisierer Der Hersteller des Konnektors, der Daten für die gSMC-K erzeugt (bspw. Schlüssel), MUSS diese Daten bei der Übertragung zum Kartenpersonalisierer hinsichtlich Vertraulichkeit, Authentizität und Integrität mit einem Verfahren nach [gemSpec_Krypt] schützen.	gemSpec_Kon gemProdT_Kon_PTV1 gemProdT_Kon_PTV2
C_6174	gemSpec_TLK_COS_G2		**Karten G2.1 – Festlegungen für Testlaborkarten G2.1** Das Dokument gemSpec_TLK_COS_G2 (Spezifikation der Testlaborkarte COS / Objektsysteme) wird zur Aufnahme von G2.1-Anteilen fortgeschrieben.	Siehe Änderungen im Dokument gemSpec_TLK_COS_G2.	gemSpec_TLK_COS_G2
C_6178	gemSpec_VPN_ZugD	Gesamtes Dokument: alle Referenzen auf den RFC 5996	**Ablösung RFC5996 durch RFC7296 (IKEv2)** Der RFC 5996 ist seit Oktober 2015 obsolet und durch den RFC 7296 ersetzt worden. Zudem wird im akutellen Protection Profile für den Netzkonnektor (BSI-CC-PP-0097) ebenfalls auf den neuen RFC 7296 referenziert. Somit ist es erforderlich, die Referenzen auch in den Spezifikationen anzupassen. Auswirkungen: Eine Anpassung der Produkte ist durch den Verweis auf den RFC 7296 nicht notwendig. Die aktuell eingesetzten Produkttypen unterstützen den RFC 7296. Zudem ergeben sich durch die Referenzierung auf den RFC 7296 keine weiteren Anpassungen im Dokument gemSpec_VPN_ZugD. Detaillierte Analyse der Änderungen zwischen RFC 5996 und RFC 7296: 1. Klarstellungen 2. ein neues Kapitel bzgl. Traffic-Selektoren beim Rekeying.	Änderungen gemSpec_VPN_ZugD: In folgenden Anforderungen wird die Referenz [RFC 5996] gestrichen und durch [RFC 7296] ersetzt: TIP1-A_4286 TIP1-A_4287 TIP1-A_4353 TIP1-A_4354 TIP1-A_4355 TIP1-A_4357 TIP1-A_4372 TIP1-A_4373 TIP1-A_4389 TIP1-A_4396 TIP1-A_4397 TIP1-A_4398 TIP1-A_4390 Änderungen im Text: Im informativen Text in Kapitel 3.7 wird die Referenz [RFC 5996] gestrichen und durch [RFC 7296] ersetzt. Änderungen in Tabellen: In der Tabelle A5.2 wird die Referenz [RFC 5996] gestrichen und durch [RFC 7296] ersetzt.	gemSpec_VPN_ZugD gemProdT_VPN_ZugD gemProdT_Kon_PTV1 gemProdT_Kon_PTV2
C_6179	gemSpec_Kon	TAB_KON_606	**Behebung Konsistensehler R1.6.4-1 zu C_6126 (OCSP-Timeout) - redaktionell** Die OCSP-Timeoutwerte wurden im Rahmen von C_6126 geändert. Die Anpassung bezieht sich nur auf TAB_KON_689. Da die Festlegung normativ jedoch in TAB_KON_606 beschrieben wird, muss diese Tabelle gleichermaßen angepasst werden.	In der Tabelle TAB_KON_606 werden entsprechende Werte analog zu Tabelle TAB_KON_689 geändert: *alt:* CERT_OCSP_TIMEOUT_NONQES X Sekunden Timeout für OCSP-Abfragen bei der Prüfung von nonQES-Zertifikaten. Der Wert MUSS zwischen 1 und **120** Sekunden liegen. Default-Wert = **10** Sekunden CERT_OCSP_TIMEOUT_QES X Sekunden Timeout für OCSP-Abfragen bei der Prüfung von QES-Zertifikaten. Der Wert muss zwischen 1 und **120** Sekunden liegen. Default-Wert = **10** Sekunden *neu:* CERT_OCSP_TIMEOUT_NONQES X Sekunden Timeout für OCSP-Abfragen bei der Prüfung von nonQES-Zertifikaten. Der Wert MUSS zwischen 1 und **30** Sekunden liegen. Default-Wert = **3** Sekunden CERT_OCSP_TIMEOUT_QES X Sekunden Timeout für OCSP-Abfragen bei der Prüfung von QES-Zertifikaten. Der Wert muss zwischen 1 und **30** Sekunden liegen. Default-Wert = **6** Sekunden	gemSpec_Kon

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	**Anpassungen** an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_6184	gemProdT_HBA	Card-G2-A_3314	**Karten G2.1 – Behebung Konsistenzfehler Objektsystem HBA G2 – redaktionell** gemProdT_HBA (G2.0) referenziert für die AFO Card-G2-A_3314 fachlich den Inhalt dieser AFO für die Generation G2.1 (Schlüssellänge R3072 anstelle des korrekten Wertes R2048).	gemSpec_HBA_ObjSys_G2.1 Die Anforderung Card-G2-A_3314 wird in Card-G2-A_3314-01 umbenannt. gemProdT_HBA_G2.1 Die Anforderung Card-G2-A_3314-01 ersetzt Card-G2-A_3314-01 in Kapitel 3.1.2 gemProdT_HBA In Kapitel 3.1.2 ändert sich die Afo-Bezeichung für Card-G2-A_3314 Alt: K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072 Neu: K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R2048	gemProdT_HBA_G2.1 gemProdT_HBA_ObjSys_G2.1 gemSpec_HBA_ObjSys_G2.1
C_6231	gemKPT_Arch_TIP		Durch C_6010 wurden die berufmäßigen Gehilfen von Psychotherapeuten als Zugriffsberechtigt auf die medizinischen Anwendungen der eGK ausgewiesen. Diese Aussage ist rechtlich nicht zulässig und muss aus den Dokumenten der gematik wieder entfernt werden. Darüber hinaus muss in den Dokumenten klargestellt werden, dass die SMC-B der Psychotherapeuten einen Zugriff auf die medizinischen Anwendungen der eGK ermöglicht, dieser Zugriff aber nur dem Psychotherapeuten selbst gestattet ist.	Die Änderungen werden in C_6231_Anlage dargestellt.	gemKPT_Arch_TIP gemSpec_PKI
C_6234	gemILF_PS	Tabelle 44: Fehlercodes VSDM	**Behebung Inkonsistenz (Fehlertext) Implementierungsleifaden VSDM** Die Tabelle 44 informiert den PS-Hersteller über VSDM-Fehlercodes. Die auslösende Bedingung des Fehlers 3039 ist falsch bzw. abweichend zur leitenden Spezfikation gemSpec_SST_PS_VSDM wiedergegeben (s. dort, Tabelle 7). Die Korrektur soll verhindern, dass der PS-Hersteller für den Fehler 3039 eine inkorrekte Fehlerbehandlung durchführt.	Tabelle 44, Zeile Code 3039, Spalte Auslöser: **alt:** "Daten von der SMC/HBA konnte nicht gelesen werden." **neu:** "Die Integritätsprüfung bei der Entschlüsselung des Prüfungsnachweises schlägt fehl."	gemILF_PS
C_6242	gemSpec_PKI	Anhang A4, Tab_SMCB_KTR	Für die SMC-B KTR ist im Release 1.6.4 ein X.509-Zertifikatsprofil aufgenommen worden. Die Einträge in der Profiltabelle sind bisher jedoch alle als "offen" gekennzeichnet. Mit dieser Änderung werden die sektorspezifischen Anteile festgelegt und die Produktion einer SMC-B KTR somit ermöglicht. Die SMC-B KTR ermöglicht den Kostenträgern die TI-Anbindung ihrer Geschäftsstellen über den VPN-Zugangsdienst.	siehe C_6242_Anlage	gemSpec_PKI, gemProdT_X.509_TSP_ nonQES_SMC-B
C_6249	gemSpec_PKI	Anhang A4, Tab_SMCB_KTR	Die TSP-ID Tabelle, die in verschiedenen Zertifikats-Profilen als Bestandteil der subjectSerialNumber aufgeführt ist, ist bisher nur innerhalb des Anhangs A1 – KZBV vollständig dargestellt. Um diese Tabelle innerhalb der Zertifikats-Profile eindeutig referenzieren zu können, wird die Tabelle in den allgemeinen Teil der Spezifikation verschoben und jeweils Hinweise auf diese Tabelle aufgeführt. Dazu werden folgende Änderungen vorgenommen. Wird die Änderung nicht durchgeführt kann die TSP-ID Tabelle weiterhin nicht eindeutig in den Zertifikatsprofilen referenziert werden.	siehe C_6249_Anlage	gemSpec_PKI, gemProdT_X.509_TSP_ nonQES_SMC-B
C_6251	gemSpec_Perf	GS-A_4159	Die Lastvorgaben für OCSP-Responder in GS-A_4159 müssen in folgenden Aspekten angepasst werden: • Die Lastzahlen berücksichtigen noch nicht die Zahl der tatsächlich vom TSP zu unterstützenden Zertifikate bzw. Karten. • Die Verweise auf Erprobung sind zu entfernen. • Es ist zu trennen zwischen einer Last, die bei Zulassung anzuwenden ist, von der Skalierung mit der Anzahl der ausgegebenen Karten im Betrieb.	siehe C_6251_Anlage	gemSpec_Perf
C_6258	gemSpec_Kon	TIP1-A_4823	Mit den Erkenntnissen der Erprobung ORS1 wird das Feature "logische Trennung" nicht benötigt und soll aus dem Konnektor entfernt werden. Als erster Schritt wird ein Handbucheintrag vorgeschrieben, der das Feature als abgekündigt ausweist.	siehe C_6258_Anlage	gemSpec_Kon

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_6260	gemSpec_Krypt	GS-A_4382 GS-A_5547 GS-A_5548 GS-A_5549 GS-A_5508	**Re-Authentisierung der IPSec Verbindung alle 7 Tage** Wenn bei der Re-Authentisierung (Re-Auth) der IPSec-Verbindung zwischen Konnektor und VPN-Konzentrator eine neue Tunnel-IP-Adresse vergeben wird, dann werden dadurch die gerade aktiven TCP-Verbindungen zerstört. Um dies zu verhindern wird gefordert, dass bei der Re-Auth keine neue Tunnel-IP-Adresse vergeben, sondern die bisherige Tunnel-IP-Adresse beibehalten wird. Da VPN-Zugangsdienste dies nicht sofort ändern können wird zusätzlich dae Re-Auth Intervall deutlich erhöht um die Anzahl der Verbindungsabbrüche zu verrringern.	siehe C_6260_Anlage Für die neuen Anforderungen gelten folgende Prüfverfahren: GS-A_5547: funktionale Eignung, Test GS-A_5548: funktionale Eignung, Test GS-A_5549: funktionale Eignung, Test	gemSpec_Krypt

Änderungsbedarf in gemSpec_HBA_ObjSys_G2.1 und gemSpec_gSMC-KT_ObjSys_G2.1

Die informativen Angaben zur Kodierung von Rollenauthentisierungen gemäß Generation 1 im Abschnitt „Nomenklatur“ des Kapitels „Methodik“ sind obsolet und werden in den betroffenen Dokumenten nicht verwendet.

In Analogie zur Spezifikation gemSpec_SMC-B_ObjSys_G2.1, die diese Angaben nicht enthält, folgt hier die Löschung der betroffenen Stellen in den verbleibenden Spezifikationen zu HBA und gSMC-KT der Generation G2.1.

Es wird rein informativer Text entfernt. Der Sinn, Zweck und normative Inhalt des jeweiligen Dokuments bleibt unverändert.

gemSpec_HBA_ObjSys_G2.1 wird wie folgt geändert:

Kapitel 1.5 Methodik, Unterpunkt 1.5.1 Nomenklatur, Tabelle: ‚Beispiele‘

Beispiele:

Langform	**Kurzform**
~~Informativ: AUT(CHA.1)~~	~~C.1~~
~~Informativ: AUT(CHA.7)~~	~~C.7~~
~~Informativ: AUT(CHA.2) OR AUT(CHA.3)~~	~~C.2.3~~
~~Informativ: PWD(PIN) AND [AUT(CHA.2) OR AUT(CHA.3)]~~	~~PWD(PIN) AND [C.2.3]~~
AUT(oid_cvc_fl_cms,’00010000000000’)	flagCMS.15
AUT(oid_cvc_fl_ti, ‘00010000000000’) OR AUT(oid_cvc_fl_ti, ‘00008000000000’)	flagTI.15 OR flagTI.16
PWD(PIN) AND [AUT(oid_cvc_fl_cms,’00010000000000’) OR AUT(oid_cvc_fl_ti, ‘00008000000000’)]	PWD(PIN) AND [flagCMS.15 OR flagTI.16)]
SmMac(oid_cvc_fl_cms, ’00800000000000’)	SmMac(flagCMS.08)

---

gemSpec_gSMC-KT_ObjSys_G2.1 wird wie folgt geändert:

Kapitel 1.5 Methodik, Unterpunkt 1.5.1 Nomenklatur, Tabelle: „Beispiele“

Beispiele:

Langform	**Kurzform**
~~Informativ: AUT(CHA.1)~~	~~C.1~~
~~Informativ: AUT(CHA.7)~~	~~C.7~~
~~Informativ: AUT(CHA.2) OR AUT(CHA.3)~~	~~C.2.3~~

~~Informativ: PWD(PIN) AND [AUT(CHA.2) OR AUT(CHA.3)]~~	~~PWD(PIN) AND [C.2.3]~~
AUT(oid_cvc_fl_cms,'00010000000000')	flagCMS.15
AUT(oid_cvc_fl_ti, '00010000000000') OR AUT(oid_cvc_fl_ti, '00008000000000')	flagTI.15 OR flagTI.16
PWD(PIN) AND [AUT(oid_cvc_fl_cms,'00010000000000') OR AUT(oid_cvc_fl_ti, '00008000000000')]	PWD(PIN) AND [flagCMS.15 OR flagTI.16)]
SmMac(oid_cvc_fl_cms, '00800000000000')	SmMac(flagCMS.08)

Sachstand

Die Struktur der Datei EF.KeyInfo der gSMC-K und gSMC-KT ist für die Generation G2.1 verändert worden. Dieses erfordert eine Anpassung der Vorgaben gegenüber gemSpec_Karten_Fach_TIP für die Version und die Inhalte dieser Datei. Darüber hinaus wurden weitere Anpassungen vorgenommen, um konsistent zu den bereits veröffentlichten Objektsystemspezifikationen zu sein.

Änderungen in gemSpec_Karten_Fach_TIP_G2.1 gegenüber gemSpec_Karten_Fach_TIP

2.3 EF.Version2

⌦ **Card-G2-A_3483-01 K_Initialisierung: Inhalt *body* von EF.Version2**

Der Inhalt des Attributes *body* MUSS eine Konkatenation von primitiven Datenobjekten sein, die von einem Constructed Element umschlossen werden.

