Einführung der Gesundheitskarte

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

führt zu

Release 1.6.4-3

Version:	1.0.0
Stand:	06.12.2017
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemErrata_R1.6.4-3]

Betroffene Produkttypen	Neue Produkttypversion
gemProdT_Kon	1.10.3-0
gemProdT_ZentrNetz	1.5.3-1
gemProdT_SG_BestNetze	1.7.0-0
gemProdT_X.509_TSP_nonQES_eGK	1.7.1-0
gemProdT_X.509_TSP_nonQES_HBA	1.7.1-0
gemProdT_X.509_TSP_nonQES_Komp	1.8.0-2
gemProdT_X.509_TSP_nonQES_SMC-B	1.9.1-0
gemProdT_X.509_TSP_QES	1.7.2-0

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	**Anpassungen** an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_6102	gemSpec_Net gemKPT_Arch_TIP	Kap. 2.6.6 Kap. 5.4.8	Mandantenfähigkeit Sicherheitsgateway Bestandsnetze Die Anforderungen an das Sicherheitsgateway Bestandsnetze werden, als Ergebnis der in der Erprobung gewonnenen Daten, geändert. Die bisher geforderte Funktion eines ALG (Application Layer Gateway) wird gestrichen. Für zukünftige weiterer Bestandsnetze, die an die TI angeschlossen werden, wird der Einsatz einer mandantenfähigen Lösung beim Sicherheitsgateway Bestandsnetze gefordert. Dies ermöglicht die logische Aufteilung des Sicherheitsgateways in jeweils eine separate Instanz je angeschlossenes Bestandsnetz. Die Konfiguration des je Bestandsnetz existierenden Regelwerkes erfolgt ohne Beeinflussung anderer angeschlossener Bestandsnetze.	Die Anforderungen GS-A_5055, GS-A_5056 und GS-A_5057 werden ersatzlos gestrichen. gemSpec_Net: neu: ☐GS-A_5507 Sicherheitsgateway Bestandsnetze, Mandantenfähigkeit Der Produkttyp Sicherheitsgateway Bestandsnetze MUSS den Anschluss von mindestens 4 Bestandsnetzen gleichzeitig und voneinander unabhängig an einer Instanz des Sicherheitsgateways ermöglichen. Das Sicherheitsgateway MUSS mindestens als Stateful Inspection Firewall ausgeführt sein. Pro Bestandsnetz MUSS ein separates Regelwerk unterstützt werden. ☐ Die gematik empfiehlt für den Produkttyp Sicherheitsgateway Bestandsnetze, die Verwendung von BSI-zugelassenen IT-Sicherheitsprodukten und -systemen wie in BSI-Schrift 71641 aufgeführt. Für weitere Informationen zum sicheren Einsatz von Komponenten in Sicherheitsgateways wird auf [BSI-SiGw2] verwiesen. [1https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/Liste_Produkte/Liste_Produkte_node.html] [2https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Konz_SiGw_pdf.pdf] Prüfverfahren: Herstellererklärung gemKPT_Arch_TIP: alt: ☐ TIP1-A_2532 Produkttyp Sicherheitsgateway Bestandsnetze, Sicherung ggü. dem Bestandsnetz Der Produkttyp Sicherheitsgateway Bestandsnetze MUSS Richtung Bestandsnetze durch Stateful Inspection Firewalls und ein Applikation Level Gateway gesichert werden. ☐ neu: ☐ TIP1-A_2532 Produkttyp Sicherheitsgateway Bestandsnetze, Sicherung ggü. dem Bestandsnetz Der Produkttyp Sicherheitsgateway Bestandsnetze MUSS Richtung Bestandsnetze durch Stateful Inspection Firewalls gesichert werden. ☐	gemSpec_Net gemProdT_SG_BestNetze gemKPT_Arch_TIP
C_6271	gemSpec_Kon	TIP1-A_4586 Anhang D	Vor der Kommunikation mit dem Konnektor holt sich ein Clientsystem über den Dienstverzeichnisdienst die SOAP-Endpunkte, über die das Clientsystem die einzelnen Dienstoperationen erreichen kann. Diese Endpunkte werden vom Konnektor mit einer Version versehen und das Clientsystem kann anhand der Versionsnummer entscheiden, ob es mit dem Endpunkt kompatibel ist. Dabei sollte das Clientsystem die ersten beiden Stellen der Versionsbezeichnung auswerten. Momentan werden jedoch alle drei Stellen ausgewertet, obwohl die Nummerierung der letzten Stelle einen Versionsfortschritt innerhalb einer zueinander kompatiblen Versionsfamilie abbildet. Daher würde ein Clientsystem, das z.B. die Version 8.1.0 eines Dienstes unterstützt, die Kommunikation mit einem Konnektor ablehnen, der die Version 8.1.1 desselben Dienstes anbietet, obwohl die Version 8.1.1 per Definition abwärtskompatibel zur Version 8.1.0 ist.	Siehe C_6271_Anlage.docx	gemSpec_Kon
C_6274	gemSpec_PKI	Kap. 5	ECC KeyUsage Anpassungen Mit der geplanten Einführung von G2.1-Karten wurde bei allen Zertifikatsprofilen der gematik die Unterstützung des Schlüsselalgorithmus ECDSA vorbereitet. Im Rahmen der ersten Umsetzungsaktivitäten für EE-Zertifikate auf ECDSA-Basis wurde festgestellt, dass bezüglich der KeyUsage Anpassungen für die ECDSA-Ausprägungen der Zertifikatsprofile notwendig sind, um RFC-Konformität zu RFC 5480 zu gewährleisten. Dabei wird ”KeyEncipherment” als KeyUsage nicht mehr für den Schlüsselalgorithmus ECDSA genutzt und dazu in den Zertifikatsprofilen fallweise in der ECDSA-Ausprägung entfernt oder durch ”KeyAgreement” ersetzt. Die existierenden Zertifikatsprofile auf RSA-Basis (G2-Karten) werden nicht angepasst. Die Änderungen wirken sich nur auf die Zulassung von TSPs aus, die Zertifikate für G2.1-Karten ausgeben wollen.	Siehe C_6274_Anlage.docx	gemSpec_PKI, gemProdT_X.509_TSP_nonQES_eGK, gemProdT_X.509_TSP_nonQES_SMC-B, gemProdT_X.509_TSP_nonQES_HBA gemProdT_X.509_TSP_nonQES_Komp