Die EF.Version2 MUSS den in Tab_Karten_Fach_TIP_002 festgelegten Inhalt aufweisen. ⌫

Tabelle 4: Tab_Karten_Fach_TIP_002 Inhalt von EF.Version2

<table>
<tr><th>Tag</th><th>L</th><th>Wert</th></tr>
<tr><td>'EF'</td><td>'XX'</td><td>Inhalt EF.Version2 'XX' = Länge abhängig vom Kartentyp:
'Wert von XX' für eGK,
'2B' (= 43 Byte)
Wert von XX' für HBA und SMC-B: '26' (= 38 Byte)
Wert von 'XX' für die gSMC-K: '30' (= 48 Byte)
Wert von 'XX' für die gSMC-KT: '2B' (= 43 Byte)</td></tr>
<tr><td colspan="2"></td><td>
<table>
<tr><th>Tag</th><th>L</th><th>Wert</th></tr>
<tr><td>'C0'</td><td>'03'</td><td>Versionsnummer der Befüllvorschrift für EF.Version2 (2.0.0) gemäß Kodierung von Versionskennungen</td></tr>
<tr><td>'C1'</td><td>'03'</td><td>Version des dem aktiven Objektsystem zugrundeliegenden Produkttyps (PT_ObjSys) gemäß Kodierung der Versionskennungen</td></tr>
<tr><td>'C2'</td><td>'10'</td><td>Produktidentifikation des aktiven Objektsystems (PI_Objektsystem) gemäß Kodierung von Produktidentifikatoren</td></tr>
<tr><td>'C4'</td><td>'03'</td><td>Versionsnummer der Befüllvorschrift für EF.GDO (1.0.0) gemäß Kodierung der Versionskennungen</td></tr>
<tr><td>'C5'</td><td>'03'</td><td>Versionsnummer der Befüllvorschrift für EF.ATR (2.0.0) gemäß Kodierung der Versi-</td></tr>
</table>
</td></tr>
</table>

Tag	L	Wert		
				onskennungen
		'C6'	'03'	Versionsnummer der Befüllvorschrift für EF.KeyInfo (~~1.0.0~~ 2.0.0) gemäß Kodierung der Versionskennungen (nur gültig für die gSMC-K und die gSMC-KT)
		'C3'	'03'	Versionsnummer der Befüllvorschrift für die Datei EF.EnvironmentSettings (1.0.0) nur gültig für die gSMC-K, sh. Kapitel 5.1
		'C7'	'03'	Versionsnummer der Befüllvorschrift für EF.Logging (1.0.0) gemäß Kodierung der Versionskennungen nur gültig für die eGK, sh. Kapitel 4.1

3.1 EF.KeyInfo (Struktur der Zugriffstabelle)

Die Datei EF.KeyInfo dient der Adressierung der Schlüssel und zugehörigen Zertifikate einer Karte, die aktuell verwendet werden müssen. Bei der Option „Lange Lebensdauer im Feld“ wird nach Ablauf der Nutzbarkeit eines Schlüssels auf einen neuen Schlüssel und das dazugehörende Zertifikat umgeschaltet. Bei diesem Umschalten müssen die Inhalte von EF.KeyInfo entsprechend geändert werden.

Inhalt und Struktur der Datei EF.Keyinfo werden erst festgelegt, wenn Funktionalität und Schnittstellen des Certificate Update Service (CUpS) spezifiziert werden. Die damit einhergehende Befüllvorschrift erhält die Versionsnummer 2.0.0.

~~**Card-G2-A_3499 K_Initialisierung: Speicherstruktur für EF.KeyInfo**~~

~~Die Records der Datei EF.KeyInfo einer Smartcard des Gesundheitswesens MÜSSEN die in Tab_Karten_Fach_TIP_004 festgelegte Struktur aufweisen.~~

~~**Tabelle 1: Tab_Karten_Fach_TIP_004 Struktur der Datei EF.KeyInfo**~~

~~Informations-element~~	~~Länge in Byte~~	~~Typ~~	~~Initialwert~~	~~Bemerkung~~
~~Kennung~~	~~1~~	~~binär~~		~~Kennung für das Schlüsselpaar, z.B. '41' für ID.AK.AUT; '12' für CA_SAK.CS siehe Tab_Karten_Fach_TIP_007 bzw. Tab_Karten_Fach_TIP_009~~
~~Status~~	~~1~~	~~binär~~	~~1~~	~~1 = current; 0 = deprecated~~
~~AID~~	~~16~~	~~binär~~		~~ApplicationId des Ordners, in dem sich sowohl das Zertifikat als auch der private~~

Informations-element	Länge in Byte	Typ	Initialwert	Bemerkung
				Schlüssel befinden siehe Hinweis 1:
FID_Cert	2	binär		FileIdentifier des Zertifikats
SFID_Cert	1	binär		Short File Identifier des Zertifikats
KeyRef	1	binär		KeyReference des privaten Schlüssels siehe Hinweis 1:
CryptSys	6	binär		Kryptosystem gemäß Tab_Karten_Fach_TIP_005
Keylength	2	binär		Schlüssellänge [Bit]
NotAfter	6	BCD	181231	Gültigkeitsende in YYMMDD

Hinweis 1: Wenn die Kodierung des AID kürzer als 16 Byte ist, dann müssen Nullen bis zum Erreichen der Länge 16 Byte vorangestellt werden..

Hinweis 2: Falls ein Schlüssel nicht vorhanden ist, muss KeyRef auf 'FF' gesetzt werden.

Card-G2-A_3500 K_ Initialisierung: Schlüssel und Zertifikat im selben Ordner für EF.KeyInfo

Der private Schlüssel eines Schlüsselpaares und das Zertifikat mit dem zugehörigen öffentlichen Schlüssel MÜSSEN sich auf der Karte im selben Ordner befinden.⌫

Card-G2-A_3501 K_Initialisierung: Kodierung der Kryptosysteme in EF.KeyInfo

Der Wert CryptSys in EF.KeyInfo MUSS entsprechend der Vorgaben in Tab_Karten_Fach_TIP_005 kodiert werden.

Tabelle 2: Tab_Karten_Fach_TIP_005 Liste der Kryptosysteme

System	Kennung
RSA	1
ELC	2

3.1.1 Initiale Belegung der Zugriffstabelle für die gSMC-K für EF.KeyInfo

Card-G2-A_3502 K_Initialisierung: Initiale Belegung von EF.KeyInfo für die gSMC-K

EF.KeyInfo für die gSMC-K MUSS initial entsprechend den Vorgaben in Tab_Karten_Fach_TIP_006 kodiert werden.

Tabelle 3: Tab_Karten_Fach_TIP_006 Initiale Belegung von EF.KeyInfo für gSMC-K (hexadezimale Werte)

Symbol. Name	Status	AID_Cert	FID_Cert	SFID_Cert	KeyRef	CryptSys (siehe Tabelle 5)	Keylength	NotAfter
CA_SAK.CS	1	0	'2F 07'	'07'	'FF'	2	256	YYMMDD
ID.RCA.CS	1	0	'2F15'	'15'	'FF'	2	256	YYMMDD
PrK.KONN.AUT	1	0			'07'	1	2048	0
PrK.GP	1	0			'0C'	1	2048	0
ID.AK.AUT	1	'D276 0001 4402'	'C5 03'	'03'	'83'	1	2048	YYMMDD
PrK.AK.CA_PS	1	'D276 0001 4402'			'88'	1	2048	0
ID.NK.VPN	1	'D276 0001 4403'	'C5 05'	'05'	'85'	1	2048	YYMMDD
PrK.CFS	1	'D276 0001 4403'			'89'	1		0
ID.SAK.AUT	1	'D276 0001 4404'	'C5 06'	'06'	'86'	1	...	YYMMDD
ID.SAK.AUTD_CVC	1	'D276 0001 4404'	'2F 0A'	'0A'	'8A'	2	256	0
PrK.SAK.CA_xTV	1	'D276 0001 4404'			'8B'	1	2048	0
PrK.SAK.SIG	1	'D276 0001 4404'			'94'	1		

Card-G2-A_3503 K_ Initialisierung: Kennungen von EF.KeyInfo für die gSMC-K

Die Kennungen von EF.KeyInfo für die gSMC-K MÜSSEN den Vorgaben in Tab_Karten_Fach_TIP_007 kodiert werden.

Tabelle 4: Tab_Karten_Fach_TIP_007 Liste der Kennungen für gSMC-K

Symbolischer Name	Kennung	Zertifikatsdatei	Schlüssel
CA_SAK.CS	'12'	C.CA_SAK.CS.xxxx	--
ID.SAK.AUTD_CVC	'13'	EF.C.SAK.AUTD_CVC.xxxx	PrK.SAK.AUTD_CVC.xxxx
PrK.KONN.AUT	'14'	--	PrK.KONN.AUTn.xxxx
PrK.GP	'15'	--	PrK.GPn.xxxx
PuK.RCA.CS	'16'	EF.C.RCA.CS	PuK.RCA.CS
ID.AK.AUT	'41'	EF.C.AK.AUTn.xxxx	PrK.AK.AUTn.xxxx
PrK.AK.CA_PS	'42'	--	PrK.AK.CA_PSn.xxxx
ID.NK.VPN	'51'	EF.C.NK.VPNn.xxxx	PrK.NK.VPNn.xxxx
PrK.CFS	'52'	--	PrK.CFSn.xxxx
ID.SAK.AUT	'61'	EF.C.SAK.AUTn.xxxx	PrK.SAK.AUTn.xxxx
PrK.SAK.CA_xTV	'62'	--	PrK.SAK.CA_xTVn.xxxx
PrK.SAK.SIG	'63'	--	PrK.SAK.SIGn.xxxx

3.1.2 Initiale Belegung der Zugriffstabelle für die gSMC-KT für EF.KeyInfo

Card-G2-A_3504 K_Initialisierung: Initiale Belegung von EF.KeyInfo für die gSMC-KT

EF.KeyInfo für die gSMC-KT MUSS initial entsprechend den Vorgaben in Tab_Karten_Fach_TIP_008 kodiert werden.

Tabelle 5: Tab_Karten_Fach_TIP_008 Initiale Belegung von EF.KeyInfo für gSMC-KT (hexadezimale Werte) // zu ergänzen

Symbol. Name	Status	AID_Cert	FID_Cert	SFID_Cert	KeyRef	CryptSys (siehe Tabelle 5	Keylength	NotAfter

CA_SMC.CS	1	0	'2F 07'	'07'	'FF'	2	256	YYMMDD
ID.SMC.AUTD_RPS_CVC	1	0	'2F 0A'	'0A'	'0A'	2	256	YYMMDD
ID.SMKT.AUT	1	'D276000144 00'	'C5 01'	'01'	'82'	1	2048	YYMMDD
SMKT.CA	1	'D276000144 00'	'C5 02'	'02'	'FF'	1	2048	YYMMDD

Card-G2-A_3505 K_ Initialisierung: Kennungen von EF.KeyInfo für die gSMC-KT

Die Kennungen von EF.KeyInfo für die gSMC-KT MÜSSEN den Vorgaben in Tab_Karten_Fach_TIP_009 kodiert werden.

Tabelle 6: Tab_Karten_Fach_TIP_009 Liste der Kennungen für gSMC-KT

Symbolischer Name	Kennung	Zertifikatsdatei	Schlüssel
CA_SAK.CS	'12'	C.CA_SAK.CS.xxxx	–
ID.SMC.AUTD_RPS_CVC	'13'	EF.C.SMC.AUTD_RPS_CVC.xxxx	PrK.SMC.AUTD_RPS_CVC.xxxx
ID.SMKT.AUT	'71'	EF.C.SMKT.AUTn.xxxx	PrK.SMKT.AUTn.xxxx
SMKT.CA	'72'	EF.C.SMKT.CAn.xxxx	–

4.2 Testkennzeichen (EF.TTN) (informativ, Platzhalter)

Die Datei EF.TTN dient zur Aufnahme des Testkennzeichens. Das Testkennzeichen kann Informationen über die Teilnahme an Testmaßnahmen enthalten. Im Rahmen von OPB1 ORS1 wird kein Testkennzeichen genutzt, EF.TTN bleibt leer.“

4.3 Vorlage für Fachanwendungen der eGK (informativ)

Tabelle 7: Tab_Karten_Fach_TIP_011 Struktur der Datei EF.Status<Fachanwendung> für eine Fachwendung

Informations-element	Länge in Byte	Typ	Initialwert	Bemerkung
Status	1	ALPHA	„0“	„1“ = Transaktionen offen „0“ = keine Transaktionen offen
Timestamp	14	ALPHA	Siehe 1.	Timestamp in UTC der letzten Aktualisierung der <Fachanwendung> im Format YYYYMMDDhhmmss
Version fachliches Informationsmodell	5	BCD	0x0000000000	Version des fachlichen Informationsmodells, z.B. des XSD-Schema.
Version fachliche Speicherstruktur	5	BCD	0x0000000000	Version der fachlichen Speicherstruktur. ~~Eine individuelle Versionierung der fachlichen Speicherstrukturen findet erst für eGKs statt, bei denen das Informationselement „Version der Speicherstrukturen“ aus EF.Version größer gleich 4.0.0 ist. Ansonsten wird dieses Feld nicht verwendet und ist reserviert.~~
Das Informationselement Timestamp wird mit dem Zeitstempel des Personalisierungszeitpunktes (UTC) vorbelegt.				

Anpassung der Produkttypsteckbriefe Konnektor und eHealth-KT

Diese Anpassung umfasst Änderungen an Prüfverfahren von Anforderungen.

Aus folgenden Gründen ist diese Anpassung notwendig:

1. Anforderungen sind im Funktionsumfang VSDM-Konnektor (PTV1) nicht relevant und daher aus PTV1 zu entfernen.
2. Anforderungen sind im Blackbox-Verfahren nicht testbar und daher nur über eine Herstellererklärung nachzuweisen.
3. Anforderungen können nur zum Teil durch Blackbox-Tests nachgewiesen werden. Nicht testbare Aspekte der Anforderung sind über Herstellererklärung zu belegen.
4. Anforderungen sind weder im Funktionsumfang VSDM-Konnektor (PTV1) noch im QES-Konnektor (PTV2) testbar und sind daher über eine Herstellererklärung nachzuweisen. Hierzu zählen auch TUCs, die nicht aufgerufen werden.
5. Anforderungen beschreiben keine funktionalen Eigenschaften des Produkts und sind daher nicht über Test, sondern eine Herstellererklärung nachzuweisen.
6. Übergreifende Anforderung wird durch konkrete Anforderungen bereits abgedeckt.
7. Anforderung wurde fälschlicherweise dem Sicherheitsgutachten der gSMC-K-Personalisierung bzw. gSMC-KT-Personalisierung zugeordnet.
8. Korrekturen der Zuordnung zur sicherheitstechnischen Eignung „CC-Evaluierung“.
9. Anforderungen müssen allein oder zusätzlich zu anderen Prüfverfahren über eine Herstellererklärung nachgewiesen werden.

Änderungen in gemProdT_Kon_PTV1:

Tabelle 1: Anforderungen zur funktionalen Eignung „Produkttest / Produktübergreifender Test“

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
~~TIP1-A_5541~~	~~Referenzen in Dokumenten nicht dynamisch auflösen~~	~~gemSpec_Kon~~	1
~~TIP1-A_4712~~	~~Protokollierung erfolgreicher Kryptooperationen~~	~~gemSpec_Kon~~	1
~~TIP1-A_4506~~	~~Initiale Identitäten der gSMC-K~~	~~gemSpec_Kon~~	2
~~TIP1-A_4981~~	~~Steuerung der Betriebsumgebung via gSMC-K~~	~~gemSpec_Kon~~	2
~~TIP1-A_4790~~	~~TUC_KON_351 „Liefere Systemzeit“~~	~~gemSpec_Kon~~	4
~~TIP1-A_4575~~	~~TUC_KON_209 „LeseRecord“~~	~~gemSpec_Kon~~	4
~~TIP1-A_4803~~	~~TUC_KON_363 „Dienstdetails abrufen“~~	~~gemSpec_Kon~~	4
~~TIP1-A_4707~~	~~Betrieb in Test- und Referenzumgebung~~	~~gemSpec_Kon~~	2
~~VSDM-A_2665~~	~~Fachmodul VSDM: Ereignisdienst - für Topics registrieren~~	~~gemSpec_FM_VSDM~~	2

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
~~VSDM-A_2208~~	~~Fachmodul VSDM: beliebige Reihenfolge der Header-Elemente~~	~~gemSpec_SST_VSDM~~	4
~~GS-A_4865~~	~~Versionierte Liste zulässiger Firmware-Versionen~~	~~gemSpec_OM~~	5
~~GS-A_3696~~	~~Zeitpunkt der Erzeugung neuer Versionsnummern~~	~~gemSpec_OM~~	5
~~GS-A_4868~~	~~Aufsteigende Nummerierung der Firmware-Gruppen~~	~~gemSpec_OM~~	5
~~GS-A_4864~~	~~Logging-Vorgaben nach dem Übergang zum Produktivbetrieb~~	~~gemSpec_OM~~	4
~~GS-A_3816~~	~~Festlegung sicherheitsrelevanter Fehler~~	~~gemSpec_OM~~	6
~~GS-A_4869~~	~~Firmware-Gruppe mindestens eine Firmware-Version~~	~~gemSpec_OM~~	5
~~GS-A_3806~~	~~Loglevel in der Referenz- und Testumgebung~~	~~gemSpec_OM~~	5
~~GS-A_5054~~	~~Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen~~	~~gemSpec_OM~~	5
~~TIP1-A_3315~~	~~Inhalt Update-Paket - DokumentationFiles~~	~~gemSpec_KSR~~	5
~~TIP1-A_6108~~	~~FirmwareGroupInfo.xml Signatur~~	~~gemSpec_KSR~~	5
~~TIP1-A_6112~~	~~Name des Update-Paketes~~	~~gemSpec_KSR~~	5
~~TIP1-A_6113~~	~~Definition Update-Paket-Struktur~~	~~gemSpec_KSR~~	5
~~TIP1-A_6114~~	~~Passwort des Update-Paketes~~	~~gemSpec_KSR~~	5
~~TIP1-A_6115~~	~~Größe des Update-Paketes~~	~~gemSpec_KSR~~	5
~~TIP1-A_6116~~	~~Update-Paket - Dateinamen und Unterverzeichnisse~~	~~gemSpec_KSR~~	5
~~TIP1-A_6117~~	~~Referenzierungen des Update-Paketes~~	~~gemSpec_KSR~~	5
~~TIP1-A_6118~~	~~Zusätzliche Dateien im Update-Paket~~	~~gemSpec_KSR~~	5
~~TIP1-A_6120~~	~~Update-Paket - Dateinamen der UpdateInformation Detached-Signatur~~	~~gemSpec_KSR~~	5
~~TIP1-A_6121~~	~~Update-Paket - Dateinamen der FirmwareGroupInfo Detached-Signatur~~	~~gemSpec_KSR~~	5
~~TIP1-A_6122~~	~~Pfadreferenz~~	~~gemSpec_KSR~~	5
~~TIP1-A_6123~~	~~Update-Paket - Signatur~~	~~gemSpec_KSR~~	5
~~TIP1-A_6131~~	~~FirmwareGroupInfo.xml - Format~~	~~gemSpec_KSR~~	5
~~TIP1-A_5570~~	~~LDAP-Client, TUC_VZD_0001 „search_Directory"~~	~~gemSpec_VZD~~	1
~~TIP1-A_6132~~	~~Detached-Signature der FirmwareGroupInfo.xml~~	~~gemSpec_KSR~~	5
~~TIP1-A_6133~~	~~FirmwareGroupInfo.xml - Element „FirmwareGroupSignature"~~	~~gemSpec_KSR~~	5

Tabelle 2: Anforderungen zur funktionalen Eignung „Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
TIP1-A_4506	Initiale Identitäten der gSMC-K	gemSpec_Kon	2
TIP1-A_5696	Prüfung der personalisierten gSMC-K	gemSpec_Kon	9
TIP1-A_4981	Steuerung der Betriebsumgebung via gSMC-K	gemSpec_Kon	2
VSDM-A_2665	Fachmodul VSDM: Ereignisdienst - für Topics registrieren	gemSpec_FM_VSDM	2

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
VSDM-A_2208	Fachmodul VSDM: beliebige Reihenfolge der Header-Elemente	gemSpec_SST_VSDM	4
GS-A_4865	Versionierte Liste zulässiger Firmware-Versionen	gemSpec_OM	5
GS-A_4868	Aufsteigende Nummerierung der Firmware-Gruppen	gemSpec_OM	5
TIP1-A_4713	Herstellerspezifische Systemprotokollierung	gemSpec_Kon	3
GS-A_4869	Firmware-Gruppe mindestens eine Firmware-Version	gemSpec_OM	5
GS-A_3806	Loglevel in der Referenz- und Testumgebung	gemSpec_OM	5
GS-A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM	5
GS-A_3816	Festlegung sicherheitsrelevanter Fehler	gemSpec_OM	6
TIP1-A_3315	Inhalt Update-Paket - DokumentationFiles	gemSpec_KSR	5
TIP1-A_6108	FirmwareGroupInfo.xml Signatur	gemSpec_KSR	5
TIP1-A_6112	Name des Update-Paketes	gemSpec_KSR	5
TIP1-A_6113	Definition Update-Paket-Struktur	gemSpec_KSR	5
TIP1-A_6114	Passwort des Update-Paketes	gemSpec_KSR	5
TIP1-A_6115	Größe des Update-Paketes	gemSpec_KSR	5
TIP1-A_6116	Update-Paket - Dateinamen und Unterverzeichnisse	gemSpec_KSR	5
TIP1-A_6117	Referenzierungen des Update-Paketes	gemSpec_KSR	5
TIP1-A_6118	Zusätzliche Dateien im Update-Paket	gemSpec_KSR	5
TIP1-A_6120	Update-Paket - Dateinamen der UpdateInformation Detached-Signatur	gemSpec_KSR	5
TIP1-A_6121	Update-Paket - Dateinamen der FirmwareGroupInfo Detached-Signatur	gemSpec_KSR	5
TIP1-A_6122	Pfadreferenz	gemSpec_KSR	5
TIP1-A_6123	Update-Paket - Signatur	gemSpec_KSR	5
TIP1-A_6131	FirmwareGroupInfo.xml - Format	gemSpec_KSR	5
TIP1-A_6132	Detached-Signature der FirmwareGroupInfo.xml	gemSpec_KSR	5
TIP1-A_6133	FirmwareGroupInfo.xml - Element „FirmwareGroupSignature“	gemSpec_KSR	5
TIP1-A_4790	TUC_KON_351 „Liefere Systemzeit“	gemSpec_Kon	4
TIP1-A_4803	TUC_KON_363 „Dienstdetails abrufen“	gemSpec_Kon	4
TIP1-A_4575	TUC_KON_209 „LeseRecord“	gemSpec_Kon	4

Tabelle 3: Anforderungen zur sicherheitstechnischen Eignung „CC-Evaluierung“

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
TIP1-A_4710	Protokollierung personenbezogener und medizinischer Daten	gemSpec_Kon	8
~~GS-A_4386~~	~~TLS-Verbindungen, optional Version 1.1~~	~~gemSpec_Krypt~~	8
~~GS-A_5542~~	~~TLS-Verbindungen (fatal Alert bei Abbrüchen)~~	~~gemSpec_Krypt~~	8

Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
~~TIP1-A_5696~~	~~Prüfung der personalisierten gSMC-K~~	~~gemSpec_Kon~~	7

Änderungen in gemProdT_Kon_PTV2:

Tabelle 5: Anforderungen zur funktionalen Eignung „Produkttest/Produktübergreifender Test“

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
~~TIP1-A_4506~~	~~Initiale Identitäten der gSMC-K~~	~~gemSpec_Kon~~	2
~~TIP1-A_4981~~	~~Steuerung der Betriebsumgebung via gSMC-K~~	~~gemSpec_Kon~~	2
~~TIP1-A_4575~~	~~TUC_KON_209 „LeseRecord“~~	~~gemSpec_Kon~~	4
~~TIP1-A_4790~~	~~TUC_KON_351 „Liefere Systemzeit“~~	~~gemSpec_Kon~~	4
~~TIP1-A_4803~~	~~TUC_KON_363 „Dienstdetails abrufen“~~	~~gemSpec_Kon~~	4
~~TIP1-A_4707~~	~~Betrieb in Test- und Referenzumgebung~~	~~gemSpec_Kon~~	2
~~VSDM-A_2665~~	~~Fachmodul VSDM: Ereignisdienst - für Topics registrieren~~	~~gemSpec_FM_VSDM~~	2
~~VSDM-A_2208~~	~~Fachmodul VSDM: beliebige Reihenfolge der Header-Elemente~~	~~gemSpec_SST_VSDM~~	4
~~GS-A_4865~~	~~Versionierte Liste zulässiger Firmware-Versionen~~	~~gemSpec_OM~~	5
~~GS-A_3696~~	~~Zeitpunkt der Erzeugung neuer Versionsnummern~~	~~gemSpec_OM~~	5
~~GS-A_4868~~	~~Aufsteigende Nummerierung der Firmware-Gruppen~~	~~gemSpec_OM~~	5
~~GS-A_4864~~	~~Logging-Vorgaben nach dem Übergang zum Produktivbetrieb~~	~~gemSpec_OM~~	4
~~GS-A_3816~~	~~Festlegung sicherheitsrelevanter Fehler~~	~~gemSpec_OM~~	6
~~GS-A_4869~~	~~Firmware-Gruppe mindestens eine Firmware-Version~~	~~gemSpec_OM~~	5
~~GS-A_3806~~	~~Loglevel in der Referenz- und Testumgebung~~	~~gemSpec_OM~~	5
~~GS-A_5054~~	~~Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen~~	~~gemSpec_OM~~	5
~~TIP1-A_3315~~	~~Inhalt Update-Paket - DokumentationFiles~~	~~gemSpec_KSR~~	5
~~TIP1-A_6108~~	~~FirmwareGroupInfo.xml Signatur~~	~~gemSpec_KSR~~	5
~~TIP1-A_6112~~	~~Name des Update-Paketes~~	~~gemSpec_KSR~~	5
~~TIP1-A_6113~~	~~Definition Update-Paket-Struktur~~	~~gemSpec_KSR~~	5
~~TIP1-A_6114~~	~~Passwort des Update-Paketes~~	~~gemSpec_KSR~~	5
~~TIP1-A_6115~~	~~Größe des Update-Paketes~~	~~gemSpec_KSR~~	5
~~TIP1-A_6116~~	~~Update-Paket - Dateinamen und Unterverzeichnisse~~	~~gemSpec_KSR~~	5
~~TIP1-A_6117~~	~~Referenzierungen des Update-Paketes~~	~~gemSpec_KSR~~	5
~~TIP1-A_6118~~	~~Zusätzliche Dateien im Update-Paket~~	~~gemSpec_KSR~~	5
~~TIP1-A_6120~~	~~Update-Paket - Dateinamen der UpdateInformation Detached-Signatur~~	~~gemSpec_KSR~~	5
~~TIP1-A_6121~~	~~Update-Paket - Dateinamen der FirmwareGroupInfo Detached-Signatur~~	~~gemSpec_KSR~~	5
~~TIP1-A_6122~~	~~Pfadreferenz~~	~~gemSpec_KSR~~	5
~~TIP1-A_6123~~	~~Update-Paket - Signatur~~	~~gemSpec_KSR~~	5

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
~~TIP1-A_6131~~	~~FirmwareGroupInfo.xml - Format~~	~~gemSpec_KSR~~	5
~~TIP1-A_6132~~	~~Detached-Signature der FirmwareGroupInfo.xml~~	~~gemSpec_KSR~~	5
~~TIP1-A_6133~~	~~FirmwareGroupInfo.xml - Element „FirmwareGroupSignature“~~	~~gemSpec_KSR~~	5

Tabelle 6: Anforderungen zur funktionalen Eignung „Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
TIP1-A_4506	Initiale Identitäten der gSMC-K	gemSpec_Kon	2
TIP1-A_5696	Prüfung der personalisierten gSMC-K	gemSpec_Kon	9
TIP1-A_4981	Steuerung der Betriebsumgebung via gSMC-K	gemSpec_Kon	2
VSDM-A_2665	Fachmodul VSDM: Ereignisdienst - für Topics registrieren	gemSpec_FM_VSDM	2
VSDM-A_2208	Fachmodul VSDM: beliebige Reihenfolge der Header-Elemente	gemSpec_SST_VSDM	4
GS-A_4865	Versionierte Liste zulässiger Firmware-Versionen	gemSpec_OM	5
GS-A_4868	Aufsteigende Nummerierung der Firmware-Gruppen	gemSpec_OM	5
TIP1-A_4713	Herstellerspezifische Systemprotokollierung	gemSpec_Kon	3
GS-A_4869	Firmware-Gruppe mindestens eine Firmware-Version	gemSpec_OM	5
GS-A_3806	Loglevel in der Referenz- und Testumgebung	gemSpec_OM	5
GS-A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM	5
GS-A_3816	Festlegung sicherheitsrelevanter Fehler	gemSpec_OM	6
TIP1-A_3315	Inhalt Update-Paket - DokumentationFiles	gemSpec_KSR	5
TIP1-A_6108	FirmwareGroupInfo.xml Signatur	gemSpec_KSR	5
TIP1-A_6112	Name des Update-Paketes	gemSpec_KSR	5
TIP1-A_6113	Definition Update-Paket-Struktur	gemSpec_KSR	5
TIP1-A_6114	Passwort des Update-Paketes	gemSpec_KSR	5
TIP1-A_6115	Größe des Update-Paketes	gemSpec_KSR	5
TIP1-A_6116	Update-Paket - Dateinamen und Unterverzeichnisse	gemSpec_KSR	5
TIP1-A_6117	Referenzierungen des Update-Paketes	gemSpec_KSR	5
TIP1-A_6118	Zusätzliche Dateien im Update-Paket	gemSpec_KSR	5
TIP1-A_6120	Update-Paket - Dateinamen der UpdateInformation Detached-Signatur	gemSpec_KSR	5
TIP1-A_6121	Update-Paket - Dateinamen der FirmwareGroupInfo Detached-Signatur	gemSpec_KSR	5
TIP1-A_6122	Pfadreferenz	gemSpec_KSR	5
TIP1-A_6123	Update-Paket - Signatur	gemSpec_KSR	5
TIP1-A_6131	FirmwareGroupInfo.xml - Format	gemSpec_KSR	5
TIP1-A_6132	Detached-Signature der FirmwareGroupInfo.xml	gemSpec_KSR	5
TIP1-A_6133	FirmwareGroupInfo.xml - Element	gemSpec_KSR	5

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
	„FirmwareGroupSignature“		
TIP1-A_4790	TUC_KON_351 „Liefere Systemzeit“	gemSpec_Kon	4
TIP1-A_4803	TUC_KON_363 „Dienstdetails abrufen“	gemSpec_Kon	4
TIP1-A_4575	TUC_KON_209 „LeseRecord“	gemSpec_Kon	4

Tabelle 7: Anforderungen zur sicherheitstechnischen Eignung „CC-Evaluierung“

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
~~TIP1-A_5663~~	~~Prüfung der technischen Rolle bei TLS-Verbindungsaufbau zum TSL-Dienst~~	~~gemSpec_Kon~~	8
TIP1-A_4710	Protokollierung personenbezogener und medizinischer Daten	gemSpec_Kon	8
~~GS-A_4386~~	~~TLS-Verbindungen, optional Version 1.1~~	~~gemSpec_Krypt~~	8
~~GS-A_5542~~	~~TLS-Verbindungen (fatal Alert bei Abbrüchen)~~	~~gemSpec_Krypt~~	8
GS-A_5484	TUC_PKI_036 „BNetzA-VL-Aktualisierung“	gemSpec_PKI	8

Tabelle 8: Anforderungen zur sicherheitstechnischen Eignung „Sicherheitsgutachten“

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
~~TIP1-A_5696~~	~~Prüfung der personalisierten gSMC-K~~	~~gemSpec_Kon~~	7

Änderungen in gemProdT_KT:

Tabelle 2: Anforderungen zur funktionalen Eignung „Produkttest/Produktübergreifender Test“

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
~~TIP1-A_6120~~	~~Update-Paket - Dateinamen der UpdateInformation Detached-Signatur~~	~~gemSpec_KSR~~	5

Tabelle 9: Anforderungen zur funktionalen Eignung „Herstellererklärung“

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
TIP1-A_7016	Prüfung der personalisierten gSMC-KT	gemSpec_KT	9
TIP1-A_6120	Update-Paket - Dateinamen der UpdateInformation Detached-Signatur	gemSpec_KSR	5

Tabelle 10: Anforderungen zur sicherheitstechnischen Eignung „CC-Evaluierung“

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
~~GS-A_5542~~	~~TLS-Verbindungen (fatal Alert bei Abbrüchen)~~	~~gemSpec_Krypt~~	8

Tabelle 11: Anforderungen zur sicherheitstechnischen Eignung „Sicherheitsgutachten“

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)	Grund
~~TIP1-A_6720~~	~~Verwendung zugelassener Gerätekarten gSMC-KT~~	~~gemSpec_KT~~	7
~~TIP1-A_7016~~	~~Prüfung der personalisierten gSMC-KT~~	~~gemSpec_KT~~	7

Konsistenzfehler in den Objektsystemspezifikationen

1 Motivation

Nach der Veröffentlichung der Dokumente wurde festgestellt, dass es Inkonsistenzen zwischen [gemSpec_COS] einerseits und den Objektsystemspezifikationen andererseits gibt bzw. Inkonsistenzen zwischen Festlegungen innerhalb einer Objektsystemspezifikation auftreten. Betroffen sind alle G2.1-Objektsystemspezifikationen.

2 Dokumentenübergreifende Befunde

2.1 Attribute *pointInTime*

Hintergrundinformation: Gemäß [gemSpec_COS#(N019.900)] besitzt das Objektsystem ein Attribut *pointInTime*, welches gemäß [gemSpec_COS#(N008.120)] als Datum in der Form YYMMDD, also zweistellige Jahreszahl, gefolgt von einer zweistelligen Monatsangabe, gefolgt von einer zweistelligen Tagesangabe, zu codieren ist. Deshalb ist der Wert ‚000000' keine gültige Datumsangabe.

Tabelle 1: Anforderungen zum Attribut *pointInTime*

Dokument	betroffene Anforderung
[gemSpec_eGK_ObjSys]	Card-G2-A_3265
[gemSpec_HBA_ObjSys]	Card-G2-A_3266
[gemSpec_SMC-B_ObjSys]	Card-G2-A_3267
[gemSpec_gSMC-KT_ObjSys]	Card-G2-A_3269

Der Inhalt der in Tabelle 1 genannten Anforderungen wird wie folgt überarbeitet:

ersetze:
~~Das Attribut pointInTime MUSS den Wert '0000-0000-0000' = 2000.00.00 haben. Der Wert MUSS initialisiert werden.~~

durch:
Der Hersteller des Objektsystems MUSS das Attribut *pointInTime* im Rahmen der Initialisierung auf den Wert von CED (Certificate Effective Date) aus dem selbst signierten CV-Zertifikat zu PuK.RCA.CS setzen.

2.2 Attribut *accessRulesPublicSignatureVerificationObject*

Hintergrundinformation: Die Spezifikation von Zugriffsregeln ist nur für die Interfaces und die Werte von *lifeCycleStatus* sinnvoll, die im realen Betrieb auftreten. Die Vorgabe für irrelevante Interfaces und irrelevante Werte von *lifeCycleStatus* ist Speicherplatzverschwendung.

Tabelle 2: Anforderungen zum Attribut *accessRulesPublicSignatureVerificationObject*

Dokument	betroffenes Objekt	betroffene Anforderung
[gemSpec_eGK_ObjSys]	PuK.RCA.CS.E256	Card-G2-A_2380-01
	PuK.RCA.ADMINCMS.CS.E256	Card-G2-A_2986-01

Bei den in Tabelle 2 genannten Anforderungen wird der Inhalt der Spalte „Wert“ für das Attribut *accessRulesPublicSignatureVerificationObject* ersetzt durch folgenden Inhalt:

> Für alle relevanten Interfaces und alle relevanten Werte von *lifeCycleStatus* gilt:
> DELETE →AUT_CMS
> PSO Verify Certificate → ALWAYS

Tabelle 3: Anforderungen zum Attribut *accessRulesPublicSignatureVerificationObject*

Dokument	betroffenes Objekt	betroffene Anforderung
[gemSpec_HBA_ObjSys]	PuK.RCA.CS.R2048	Card-G2-A_2077-01
	PuK.RCA.CS.E256	Card-G2-A_2078-01
	PuK.RCA.ADMINCMS.CS.E256	Card-G2-A_3016-01
[gemSpec_SMC-B_ObjSys]	PuK.RCA.CS.R2048	Card-G2-A_2191-01
	PuK.RCA.CS.E256	Card-G2-A_2192-01
	PuK.RCA.ADMINCMS.CS.E256	Card-G2-A_3039-01
[gemSpec_gSMC-KT_ObjSys]	PuK.RCA.CS.E256	Card-G2-A_2514-01
	PuK.RCA.ADMINCMS.CS.E256	Card-G2-A_3028-01

Bei den in Tabelle 3 genannten Anforderungen ist das Löschrecht teilweise nicht eingeschränkt und teilweise an einen Administrator gebunden. Zur Klarstellung und zur Vereinheitlichung wird der Inhalt der Spalte „Wert“ für das Attribut *accessRulesPublicSignatureVerificationObject* ersetzt durch folgenden Inhalt:

> Für alle relevanten Interfaces und alle relevanten Werte von *lifeCycleStatus* gilt:
> DELETE → ~~ALWAYS~~ AUT_CMS OR AUT_CUP
> PSO Verify Certificate → ALWAYS

2.3 Attribut *accessRulesPublicAuthenticationObject*

Die Spezifikation von Zugriffsregeln ist nur für die Interfaces und die Werte von *lifeCycleStatus* sinnvoll, die im realen Betrieb auftreten. Die Vorgabe für irrelevante Interfaces und irrelevante Werte von *lifeCycleStatus* ist Speicherplatzverschwendung.

Tabelle 4: Anforderungen zum Attribut *accessRulesPublicAuthenticationObject*

Dokument	betroffenes Objekt	betroffene Anforderung
[gemSpec_eGK_ObjSys]	PuK.RCA.CS.E256	Card-G2-A_2380-01
[gemSpec_HBA_ObjSys]	PuK.RCA.CS.R2048	Card-G2-A_2077-01
	PuK.RCA.CS.E256	Card-G2-A_2078-01
[gemSpec_SMC-B_ObjSys]	PuK.RCA.CS.R2048	Card-G2-A_2191-01
	PuK.RCA.CS.E256	Card-G2-A_2192-01
[gemSpec_gSMC-KT_ObjSys]	PuK.RCA.CS.E256	Card-G2-A_2514-01

Änderung 1: Bei den in Tabelle 4 genannten Anforderungen wird der Inhalt der Spalte „Wert“ für das Attribut *accessRulesPublicAuthenticationObject* ersetzt durch folgenden Inhalt:

> Für alle relevanten Interfaces und alle relevanten Werte von *lifeCycleStatus* gilt:
> DELETE → ALWAYS
> ~~GENERAL AUTHENTICATE → ALWAYS~~
> EXTERNAL AUTHENTICATE → ALWAYS

Tabelle 5: Anforderungen zum Attribut *accessRulesPublicAuthenticationObject*

Dokument	betroffenes Objekt	betroffene Anforderung
[gemSpec_eGK_ObjSys]	PuK.RCA.ADMINCMS.CS.E256	Card-G2-A_2986-01
[gemSpec_HBA_ObjSys]	PuK.RCA.ADMINCMS.CS.E256	Card-G2-A_3016-01
[gemSpec_SMC-B_ObjSys]	PuK.RCA.ADMINCMS.CS.E256	Card-G2-A_3039-01
[gemSpec_gSMC-KT_ObjSys]	PuK.RCA.ADMINCMS.CS.E256	Card-G2-A_3028-01

Änderung 2: Bei den in Tabelle 5 genannten Anforderungen wird der Inhalt der Spalte „Wert“ für das Attribut *accessRulesPublicAuthenticationObject* ersetzt durch folgenden Inhalt:

> Für alle relevanten Interfaces und alle relevanten Werte von *lifeCycleStatus* gilt:
> DELETE → ALWAYS
> ~~GENERAL AUTHENTICATE → ALWAYS~~

Änderung 3: In den Kapiteln zu den in Tabelle 4 genannten Objekten wird folgender Hinweis ergänzt:

Hinweis (1): Es ist möglich, dass importierte Authentisierungsschlüssel auch zum Aufbau eines Trusted Channels verwendet werden. Dabei wird das Kommando GENERAL AUTHENTICATE verwendet. Deshalb ist es erforderlich, dass importierte Authentisierungsschlüssel das

Kommando GENERAL AUTHENTICATE unterstützen. Die Zugriffsart GENERAL AUTHENTICATE fehlt in der oben genannten Zugriffsregel, weil gemäß [gemSpec_COS] dabei lediglich für private Schlüssel, nicht aber für öffentliche Schlüssel Zugriffsregeln ausgewertet werden. Falls das herstellerspezifische COS im Rahmen eines GENERAL AUTHENTICATE Kommandos auch Zugriffsregeln für öffentliche Schlüssel auswertet, dann ist eine entsprechende Zugriffsart herstellerspezifisch mit der Zugriffsbedingung ALWAYS zu ergänzen.

2.4 Attribut numberScenario

Hintergrundinformation: Gemäß [gemSpec_COS#(N017.430)] darf das Attribut *numberScenario* bei einem privaten ELC Schlüssel nur dann vorhanden sein, falls dieser den Algorithmus elcAsynchronAdmin unterstützt.

Tabelle 6: Anforderungen zum Attribut *accessRulesPublicAuthenticationObject*

Dokument	betroffenes Objekt	betroffene Anforderung
[gemSpec_eGK_ObjSys]	PrK.CH.AUT.E256	Card-G2-A_3611
	PrK.CH.AUTN.E256	Card-G2-A_3613
	PrK.CH.ENC.E256	Card-G2-A_3615
	PrK.CH.ENCV.E256	Card-G2-A_3617
	PrK.CH.QES.E256	Card-G2-A_3621
[gemSpec_HBA_ObjSys]	PrK.HP.QES.E256	Card-G2-A_3629
	PrK.HP.AUT.E256	Card-G2-A_3639
	PrK.HP.ENC.E256	Card-G2-A_3641
[gemSpec_SMC-B_ObjSys]	PrK.HCI.OSIG.E256	Card-G2-A_3658
	PrK.HCI.AUT.E256	Card-G2-A_3660
	PrK.HCI.ENC.E256	Card-G2-A_3662

Bei den in Tabelle 6 genannten Objekten wird das Attribut *numberScenario* ersatzlos gestrichen.

3 Dokumentenspezifische Befunde

3.1 Befunde zu [gemSpec_eGK_ObjSys]

3.1.1 MRPIN und LCS=deactivated

Die MRPINs der Fachanwendungen wurden in das MF verschoben. Damit ist der Zustand LCS="operational state (deactivated)" für die Beurteilung der Zugriffsregeln irrelevant. Deshalb werden für folgende Objekte die Zugriffsregeln für LCS="operational state (deactivated)", die derzeit objektspezifisch sind, einheitlich auf „herstellerspezifisch" geändert, sowohl für die kontaktbehaftete, als auch für die kontaktlose Schnittstelle:

1) MRPIN.NFD, siehe Card-G2-A_2408-01
2) MRPIN.DPE, siehe Card-G2-A_2413-01
3) MRPIN.GDD, siehe Card-G2-A_2417-01
4) MRPIN.OSE, siehe Card-G2-A_3236-01
5) MRPIN.AMTS, siehe Card-G2-A_3247-01

Tabelle 7: Neuer Wert der entsprechenden Tabellenzeilen:

Zugriffsregel für logischen LCS „Operational state (deactivated)"		
alle	herstellerspezifisch	

Aus Konsistenzgründen werden die Zugriffsregeln für den logischen LCS = „operational State(deactivated)" von „alle = NEVER" auf „alle = herstellerspezifisch" für jedes Interface geändert

6) MRPIN.NFD_READ siehe Card-G2-A_2864-01
7) PIN.AMTS_REP siehe Card-G2-A_3248-01

3.1.2 EF.VerweiseAMTS und Attribut *flagRecordLCS*

Die Zugriffsregeln des EF.VerweiseAMTS erlauben keine Statusänderungen der Records. Deshalb ist ein Attribut „lifeCycleStatus" für die Records dieser Datei nicht erforderlich, siehe Card-G2-A_3245-01.

flagRecordLCS	~~True~~ False	

3.1.3 MRPIN und Zugriffsregel mit Zugriffsbedingung=NEVER

Die Zugriffsregeln einiger MRPINs enthalten explizite Angaben für die Kommandos Enable- und Disable Verification Requirement für die *nicht* zulässigen Kombinationen des Parameters P1, also Zugriffsregeln, deren Zugriffsbedingung NEVER ist. Diese Angabe ist redundant, da sie in der Zugriffsregel: andere = NEVER enthalten ist. Die Angabe dieser expliziten Regeln für Enable/Disable können daher entfernt werden, die entsprechenden Tabellenzeilen sind zu löschen (für alle Interfaces und LCS)

Objekt	Tabelle	betroffene Anforderung
MRPIN.NFD	Tab_eGK_ObjSys_047	Card-G2-A_2408-01

Objekt	Tabelle	betroffene Anforderung
MRPIN.DPE	Tab_eGK_ObjSys_052	Card-G2-A_2413-01
MRPIN.GDD	Tab_eGK_ObjSys_056	Card-G2-A_2417-01
MRPIN.AMTS	Tab_eGK_ObjSys_194	Card-G2-A_3247-01
MRPIN.NFD_READ	Tab_eGK_ObjSys_092	Card-G2-A_2864-01
PIN.AMTS_REP	Tab-eGK_ObjSys_195	Card-G2-A_3248-01

~~DISABLE_VERIFICATION_REQUIREMENT (P1='1')~~ ~~ENABLE_VERIFICATION_REQUIREMENT (P1='1')~~	~~NEVER~~	

3.1.4 AUT_PACE Nomenklatur für alle Zugriffsregeln

Es sind noch Zugriffsregeln im Dokument vorhanden, die SmMac(SK.CAN) anstelle von AUT_PACE in den Zugriffsregeln verwenden. Gemäß C_5862 hätten diese Stellen schon bei der Erstellung der Version für Generation G2.1 berücksichtigt werden sollen.

Es sind im Dokument alle Vorkommen von SmMac(SK.CAN) in den Beschreibungen von Zugriffsregeln durch AUT_PACE zu ersetzen.

Betroffen sind folgende Anforderungen:

Objekt	Tabelle	betroffene Anforderung
PrK.eGK.AUT_CVC.E256	Tab_eGK_ObjSys_020	Card-G2-A_2377-01
EF.Einwilligung	Tab_eGK_ObjSys_034	Card-G2-A_2395-01
EF.Verweis	Tab_eGK_ObjSys_043	Card-G2-A_2404-01
PrK.CH.AUT.R2048	Tab_eGK_ObjSys_064	Card-G2-A_2437-01
PrK.CH.AUTN.R2048	Tab_eGK_ObjSys_067	Card-G2-A_2440-01
PrK.CH.AUT.E256	Tab_eGK_ObjSys_208	Card-G2-A_3611 (*)
PrK.CH.AUTN.E256	Tab_eGK_ObjSys_210	Card-G2-A_3613 (*)

(*) eine Suffixanpassung ist aufgrund dieser Änderung nicht notwendig, lediglich die Darstellung der Zugriffsbedingung wird angepasst.

3.1.5 Korrektur Schreibfehler im Text

In Kapitel 5.5.3 wird die Bezeichnung ~~PuK.CH.ENC1.R2048~~ auf PuK.CH.ENC.R2048 geändert.

4 Änderungen der AFO Nummerierung durch die dargestellten Änderungen

Die Objektsysteme der Kartengeneration G2.0 und G2.1 sind in OPB1 parallel verfügbar. Einige der von der Änderung betroffenen AFOs sind jedoch zurzeit (vor der Änderung) in G2.0 und G2.1 identisch. Da durch die Änderung hier die G2.1-Variante von der G2.0-Variante abweicht, muss dies durch eine neue bzw. eine erweiterte Nummer mit Suffix abgebildet werden.

Existierende Nummern mit Suffix treten zurzeit ausschließlich in G2.1 auf. Da diese schon veröffentlicht sind, ist hier eine Erhöhung des Suffixes notwendig.

4.1 Liste aller durch die Änderungen dieses Dokuments betroffenen AFOs

Alt, bisher	Neu, wird zu
Card-G2-A_3265	Card-G2-A_3265-01
Card-G2-A_3266	Card-G2-A_3266-01
Card-G2-A_3267	Card-G2-A_3267-01
Card-G2-A_3268	Card-G2-A_3268-01
Card-G2-A_3269	Card-G2-A_3269-01
Card-G2-A_2380-01	Nur Inhalt geändert
Card-G2-A_2986-01	Nur Inhalt geändert
Card-G2-A_2077-01	Nur Inhalt geändert
Card-G2-A_2078-01	Nur Inhalt geändert
Card-G2-A_3016	Card-G2-A_3016-01
Card-G2-A_2191-01	Nur Inhalt geändert
Card-G2-A_2192-01	Nur Inhalt geändert
Card-G2-A_3039-01	Nur Inhalt geändert
Card-G2-A_2514-01	Nur Inhalt geändert
Card-G2-A_3028-01	Nur Inhalt geändert
Card-G2-A_3611	Card-G2-A_3611-01
Card-G2-A_3613	Card-G2-A_3613-01
Card-G2-A_3615	Card-G2-A_3615-01
Card-G2-A_3617	Card-G2-A_3617-01
Card-G2-A_3629	Card-G2-A_3629-01
Card-G2-A_3639	Card-G2-A_3639-01
Card-G2-A_3641	Card-G2-A_3641-01
Card-G2-A_3658	Card-G2-A_3658-01
Card-G2-A_3658	Card-G2-A_3658-01

Alt, bisher	Neu, wird zu
Card-G2-A_3660	Card-G2-A_3660-01
Card-G2-A_3662	Card-G2-A_3662-01
Card-G2-A_2408-01	Nur Inhalt geändert
Card-G2-A_2413-01	Nur Inhalt geändert
Card-G2-A_3236-01	Nur Inhalt geändert
Card-G2-A_3247-01	Nur Inhalt geändert
Card-G2-A_2417-01	Nur Inhalt geändert
Card-G2-A_3245-01	Nur Inhalt geändert
Card-G2-A_2864-01	Nur Inhalt geändert
Card-G2-A_3248-01	Nur Inhalt geändert
Card-G2-A_2377-01	Nur Inhalt geändert
Card-G2-A_2395-01	Nur Inhalt geändert
Card-G2-A_2404-01	Nur Inhalt geändert
Card-G2-A_2437-01	Nur Inhalt geändert
Card-G2-A_2440-01	Nur Inhalt geändert

5 Mitgeltende/betroffene Dokumente

[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.10.0, https://www.gematik.de
[gemSpec_eGK_ObjSys]	gematik: Spezifikation der elektronischen Gesundheitskarte, eGK-Objektsystem, Version 4.0.0, https://www.gematik.de
[gemSpec_HBA_ObjSys]	gematik: Spezifikation des elektronischen Heilberufsausweises, HBA-Objektsystem, Version 4.0.0, https://www.gematik.de
[gemSpec_SMC-B_ObjSys]	gematik: Spezifikation der Security Module Card SMC-B, Objektsystem, Version 4.0.0, https://www.gematik.de
[gemSpec_gSMC-KT_ObjSys]	gematik: Spezifikation der gSMC-KT – Objektsystem, Version 4.0.0, https://www.gematik.de

Um das Erfüllen der Anforderung GS-A_5327 nachvollziehbar und reproduzierbar sicherzustellen, hat es sich als notwendig erwiesen, den Messaufbau für diese Anforderung zu normieren. Zu diesem Zweck wird mit diesem Change der Anhang D der [gemSpec_Perf] hinzugefügt.

In diesem Zusammenhang wurden die Bearbeitungsvorgaben für 25MB-Dokumente angepasst, da sich die in Tab_gemSpec_Perf_Konnektor aufgeführten Werte als nicht sachgerecht herausgestellt hatten. Die Anpassung von Tab_gemSpec_Perf_Konnektor und Tab_gemSpec_Perf_Konnektorbearbeitungszeiten_pro_Komponente an sachgerechte Werte wird in einem nachfolgenden Change vorgenommen, sobald die dafür notwendigen Untersuchungen abgeschlossen sind.

Änderungsbedarf in gemSpec_Perf

4.1.2 Produkttyp Konnektor

Skalierbarkeit

⌦ **GS-A_5327 Performance - Konnektor - Skalierbarkeit**

Der Konnektor MUSS die von 8 durchschnittlichen Anwendungen erzeugte Last im vorgegebenen Bearbeitungszeitrahmen für die vorgesehene Leistungserbringerumgebung bedienen können. Dabei wird die erzeugte Last einer durchschnittlichen Anwendung als die durch Tabelle Tab_gemSpec_Perf_Konnektor definierte Last (VSDM, KOM-LE, QES) geteilt durch 3 definiert. ⌫

Der Test von [GS-A_5327] erfolgt für den VSDM-Konnektor anhand eines QES-Produktmusters. Das QES-Produktmuster muss dafür funktional nur soweit implementiert sein, dass eine Überprüfung der Bearbeitung paralleler Requests unter der Ziellast möglich ist. Welche Tests durchgeführt werden und welche Eigenschaften dafür beim QES-Produktmuster erforderlich sind, beschreibt „Anhang D – Performancerelevante Produktmustereigenschaften des QES-Konnektors“.

~~Die Eigenschaft wird wie folgt getestet:~~

~~Für die in Tabelle Tab_gemSpec_Perf_Konnektor angegebenen Operationen mit Lastangabe wird für alle Operationen gemeinsam eine Testanfragenrate erzeugt, die eine den Lastangaben für diese Leistungserbringerumgebung entsprechende Zusammenstellung von Aufrufen repräsentiert. Die Anfrageraten werden zusätzlich um den Faktor 8/3 erhöht. Die Aufrufe müssen innerhalb der Antwortzeitvorgaben korrekt bearbeitet werden.~~

Anhang D - Performancerelevante Produktmustereigenschaften des QES-Konnektors

Im Folgenden werden die erforderlichen, performance-relevanten Produktmustereigenschaften des QES-Konnektors festgelegt, auf deren Basis die zum

Nachweis von [GS-A_5327] erforderlichen Performance-Messungen durchgeführt werden können.

Entsprechend der Lastvorgaben aus [GS-A_5327] für 8 Anwendungen wird das Messverfahren festgelegt. Auf Grund der unterschiedlichen Lastanforderungen für die beiden Ausprägungsformen „Einbox-Konnektor“ und „HighSpeed-Konnektor“ wird das Verfahren für beide Fälle dargestellt.

Aus den Lastvorgaben in Tab_gemSpec_Perf_Konnektor und dem Skalierungsfaktor 8/3 wird die perspektivische Last für 8 Anwendungen berechnet. Dabei werden jeweils Operationen mit 25MB-Dokumenten und Operationen mit 100kB-Dokumenten als eine Klasse betrachtet. Die Wahrscheinlichkeit, dass n parallele Bearbeitungen zu einem Zeitpunkt stattfinden, ergibt sich als Poisson-Verteilung mit dem Erwartungswert „Last * Mittlere Bearbeitungszeit“.

Einbox-Konnektor

Tab_gemSpec_Perf_Einbox_Konnektor_Last_8_Anwendungen

					Wahrscheinlichkeit für n parallele Aufrufe zu einem Zeitpunkt				
	Last [1/h]	Last *8/3 [1/h]	Mittlere Bearb.z. μ_o^{SOLL} [ms]	Last * Mittlere Bearb.z. [Anzahl]	0	1	2	3	4
I_Sign_Operations:: sign_Document (100 kB, LE-U2)	389	1037	840	0,24					
I_Sign_Operations:: sign_Document (25 MB)	13	35	7300	0,07					
I_Sign_Operations:: verify_Document (100 kB, LE-U2)	297	792	1430	0,31					
I_Sign_Operations:: verify_Document (25 MB)	13	35	7900	0,08					
I_Crypt_Operations:: encrypt_Document (100 kB, LE-U2)	258	688	1880	0,36					
I_Crypt_Operations:: encrypt_Document (25 MB)	13	35	6700	0,07					
I_Crypt_Operations:: decrypt_Document (100 kB, LE-U2)	258	688	510	0,10					
I_Crypt_Operations:: decrypt_Document (25 MB)	13	35	8900	0,09					
Operationen 25 MB Dokument	52	140	7700	0,30	74%	22%	3%	0%	0%
Operation 100 kB Dokument	1202	3205	1165	1,04	35%	37%	19%	7%	2%

In der Lastsituation für 8 Anwendungen ergeben sich verschiedene Situationen in Bezug auf die parallele Bearbeitung von Anfragen, dargestellt in Tabelle Tab_gemSpec_Perf_Einbox_Konnektor_Lastsituationen. In Situation 1 bearbeitet der Konnektor weder Operationen mit 25 MB-Dokumenten noch solche mit 100kB-Dokumenten. In den Situationen 2 und 5 bearbeitet der Konnektor genau jeweils ein Dokument. In den übrigen Situationen liegt parallele Verarbeitung vor.

Tab_gemSpec_Perf_Einbox_Konnektor_Lastsituationen

Lastsituationen i			
i	Parallele Bearbeitungen mit 25 MB Dokumenten [Anzahl]	Parallele Bearbeitungen mit 100 kB Dokumenten [Anzahl]	Wahrscheinlichkeit p_i
1	0	0	26%
2	0	1	27%
3	0	2	14%
4	0	3	5%
5	1	0	8%
6	1	1	8%
7	1	2	4%
8	1	3	1%

Für jede der Lastsituationen i in Tab_gemSpec_Perf_Einbox_Konnektor_Lastsituationen ist eine Messreihe zu erstellen. In jeder Messreihe sind vom Clientsystem jeweils ein Aufruferthread pro parallele Bearbeitung zu starten, der 100mal sign_Document, encrypt_Document, decrypt_Document und verify_Document sequentiell, direkt nacheinander aufruft. In Lastsituation 8 sind es beispielsweise 1 Thread, der 25 MB große Dokumente bearbeitet, und 3 Threads, die 100 kB große Dokumente bearbeiten.

Für jede der Lastsituationen i und der Operationen o sind die Mittelwerte ${\mu_{i,o}}^{IST}$ der Bearbeitungszeiten für die beiden Klassen 25MB-Dokumente und 100kB-Dokumente zu bestimmen.

Durch den Test ist nachzuweisen, dass die über die Lastsituationen gemittelte Bearbeitungszeit ${\mu_o}^{IST}$ für jede Operation o kleiner als die vorgegebene Bearbeitungszeit ${\mu_o}^{SOLL}$ gemäß Tab_gemSpec_Perf_Einbox_Konnektor_Last_8_Anwendungen ist:

$$ {\mu_o}^{IST} < {\mu_o}^{SOLL} $$

${\mu_o}^{IST}$ wird für 100 kB Dokumente wie folgt gemittelt:

$$ {\mu_o}^{IST} = \frac{p_2{\mu_{2,o}}^{IST} + p_3{\mu_{3,o}}^{IST} + p_4{\mu_{4,o}}^{IST} + p_6{\mu_{6,o}}^{IST} + p_7{\mu_{7,o}}^{IST} + p_8{\mu_{8,o}}^{IST}}{p_2 + p_3 + p_4 + p_6 + p_7 + p_8} $$

${\mu_o}^{IST}$ wird für 25 MB Dokumente wie folgt gemittelt:

$$\mu_o{}^{IST} = \frac{p_5\mu_{5,o}{}^{IST} + p_6\mu_{6,o}{}^{IST} + p_7\mu_{7,o}{}^{IST} + p_8\mu_{8,o}{}^{IST}}{p_5 + p_6 + p_7 + p_8}$$

HighSpeed-Konnektor

Tab_gemSpec_Perf_HighSpeed_Konnektor_Last_8_Anwendungen

					Wahrscheinlichkeit für n parallele Aufrufe zu einem Zeitpunkt							
	Last [1/h]	Last *8/3 [1/h]	Mittlere Bearb.z. $\mu_o{}^{SOLL}$ [ms]	Last * Mittlere Bearb.z. [Anzahl]	0	1	2	3	4	5	6	7
I_Sign_Operations:: sign_Document (100 kB, LE-U4)	1459	3891	840	0,91								
I_Sign_Operations:: sign_Document (25 MB)	13	35	7300	0,07								
I_Sign_Operations:: verify_Document (100 kB, LE-U4)	857	2285	1430	0,91								
I_Sign_Operations:: verify_Document (25 MB)	13	35	7900	0,08								
I_Crypt_Operations:: encrypt_Document (100 kB, LE-U4)	575	1533	1880	0,80								
I_Crypt_Operations:: encrypt_Document (25 MB)	13	35	6700	0,06								
I_Crypt_Operations:: decrypt_Document (100 kB, LE-U4)	575	1533	510	0,22								
I_Crypt_Operations:: decrypt_Document (25 MB)	13	35	8900	0,09								
Operationen mit 25 MB Dokument	52	139	7700	0,30	74%	22%	3%	0%	0%	0%	0%	0%
Operationen mit 100 kB Dokument	3466	9243	1165	2,99	5%	15%	22%	22%	17%	10%	5%	2%

In der Lastsituation für 8 Anwendungen ergeben sich verschiedene Situationen in Bezug auf die parallele Bearbeitung von Anfragen, dargestellt in Tabelle Tab_gemSpec_Perf_HighSpeed_Konnektor_Lastsituationen.

Tab_gemSpec_Perf_HighSpeed_Konnektor_Lastsituationen

Situationen i			
i	Parallele Bearbeitungen mit 25 MB Dokumenten [Anzahl]	Parallele Bearbeitungen mit 100 kB Dokumenten [Anzahl]	Wahrscheinlichkeit p_i
1	0	0	4%
2	0	1	11%
3	0	2	17%
4	0	3	17%
5	0	4	12%
6	0	5	7%
7	0	6	4%
8	0	7	2%
9	1	0	1%
10	1	1	3%
11	1	2	5%
12	1	3	5%
13	1	4	4%
14	1	5	2%
15	1	6	1%
16	2	3	3%

Für jede der Lastsituationen i in Tab_gemSpec_Perf_HighSpeed_Konnektor_Lastsituationen ist eine Messreihe zu erstellen. In jeder Messreihe sind vom Clientsystem jeweils ein Aufruferthread pro parallele Bearbeitung zu starten, der 100 mal sign_Document, encrypt_Document, decrypt_Document und verify_Document sequentiell, direkt nacheinander aufruft. In Lastsituation 16 sind es beispielsweise 2 Threads, die 25 MB große Dokumente bearbeiten, und 3 Threads, die 100 kB große Dokumente bearbeiten.

Für jede der Lastsituationen i und die Operationen o sind die Mittelwerte ${\mu_{i,o}}^{IST}$ der Bearbeitungszeiten für die beiden Klassen 25 MB-Dokumente und 100 kB-Dokumente zu bestimmen.

Durch den Test ist nachzuweisen, dass die über die Lastsituationen gemittelte Bearbeitungszeit ${\mu_o}^{IST}$ für jede Operation o kleiner als die vorgegebene Bearbeitungszeit ${\mu_o}^{SOLL}$ gemäß Tab_gemSpec_Perf_HighSpeed_Konnektor_Last_8_Anwendungen ist:

$$ {\mu_o}^{IST} < {\mu_o}^{SOLL} $$

${\mu_o}^{IST}$ wird für 100 kB Dokumente wie folgt gemittelt:

$$\mu_o{}^{IST} = \frac{\sum_{i=2,3,4,5,6,7,8,10,11,12,13,14,15} p_i \mu_{i,o}{}^{IST}}{\sum_{i=2,3,4,5,6,7,8,10,11,12,13,14,15} p_i}$$

$\mu_0{}^{IST}$ wird für 25 MB Dokumente wie folgt gemittelt:

$$\mu_o{}^{IST} = \frac{\sum_{i=9}^{16} p_i \mu_{i,o}{}^{IST}}{\sum_{i=9}^{16} p_i}$$

Rahmenbedingungen

Folgende konkretisierende Rahmenbedingungen gelten für Einbox-Konnektoren und HighSpeed-Konnektoren gleichermaßen:

- Die Messungen werden mit den Referenzdokumenten TIFF_25MB und TEXT_100KB durchgeführt.
- Es wird im Offline Modus (MGM_LU_ONLINE = Disabled) getestet.
- Pro Aufruferthread wird eine Karte und ein Kartenterminal für Signatur und Entschlüsselung eingesetzt.
- Die „Mittlere Bearbeitungszeit Soll“ in Tab_gemSpec_Perf_HighSpeed_Konnektor_Last_8_Anwendungen basiert auf Kartenterminal- und Kartenzeiten von:
  - Sign_Document: 520 ms
  - Decrypt_Document: 340 ms

  Weichen die in den Messungen durchgeführten Rahmenbedingungen hiervon ab, müssen die Werte entsprechend auf diese Rahmenbedingungen korrigiert werden.
- Wenn der Konnektor 1Gbit/s am LAN-Anschluss unterstützt, müssen die Performancevorgaben für Signatur- und Verschlüsselungsdienst in einem LAN nachgewiesen werden, das 1Gbit/s Bandbreite ermöglicht.
- Für die einzelnen Operationen wird konkretisiert:
  - sign_Document: CAdES Signatur (detached) des Gesamtdokuments, nonQES
  - verify_Document: Signatur verifizieren, die in sign_Document erzeugt wurde, IncludeRevocationInfo=false
  - encrypt_Document: TIFF_dokument, CMS-Verschlüsselung, ein Empfänger
  - decrypt_Document: Dokument entschlüsseln, das mit encrypt_Document verschlüsselt wurde.

Änderungsbedarf:

Durch C_6010 wurden die berufmäßigen Gehilfen von Psychotherapeuten als zugriffsberechtigt auf die medizinischen Anwendungen der eGK ausgewiesen. Diese Aussage ist rechtlich nicht zulässig und muss aus den Dokumenten der gematik wieder entfernt werden.

Darüber hinaus muss in den Dokumenten klargestellt werden, dass die SMC-B der Psychotherapeuten einen Zugriff auf die medizinischen Anwendungen der eGK ermöglicht, dieser Zugriff aber nur dem Psychotherapeuten selbst gestattet ist.

Folgende Konzepte und Spezifkationen werden dahingehend angepasst:

gemKPT_Arch_TIP
gemSpec_PKI

Änderungen in gemKPT_Arch_TIP

2.6 Rollen der TI-Plattform

2.6.1 Personenkreise der Telematikinfrastruktur

[...]

~~Obwohl nicht namentlich benannt, erstreckt sich der Personenkreis 5 ebenfalls auf berufsmäßige Gehilfen von psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten.~~

[…]

Änderungen in gemSpec_PKI

5.3 SMC-B – Ausweis einer Organisation/Einrichtung des Gesundheitswesens

[…]

Tabelle 50: Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung

Profile / Akteure / Rollen und OID aus gemSpec_PKI					X.509 Admission Extension	
Zugriffs-profil	**Kartentyp**	**Beschreibung fachlicher Akteur**	**Fachliche Rolle**	**Qualifizierende Stelle**	**professionItem**	**OID-Referenz**
[…]						
4						

Profile / Akteure / Rollen und OID aus gemSpec_PKI					X.509 Admission Extension	
Zugriffs-profil	**Kartentyp**	**Beschreibung fachlicher Akteur**	**Fachliche Rolle**	**Qualifizierende Stelle**	**professionItem**	**OID-Referenz**
CHA.4	SMC–B	Institutionskarte eines Psychotherapeuten. Der mit der Karte mögliche Zugriff auf die medizinischen Anwendungen der eGK ist ausschließlich dem psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten selbst gestattet und nicht seinen berufsmäßigen Gehilfen.	nicht definiert	KV	Betriebsstätte Psychotherapeut	oid_praxis_psychotherapeut
[…]						

Für die SMC-B-KTR ist im Dokumentenpaket G2.1 ein X.509-Zertifikatsprofil aufgenommen worden. Die Einträge in der Profiltabelle sind bisher jedoch alle als „offen" gekennzeichnet. Mit dieser Änderung werden die sektorspezifischen Anteile festgelegt.

Änderungen in gemSpec_PKI

Es wird Kap. 4.7.2.1 wie folgt angepasst

4.7.2.1 Sektoraler Präfix

…

Tabelle 14: Tab_PKI_101 Normative Festlegung für das Präfix der Telematik-ID.

Präfix	Sektor	Zuständige Organisationen
1	Ärzteschaft	BAEK, KBV
2	Zahnärzteschaft	BZÄK, KZBV
3	Apothekerschaft	BAK
4	Psychotherapeutenschaft	BPTK
5	Krankenhaus	DKG
6	reserviert	
7	reserviert	
8	Kostenträger	GKV-SV

…

Es wird Anhang A4 wie folgt angepasst

A4 – GKV-Spitzenverband

Die nachfolgende Profiltabelle des GKV-Spitzenverbandes gilt für Betriebsstätten bzw. Geschäftsstellen der gesetzlichen Krankenkassen.

Tabelle 117: Tab_SMCB_KTR SMC-B-Zertifikate für Mitarbeiter Kostenträger

Element	Inhalt	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	*siehe Kap 5.3.4*		

Element				Inhalt	Kar.	
		serialNumber		*siehe Kap 5.3.4*		
		signature		*siehe Kap 5.3.4*		
		issuer		*siehe Kap 5.3.4*		
		validity		*siehe Kap 5.3.4*		
		subject				
			commonName	~~offen~~Kurzbezeichnung der Krankenkasse gemäß Freigabedaten des GKV-SV	~~**~~)1	
			title	~~offen~~nicht belegt	~~**~~)0	
			givenName	~~offen~~nicht belegt	~~**~~)0	
			surName	~~offen~~nicht belegt	~~**~~)0	
			serialNumber	~~offen~~TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	~~**~~)1	
			organizationalUnitName	~~offen~~nicht belegt	~~**~~)0	
			organizationName	~~offen~~8-stellige eindeutige Betriebsnummer (BBNR) der Krankenkassenhauptverwaltung gemäß Freigabedaten des GKV-SV	~~**~~)1	
			streetAddress	~~offen~~Straßenanschrift und Hausnummer des Krankenkassenhauptsitzes gemäß Freigabedaten des GKV-SV	~~**~~)1	
			postalCode	~~offen~~Postleitzahl des Krankenkassenhauptsitzes gemäß Freigabedaten des GKV-SV (Deutsche PLZ werden 5-stellig abgebildet)	~~**~~)1	
			localityName	~~offen~~Stadt des Krankenkassenhauptsitzes gemäß Freigabedaten des GKV-SV	~~**~~)1	
			stateOrProvinceName	~~offen~~nicht belegt	~~**~~)0	
			countryName	*siehe Kap 5.3.4*		
			andere Attribute	*siehe Kap 5.3.4*		
		subjectPublicKeyInfo		*siehe Kap 5.3.4*		
		extensions				critical
			SubjectKeyIdentifier {2 5 29 14}	*siehe Kap 5.3.4*		FALSE
			KeyUsage {2 5 29 15}	*siehe Kap 5.3.4*		**TRUE**
			SubjectAltNames {2 5 29 17}	~~offen~~ otherName (s. Tab_PKI_228) type-id= {2 5 4 3}; value=ggf. überlange Bezeichnung der Krankenkasse oder Ergänzungen	~~**~~)0-1	FALSE
			BasicConstraints {2 5 29 19}	*siehe Kap 5.3.4*		**TRUE**
			CertificatePolicies {2 5 29 32}	*siehe Kap 5.3.4*		FALSE
			CRLDistributionPoints {2 5 29 31}	~~offen~~nicht belegt	~~**~~)0	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap 5.3.4*		FALSE
			AuthorityKeyIdentifier	*siehe Kap 5.3.4*		FALSE

Element				Inhalt	Kar.	
			{2 5 29 35}			
			Admission {1 3 36 8 3 3}	~~offen~~ admissionAuthority = {O=GKV-Spitzenverband,C=DE} professionItem = Beschreibung zu <oid_kostentraeger> gemäß [gemSpec_OID#GS-A_4443] professionOID = OID <oid_kostentraeger> gemäß [gemSpec_OID#GS-A_4443] registrationNumber = siehe Tabelle Tab_SMCB_TID_GKVSV	~~**)~~ 1 1 1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	*siehe Kap 5.3.4*	*)	FALSE
			andere Erweiterungen		0	
		signatureAlgorithm		*siehe Kap 5.3.4*		
		signature		*siehe Kap 5.3.4*		

**) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.*

~~***) Kardinalität ist offen, abhängig von der Festlegung in der jeweiligen Inhalts-Spalte.*~~

Tabelle 1: Tab_SMCB_TID_GKVSV Aufbau Telematik-ID in SMC-B-Zertifikaten des GKV-SV

Präfix s. Kap 4.7.2.1	Separator s. Kap 4.7.2.2	Fortsatz s. Kap 4.7.2.3
8 (Kostenträger)	-	8-stellige eindeutige Betriebsnummer (BBNR) des GKV-SV

Die TSP-ID Tabelle, die in verschiedenen Zertifikats-Profilen als Bestandteil der *subjectSerialNumber* aufgeführt ist, ist bisher nur innerhalb des Anhangs A1 – KZBV vollständig dargestellt.

Um diese Tabelle innerhalb der Zertifikats-Profile eindeutig referenzieren zu können, wird die Tabelle in den allgemeinen Teil der Spezifikation verschoben und jeweils Referenzen auf diese Tabelle aufgeführt. Dazu werden folgende Änderungen vorgenommen.

Änderungen in gemSpec_PKI

Es wird Kap. 4.8.3.1 wie folgt angepasst

4.8.3.1 serialNumber

Wird zur Eindeutigkeit von Zertifikaten innerhalb der TI und zur Identifizierung von Zertifikaten verschiedener TSPs, das Präfix TSP-ID innerhalb der *subjectSerialNumber* genutzt, so werden die Werte folgender Tabelle Tab_PKI_109 verwendet.

Tabelle 112: Tab_PKI_109 Werte für das Präfix <TSP-ID>

Präfix <TSP-ID>	Zertifizierungsdiensteanbieter
10	*D-TRUST*
11	*Signtrust*
12	*T-Systems Telesec*
13	*S-Trust*
14	*TC TrustCenter*
15	*DGN*
16	*medisign*

Der Nummernraum des Präfixes wird durch die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) verwaltet.

Im Falle der Clusterung von Diensten besteht evtl. die Notwendigkeit jeder Instanz ein eigenes Zertifikat auszustellen. Damit die Eindeutigkeit des SubjectDN im jeweiligen Zertifikat gewährleistet ist, kann die Ausprägung der Instanz in das Feld serialNumber übernommen werden.

…

Es wird Kap. 5.2.1 wie folgt angepasst

5.2.1 X.509 Zertifikatsprofile des HBA

…

Zusatzinformationen zu einzelnen Feldern:

….

- **SubjectSerialNumber**

  Zusätzliche Hinweise gemäß Informationen aus bisherigen Sektor-Spezifikationen:
  Das Attribut serialNumber im ENC und AUT-Zertifikat soll den gleichen Wert wie im QES-Zertifikat haben. Hiermit soll ermöglicht werden, dass mit einem präsentierten AUT-Zertifikat leichter das entsprechende ENC-Zertifikat desselben HBAs, mittels Konstruktion des DN, aufgefunden werden kann.

  Bildungs-Vorschlag für subjectSerialNumber:

  subjectSerialNumber = <TSP-ID>.<ICCSN>

  (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)

  Hinweis: Statt der ICCSN in der Bildungsregel können auch andere TSP-spezifische IDs verwendet werden, die der Länge der ICCSN entsprechen.

Es werden die Anhänge A1, A2, A3 und A5 wie folgt angepasst

A1 – KZBV

Tabelle 1: Tab_SMCB_KZBV_ZA SMC-B-Zertifikate für Zahnarzt (Sektor KZBV)

Element			Inhalt	Kar.	
certificate			C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
	tbsCertificate				
		version	siehe Kap 5.3.4		
		serialNumber	siehe Kap 5.3.4		
		signature	siehe Kap 5.3.4		
		issuer	siehe Kap 5.3.4		
		validity	siehe Kap 5.3.4		
		subject			
		commonName	Gemäß Freigabedaten der zuständigen KZV	1	
		title	nicht belegt	0	
		givenName	nicht belegt	0	
		surName	nicht belegt	0	
		serialNumber	TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN> ~~(die <TSP-ID> wird für Zertifikatsprofile~~	1	

Element				Inhalt	Kar.	
				~~dieses Sektors von der KZBV vergeben)~~ (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)		
			…			

…

Tabelle 111: Tab_SMCB_KZBV_KZV SMC-B-Zertifikate für KZV (Sektor KZBV)

Element			Inhalt	Kar.	
certificate			C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
	tbsCertificate				
		version	siehe Kap 5.3.4		
		serialNumber	siehe Kap 5.3.4		
		signature	siehe Kap 5.3.4		
		issuer	siehe Kap 5.3.4		
		validity	siehe Kap 5.3.4		
		subject			
		commonName	Gemäß Freigabedaten der KZBV	1	
		title	nicht belegt	0	
		surName	nicht belegt	0	
		givenName	nicht belegt	0	
		serialNumber	TI-weit eindeutiger Identifier der Karte ~~z.B.~~ in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	1	
		…			

…

**) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.*

~~**Tabelle 112: Tab_SMCB_TSP-ID Werte für dasPräfix <TSP-ID>**~~

~~Präfix <TSP-ID>~~	~~Zertifizierungsdiensteanbieter~~
~~*10*~~	~~*D-TRUST*~~
~~*11*~~	~~*Signtrust*~~
~~*12*~~	~~*T-Systems Telesec*~~
~~*13*~~	~~*S-Trust*~~
~~*14*~~	~~*TC TrustCenter*~~
~~*15*~~	~~*DGN*~~
~~*16*~~	~~*medisign*~~

A2 – KBV

Die nachfolgende Profiltabelle der durch die KBV betreuten Sektoren gilt für die Sektoren:

- Niedergelassene Vertragsärzte (KV)
- Niedergelassene Psychologische Psychotherapeuten (KV)
- Niedergelassene Kinder- und Jugendlichenpsychotherapeuten (KV)

Tabelle 113: Tab_SMCB_KV-T SMC-B-Zertifikate für Sektoren der KBV

Element	Inhalt	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	siehe Kap 5.3.4		
serialNumber	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		
issuer	siehe Kap 5.3.4		
validity	siehe Kap 5.3.4		
subject			
commonName	**Erste zwei Zeilen der Anschriftenzone (DIN5008), somit „Kurzname“ der Institution, so wie für das Anschriftenfeld definiert.**	**1**	
title	**Titel des Verantwortlichen/Inhabers**	**0-1**	
givenName	**Vorname des Verantwortlichen/Inhabers (mehrere Vornamen sind durch Blank oder Bindestrich getrennt)**	**0-1**	
surName	**Familienname des Verantwortlichen/Inhabers**	**0-1**	
serialNumber	~~**TI-weit eindeutiger Identifier der Karte z.B. in der Form: <TSP-ID>.<ICCSN>**~~ **nicht belegt**	**0**	
…			

…

A3 – DKG

Die nachfolgende Profiltabelle der DKTIG gilt für den Sektor:

- Krankenhäuser (DKTIG)

Tabelle 2: Tab_SMCB_DKTIG SMC-B-Zertifikate für Sektor der DKTIG

Element	Inhalt	Kar.	

Element			Inhalt	Kar.	
certificate			C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
	tbsCertificate				
		version	siehe Kap 5.3.4		
		serialNumber	siehe Kap 5.3.4		
		signature	siehe Kap 5.3.4		
		issuer	siehe Kap 5.3.4		
		validity	siehe Kap 5.3.4		
		subject			
		commonName	**Gemäss Freigabedaten der DKTIG.**	**1**	
		title	**nicht belegt**	**0**	
		givenName	**nicht belegt**	**0**	
		surName	**nicht belegt**	**0**	
		serialNumber	**TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN>** **(<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)**	**1**	
		…			

…

A5 – Apothekerschaft

Tabelle 118: Tab_SMCB_BAK SMC-B-Zertifikate für Apotheker

Element			Inhalt	Kar.	
certificate			C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
	tbsCertificate				
		version	*siehe Kap 5.3.4*		
		serialNumber	*siehe Kap 5.3.4*		
		signature	*siehe Kap 5.3.4*		
		issuer	*siehe Kap 5.3.4*		
		validity	*siehe Kap 5.3.4*		
		subject			
		commonName	Name der Apotheke	1	
		title	siehe Kap 5.3.4		
		givenName	Vorname des Verantwortlichen/Inhabers (mehrere Vornamen sind durch Blank oder Bindestrich getrennt) *Hinweis: bei mehreren Personen bleibt das Feld leer*	0-1	
		surName	Familienname des Verantwortlichen/Inhabers *Hinweis: bei mehreren Personen bleibt das Feld leer*	0-1	
		serialNumber	TI-weit eindeutiger Identifier der Karte ~~z.B.~~ in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	0-1	

Element	Inhalt	Kar.	
…			

Die Lastvorgaben für OCSP-Responder in GS-A_4159 müssen in folgenden Aspekten angepasst werden:

- Die Lastzahlen berücksichtigen noch nicht die Zahl der tatsächlich vom TSP zu unterstützenden Zertifikate bzw. Karten.
- Die Verweise auf Erprobung sind zu entfernen.
- Es ist zu trennen zwischen einer Last, die bei Zulassung anzuwenden ist, von der Skalierung der Last mit der Anzahl der ausgegebenen Karten im Betrieb.
- Die Anforderung GS-A_4159 wurde im Rahmen der eIDAS-Teil 1 Änderungen inhaltlich so angepasst, dass sie nichts vom OCSP-Proxy verlangt. Sie ist noch in dessen Produkttypsteckbrief aufgeführt. Hier ist sie zu entfernen.

Änderungsbedarf in gemSpec_Perf

Kapitel 4.2.4. Produkttyp Konnektor Produkttypen der PKI – OCSP-Responder

Die Schnittstelle I_OCSP_Status_Information mit der Operation check_Revocation_Status zur Abfrage des Sperrstatus von X.509-Zertifikaten stellen die Produkttypen OCSP-Proxy, TSP-X.509QES und TSP-X.509nonQES bereit. Ausgelöst werden die Aufrufe durch die Prüfung der QES-Signatur durch den HBA, das Prüfen der eGK bei VSD-Anwendungsfällen, beim Prüfen der Datensignatur, beim Zertifikatsprüfen bei der Datenverschlüsselung und beim Verbindungsaufbau zwischen Konnektor und VPN-Konzentrator sowie dem Verbindungsaufbau zwischen Konnektor und VSDM-Intermediär (weitere Verbindungsaufbaue fallen im Vergleich kaum ins Gewicht).

Tabelle 28 Tab_gemSpec_Perf_OCSP_Responder – Last- und Bearbeitungszeitvorgaben

Produkttyp	Funktion	Spitzenlast [1/sec]	Mittelwert [msec]	99%-Quantil [msec]
OCSP-Resp. TSP-X.509QES	Prüfung von HBA-Zertifikaten aus der TI (C.HP.QES): EE-Zert	~~E: 3,3~~ ~~P:~~ 500	2.000	2.400
	Prüfung von HBA-Zertifikaten aus dem Internet (C.HP.QES): EE-Zert	~~E: 1~~ ~~P:~~ 30		
OCSP-Resp. TSP-X.509nonQES	Prüfung von eGK-Zertifikaten aus der TI (C.CH.AUT)	~~E: 7~~ ~~P:~~ 1000	1.000	1.300
	Prüfung von SMC-B-Zertifikaten aus der TI (C.HCI.OSIG)	~~E: 4~~ ~~P:~~ 620		

Produkttyp	Funktion	Spitzenlast [1/sec]	Mittelwert [msec]	99%-Quantil [msec]
	Prüfung von SMC-B-Zertifikaten aus dem Internet (C.HCI.OSIG)	~~E: 1~~ ~~P:~~ 30		
	Prüfung von HBA-Zertifikaten aus der TI (C.HP.ENC)	~~E: 2~~ ~~P:~~ 310		
	Prüfung von HBA-Zertifikaten aus dem Internet (C.HP.ENC)	~~E: 0,1~~ ~~P:~~ 15		
	Prüfung von SMC-B Zertifikaten aus der TI (C.HCI.ENC)	~~E: 2~~ ~~P:~~ 310		
	Prüfung von SMC-B Zertifikaten aus dem Internet (C.HCI.ENC)	~~E: 0,1~~ ~~P:~~ 15		
	Prüfung von Konnektor-Zertifikaten aus der TI (SMC-K, C.NK.VPN)	~~E: 0,6~~ ~~P:~~ 85		
	Prüfung von SMC-B-Zertifikaten aus der TI (C.HCI.AUT)	~~E: 3,0~~ ~~P:~~ 380		
	Prüfung von SMC-B-Zertifikaten aus dem Internet (C.HCI.AUT)	~~E: 0,2~~ ~~P:~~ 30		
	Prüfung von HBA-Zertifikaten aus der TI (C.HP.AUT)	~~E: -~~ ~~P:~~ -		
	Prüfung von HBA-Zertifikaten aus dem Internet (C.HP.AUT)	~~E: 0,2~~ ~~P:~~ 30		
	Prüfung von TLS Zertifikaten der aus der TI zentralen Dienste (C.ZD.TLS)	~~E: 0,6~~ ~~P:~~ 85		
	Prüfung von TLS Zertifikaten der aus der TI Fachdienste (C.FD.TLS)	~~E: 2,0~~ ~~P:~~ 235		
OCSP-Resp. TSL-Dienst	Prüfung des TSL-Signerzertifikats aus der TI	~~E: 0,3~~ ~~P:~~ 45	1.000	1.300
OCSP-Resp. gematik-Root-CA	Prüfung von HBA-Zertifikaten aus dem Internet (C.HP.ENC): CA-Zert	~~E: 0,1~~ ~~P:~~ 15	1.000	1.300

Produkttyp	Funktion	Spitzenlast [1/sec]	Mittelwert [msec]	99%-Quantil [msec]
	Prüfung von HBA-Zertifikaten aus dem Internet (C.HP.AUT): CA-Zert	~~E: 0,2~~ ~~P:~~ 30		
	Prüfung von SMC-B-Zertifikaten aus dem Internet (C.HCI.ENC): CA-Zert	~~E: 0,1~~ ~~P:~~ 15		
	Prüfung von SMC-B-Zertifikaten aus dem Internet (C.HCI.AUT): CA-Zert	~~E: 0,2~~ ~~P:~~ 30		
	Prüfung von SMC-B-Zertifikaten aus dem Internet Root-CA-Zert	~~E: 0,3~~ ~~P:~~ 45		

⌦ **GS-A_5550 Performance – OCSP Responder – Grundlast**

Die Produkttypen TSP-X.509QES, TSP-X.509nonQES, TSL-Dienst und gematik-Root-CA MÜSSEN die Bearbeitungszeitvorgaben aus Tab_gemSpec_Perf_OCSP_Responder unter einer Last von 5 Anfragen pro Sekunde erfüllen. ⌫

⌦ **GS-A_4159 Performance – OCSP Responder – Bearbeitungszeiten unter Spitzenlast**

Die Produkttypen TSP-X.509QES, TSP-X.509nonQES, TSL-Dienst und gematik-Root-CA MÜSSEN die Bearbeitungszeitvorgaben ~~unter Last aus Tab_gemSpec_Perf_OCSP_Responder~~ unter der für alle Funktionen parallel anliegenden Spitzenlast dauerhaft erfüllen. ~~Die Vorgaben gelten gleichermaßen für die Nutzung von innerhalb wie außerhalb der TI.~~

Die dabei geltende Spitzenlast pro Funktion wird aus Tabelle Tab_gemSpec_Perf_OCSP_Responder wie folgt abgeleitet:

- Last für Zertifikate zu HBA und SMC-B = Anzahl der herausgegebenen Karten mit zeitlich noch gültigen Zertifikaten in Tausend / 210 * Spitzenlastwert aus Tabelle Tab_gemSpec_Perf_OCSP_Responder
- Last für Zertifikate zu eGK: Anzahl der herausgegebenen Karten mit zeitlich noch gültigen Zertifikaten in Millionen / 70 * Spitzenlastwert aus Tabelle Tab_gemSpec_Perf_OCSP_Responder
- Last für OCSP-Responder TSL-Dienst und OCSP-Resp. gematik-Root-CA: Spitzenlastwert aus Tabelle Tab_gemSpec_Perf_OCSP_Responder

~~Die Lastvorgaben für die Erprobungsphase (E) sind normativ, während die perspektivischen Vorgaben für den späteren Produktivbetrieb (P) gegebenenfalls unter den in der Erprobung gewonnenen Erkenntnissen angepasst werden.~~ ⌫

Änderungen in Produkttypsteckbriefen

Die Änderung betrifft die folgenden Produkttypsteckbriefe:

- gemProdT_X.509_TSP_nonQES_eGK
- gemProdT_X.509_TSP_nonQES_HBA
- gemProdT_X.509_TSP_nonQES_Komp
- gemProdT_X.509_TSP_nonQES_SMC-B
- gemProdT_X.509_TSP_QES
- gemProdT_TSL
- gemProdT_gematik-Root-CA

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 1: Anforderungen zur funktionalen Eignung "Produkttest / Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5550	Performance – OCSP Responder – Grundlast	gemSpec_Perf
~~GS-A_4159~~	~~Performance – OCSP Responder – Bearbeitungszeiten unter Spitzenlast~~	~~gemSpec_Perf~~

Tabelle 2: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4159	Performance – OCSP Responder – Bearbeitungszeiten unter Spitzenlast	gemSpec_Perf

Weitere Änderung:

In gemProdT_OCSP_Proxy wird die Anforderung GS-A_4159 gelöscht.

Änderungsbedarf:

Folgende Konzepte und Spezifkationen sind von dieser Änderung betroffen:

[gemKPT_Arch_TIP]

[gemSpec_Kon]

[gemILF_PS]

[gemProdT_Kon_PTV1] (Produkttypsteckbrief VSDM-Konnektor)

[gemProdT_Kon_PTV2] (Produkttypsteckbrief QES-Konnektor)

Änderungen in gemKPT_Arch_TIP

5.3.9.1 Konfigurationsmodell des Konnektors

….

~~Neben dem Standalone-Szenario (siehe auch § 291 Abs. 2b Satz 2 SGB V) mit einer physischen Trennung der Umgebung der Clientsysteme und der zentralen TI-Plattform, und dem damit verbunden Einsatz von 2 Konnektoren und 2 eHealth-Kartenterminals, muss entsprechend (LH-BasisTI-A_1981) zusätzlich ein Modus der logischen Trennung ermöglicht werden, in dem lediglich ein Konnektor benötigt wird. In diesem Modus wird durch den Konnektor sichergestellt, dass keine Daten zwischen Clientsystem und der zentralen TI-Plattform oder den fachanwendungsspezifischen Diensten fließen. Die Sicherheitseigenschaft dieser logischen Trennung im Konnektor wird nach einheitlichen Kriterien gemäß Common Criteria (CC) evaluiert und zertifiziert.~~

~~5.3.9.2 Logische Trennung innerhalb des Konnektors~~

~~Für den Konnektor werden nur eingeschränkt Vorgaben zur internen Architektur der Konnektor-Hardware und -Firmware getroffen. Bei derzeitiger Konnektorarchitektur wird das Sicherheitsniveau der logischen Trennung nicht durch den Einsatz zusätzlicher logischer Software-Komponenten (z. B. zwei Fachmodule VSDM zur Unterstützung der logischen Trennung) erhöht. Daher ist es ausreichend, die Konnektorleistungen zur Unterstützung der logischen Trennung an der Außensicht des Konnektor zu definieren. Auch der Einsatz von 2 Kartenterminals zur Separierung von Anwendungsfällen mit Online-Nutzung der TI und rein lokal ablaufenden Anwendungsfällen erhöht das Sicherheitsniveau nicht.~~

~~TIP1-A_2462 Logische Trennung im Konnektor~~

~~Der Konnektor MUSS zur Unterstützung des Standalone-Szenarios einen Modus der logischen Trennung zwischen Clientsystemen und der zentralen TI-Plattform unterstützen.~~

~~Folgende Eigenschaften sind für den Modus der logischen Trennung zu berücksichtigen:~~

- ~~Der Modus der logischen Trennung MUSS durch den Administrator über eine Konfigurationseinstellung aktivierbar und deaktivierbar sein.~~

- ~~Im Modus der logischen Trennung MUSS der Konnektor alle vorgesehenen Funktionen auch mit einem einzelnen angeschlossen Kartenterminal anbieten. Ausgenommen davon sind nur Funktionen deren Erbringung zwei oder mehrere Kartenterminals benötigt, wie z. B. Remote-PIN.~~

- ~~Der Konnektor MUSS jeglichen direkten Netzwerkverkehr zwischen Clientsystemen und der TI unterbinden (Dies schließt speziell auch die Kommunikation zwischen Clientsystemen und Bestandsnetzen ein).~~

- ~~Es MÜSSEN folgende Funktionen (und die hierfür notwendigen Netzwerk- und Infrastrukturdienste) im Konnektor unterstützt werden, die einen Zugriff vom Konnektor auf die zentrale TI-Plattform haben:~~

  - ~~VPN-Verbindung in die zentrale TI-Plattform (I_Secure_Channel_Tunnel)~~
  - ~~Download der TSL (I_TSL_Download)~~
  - ~~alle Anwendungsfälle der Fachanwendung VSDM und die hierfür nötigen Leistungen der TI-Plattform (z.B. Zertifikatsprüfung)~~
  - ~~Unterstützung des Basisdienstes KSR~~

~~Alle anderen Funktionen des Konnektors sowie alle weiteren Fachanwendungen MÜSSEN derart bereitgestellt werden, als wäre keine Online-Anbindung vorhanden.~~

Änderungen in gemSpec_Kon

⌧ TIP1-A_4823 Konnektor mit logischer Trennung

Die Managementschnittstelle MUSS es einem Administrator ermöglichen Konfigurationsänderungen gemäß Tabelle TAB_KON_660 vorzunehmen:

Die Aktivierung der logischen Trennung DARF sich NICHT auf die Anzahl benötigter Kartenterminals auswirken. Alle mit deaktivierter logischer Trennung mit einem Kartenterminal verfügbaren Funktionen des Konnektors müssen auch mit aktivierter logischer Trennung weiterhin mit nur einem Kartenterminal zur Verfügung stehen.

Tabelle 307 TAB_KON_660 Konnektor mit logischer Trennung

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
`MGM_LOGICAL_SEPARATION`	`Enabled / Disabled`	Der Administrator MUSS die logische Separation zwischen TI und lokalem Netz der Einsatzumgebung aktivieren / deaktivieren können. Default-Wert: Disabled Bei Veränderung MUSS TUC_KON_256 gerufen werden {"MGM/LOGICAL_SEP_CHANGED“; Op; Info; „Active=$MGM_LOGICAL_SEPARATION“}

⌫

Das Feature „logische Trennung“ ist abgekündigt und wird in nachfolgenden Versionen der Spezifikation entfernt.

⌦ TIP1-A_XXXX Handbucheintrag zur logischen Trennung

Herrsteller MÜSSEN im Handbuch darauf hinweisen, dass die Konfigurationsmöglichkeit logische Trennung abgekündigt ist und nicht verwendet werden soll. ⌫

Änderung in gemILF_PS

3.1.1 Begriffe der Konfigurationseinheiten

- Online-Konnektor: ~~Logische oder physische Einheit des Konnektors, die~~ Konnektor, der online mit der TI verbunden ist
- Offline-Konnektor: ~~Logische oder physische Einheit des Konnektors, die keinen~~ Konnektor ohne Online-Zugang zur TI ~~besitzt~~.

3.2 Arbeitsplätze in der Leistungserbringerumgebung

Um in der Umgebung des Leistungserbringers die Online-Prüfung und -Aktualisierung durchzuführen, können grundsätzlich ~~drei~~ zwei verschiedene Szenarien verwendet werden, die sich in der Konfiguration der Arbeitsplätze widerspiegeln.

- Online-Szenario am Arbeitsplatz eines Primärsystems mit TI-Anbindung (3.2.1) oder im
- Standalone-Szenario mit Arbeitsplatz/Kartenterminal am Online-Konnektor und Lesen der VSD am Offline-Konnektor (physische Trennung, 3.2.2)
- ~~Szenario mit logischer Trennung (keine Internetverbindung und keine Dienste am Konnektor verfügbar außer VSDM, 3.2.3)~~

3.2.3 Szenario mit logischer Trennung

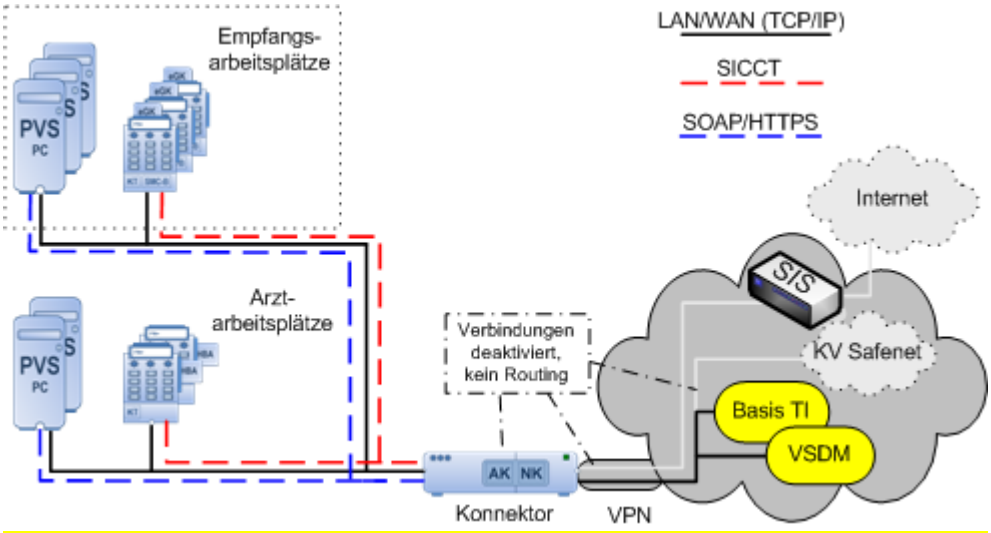

Abbildung 6: Szenario mit logischer Trennung im Konnektor

In diesem Szenario kommt nur ein Konnektor zum Einsatz, dessen Online-Funktionen eingeschränkt sind. Verbindungen in die TI sind nur durch den Konnektor intern oder durch Fachmodule möglich. Die Verbindung in das sichere Internet (SIS) oder andere Dienste außerhalb der TI sind über eine entsprechende Konnektorkonfiguration deaktiviert. Es stehen keinerlei Internet- oder Basis-TI-Dienste für das Clientsystem zur Verfügung. Einzig verfügbare Online-Operation für das Primärsystem ist `ReadVSD`. Details zur Konfiguration und zum Verhalten des Konnektors in diesem Szenario finden sich in [gemSpec_Kon#4.3.6].

Dieses Szenario entspricht für die Fachanwendung VSDM funktional dem Online-Szenario und wird daher für VSDM nicht separat betrachtet. Einziger Unterschied ist die netzwerktechnische Trennung im Konnektor zwischen Praxis und Internet.

4.4.1.7 Qualifizierte elektronische Signatur

Das PS kann Dokumente über den SignatureService des Konnektors qualifiziert signieren, unabhängig vom Szenario (Online-Szenario, Standalone-Szenario mit Online- und Offline-Konnektor, Szenario mit logischer Trennung). Wenn eine OCSP-Anfrage Online durchgeführt werden kann, kann das Ergebnis in die Signatur eingebettet werden, so dass beim Verifizieren bekannt ist, dass das benutzte Zertifikat zum Zeitpunkt der Erstellung gültig war. Das Erstellen einer QES ist ansonsten auch ohne OCSP-Anfrage möglich.

4.5.2 Schnittstellen

Das PS kann eine E-Mail-Kommunikation mittels KOM-LE nur im Online-Modus des Konnektors durchführen (keine logische Trennung, kein Offline-Modus).

Änderungsbedarf in gemSpec_Krypt

In Abschnitt ”3.3.1 IPsec-Kontext” in Anforderung GS-A_4382

⌦ **GS-A_4382 IPsec-Kontext - Schlüsselvereinbarung**

Alle Produkttypen, die die Authentifizierung, den Schlüsselaustausch und die verschlüsselte Kommunikation im IPsec-Kontext durchführen, MÜSSEN die Schlüsselvereinbarung mittels IKEv2 [RFC-~~5996~~7296] gemäß den folgenden Vorgaben durchführen:

[…]

- ~~Rekeying~~ Schlüsselaktualisierung: die IKE-Lifetime darf maximal ~~86400 Sekunden~~ 24*7 Stunden betragen (Reauthentication). Die IPsec-SA-Lifetime darf maximal ~~3600 Sekunden~~ 24 Stunden betragen (Rekeying). Der Initiator soll nach Möglichkeit vor Ablauf der Lifetime das Rekeying anstoßen. Ansonsten muss der Responder bei Ablauf der Lifetime das Rekeying von sich aus sicherstellen, bzw. falls dies nicht möglich ist, die Verbindung beenden.

[…]

- Für die Schlüsselberechnung muss Forward Secrecy [BSI-TR-02102-1, S.ix] (in [RFC-~~5996~~7296] ~~noch~~ „Perfect Forward Secrecy“ genannt) gewährleistet werden. Meint die Wiederverwendung von zuvor schon verwendeten (EC-)Diffie-Hellman-Schlüsseln ([RFC-~~5996~~7296#Abschnitt 2.12]) ist nicht erlaubt.⌫

Weiter in Abschnitt ”3.3.1 IPsec-Kontext”

Ziel ist es zum Zeitpunkt der IKE-SA-Reauthentication ausgeführte Anwendungsfälle nicht zu unterbrechen. Aktuell wird aufgrund von TIP1-A_4492 im Rahmen der Reauthentication dem Konnektor eine neue (i.d.R. andere) VPN-TI-IP-Adresse zugewiesen, was dazu führt, dass bestehende TCP-Verbindungen in die TI effektiv zerstört und laufende Anwendungsfälle unterbrochen werden. Perspektivisch wird die folgende Anforderung als MUSS-Anforderung in TIP1-A_4492 integriert.

⌦ **GS-A_5547 gleiche VPN-IP-Adresse nach Reauthentication**

Der VPN-Zugangsdienst KANN nach einer Reauthentication (vgl. GS-A_4382 Spiegelstrich „Schlüsselaktualisierung“) die gleiche VPN-IP-Adresse wie vor der Reauthentication vergeben. Die Reauthentication ist in Bezug auf TIP1-A_4492 nicht als „neue Verbindung / Neuaufbau des Tunnels“ zu betrachten.⌫

Da noch nicht alle VPN-Zugangsdienste technisch in der Lage sind GS-A_5547 umzusetzen werden als Symptomlinderung die Gültigkeitsdauern der ausgehandelten Schlüssel erhöht, auch in Anbetracht, dass weitere Sicherheitsmaßnahmen (bspw. TIP1-A_5389) umgesetzt werden neben den klassischen Prüfungen, die im Rahmen einer Reauthentication durchgeführt werden.

⌦ **GS-A_5548 Mindestgültigkeitszeiten IKE- und IPsec-SAs (Konnektor)**

Der Konnektor MUSS die Konfiguration der Gültigkeitsdauern der IKE- bzw. IPsec-SAs auf (1) mindestens 90% und (2) kleiner als 100% der in GS-A_4382 Spiegelstrich „Schlüsselaktualisierung“ aufgeführten Maximalwerte setzen.⌫

Auszug Beispielkonfiguration /etc/ipsec.conf

```
ikelifetime=161h
lifetime=23h
margintime = 20m
rekeyfuzz = 40%
keyexchange=ikev2
```

⌦ **GS-A_5549 Mindestgültigkeitszeiten IKE- und IPsec-SAs (VPN-Zugangsdienst)**

Der VPN-Zugangsdienst MUSS die Konfiguration der Gültigkeitsdauern der IKE- bzw. IPsec-SAs auf die in GS-A_4382 Spiegelstrich „Schlüsselaktualisierung“ aufgeführten Maximalwerte setzen.⌫

⌦ **GS-A_5508 IPsec make_before_break**

Alle Produkttypen, die mittels IPsec Daten schützen, SOLLEN die ~~Re-Authentication~~ Reauthentication (vgl. [RFC-7296#2.8.3 „Reauthentication is done by […]“]) durchführen, indem die neue ~~IPsec~~IKE-SA aufgebaut wird bevor die bestehende ~~IPsec~~IKE-SA gelöscht wird. ⌫