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	**Anpassungen** an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_6252	gemSpec_X.509_TSP	6.2.1.1 Schnittstellendefinition TIP1-A_3603	Jedem Hersteller von dezentralen Komponenten wird die Möglichkeit gewährt bereits vor Erteilung der produktiven Zulassung auf eigenes Risiko mit der Produktion aller für einen Vertrieb notwendigen Komponenten zu beginnen.	TIP1-A_3603 folgendermaßen ergänzt Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS bei der Registrierung von Antragsberechtigten für Komponenten- und Signerzertifikaten prüfen, ob a) der Antragsteller berechtigt ist, Komponenten- oder Signerzertifikate zu beziehen und b) eine Freigabe der gematik zum Abruf produktiver Zertifikate für diesen Antragsteller vorliegt. Hinweis: Die Möglichkeit zum Abruf produktiver Zertifikate kann auch vor formaler Erteilung der Zulassung des Produkts durch die gematik erfolgen. Der Bedarf hierzu ist durch den Hersteller unter Nennung von Gründen anzuzeigen und wird unter folgenden Rahmenbedingungen erteilt: - erfolgreiche Prüfung der Sicherheitseignung gemäß [gemRL_PruefSichEig] durch den Personalisierer der Gerätekarte abgeschlossen, - der Bestätigung des sicheren Transports zum Kartenherausgeber, - eine ausreichende funktionale Qualität des Produktes wurde durch die gematik geprüft und - ggf. Bestätigung der erfolgreichen fachlichen und technischen Prüfung seitens BSI.	gemSpec_X.509_TSP gemProdT_X.509_TSP_nonQES_Komp
C_6282	gemSpec_Kon	TIP1-A_4512 TIP1-A_4545 TIP1-A_4833	Die Schreibweise des Parameterbezeichners "Value" soll vereinheitlicht und gegebenen Implementierungen angepasst werden. In diesem Zug soll auch die Schreibweise des Parameterbezeichners "CtID" vereinheitlicht werden.	Siehe C_6282_Anlage.docx	gemSpec_Kon
C_6306	gemSpec_PKI	Anhang C4 - Apothekerschaft	Festlegung URL für CP in HBA-Profilen der Apotheker Im Rahmen des OPB 1.6.4 -Releases wurden für HBAs der Apotheker entsprechende X.509-Zertifikatsprofile abgestimmt und in in die PKI-Spezifikation aufgenommen. Im Rahmen der Festlegungen wurde im Feld CertificatePolicies ein Platzhalter für die URL aufgeführt, unter der eine CP für Apotheker aufgerufen werden kann. Der Platzhalter war zur Aufnahme dieses optionalen Feldes ausreichend, wurde mittlerweile von der Apothekerschaft bereitgestellt und kann so in die Spezifikation aufgenommen werden, damit TSPs dieses so umsetzen können.	In der CertificatePolicies Extension wird in dem sektorspezifischen HBA-Zertifikatsprofil der Apothekerschaft (Anhang C4 / Tabelle 121) das dort ersterwähnte Element policyQualifierInfo wie folgt angepasst: ALT: policyQualifierInfo = <URL der Apotheker, unter der die o.a. CP aufzurufen ist> NEU: policyQualifierInfo = https://www.abda.de/themen/positionen-und-initiativen/telematik/hba/	gemSpec_PKI gemProdT_X.509_TSP_nonQES_HBA gemProdT_X.509_TSP_ QES_HBA
C_6320	gemSpec_Net	2.3.3 Adresskonzept Ipv	Anpassung IPv4-Adresskonzept für die Produktiv- und Testumgebung Mit der Änderung wird das IPv4-Adresskonzept für die Produktiv- und Testumgebung optimiert. Dadurch ist es möglich mehr IP-Adressen für den dezentralen Zugang zur TI bereitzustellen. Dem dezentralen SIS-Zugang wird ein fester IP-Adressblock zugeteilt, der für jeden VPN-Zugangsdienstanbieter identisch ist.	Siehe C_6320_Anlage.docx	gemSpec_Net
C_6189	gemSpec_PKI	Kap. 5.6.2 GS-A_4609 GS-A_4610 GS-A_4611 Kap. 5.5.1 GS-A_4604 GS-A_4617 GS-A_4618 GS-A_4615 GS-A_5280 GS-A_4613 GS-A_4830	Keine Beschränkung auf DE-Länderkürzel in Komponenten-PKI Derzeit ist der Bezug von Konnektor-Zertifikaten auf Konnektor-Hersteller aus Deutschland begrenzt. Diese unnötige Einschränkung wird aufgehoben. Dieselbe Einschränkung gilt für Kartenterminal- und Dienstezertifikate der Komponenten-PKI. Auch für diese ist die Einschränkung unnötig und wird aufgehoben.	In Kapitel 5.6.2: ALT: • countryName = [Herkunftsland des Konnektor-Herstellers, DE] NEU: • countryName = [Herkunftsland des Konnektor-Herstellers~~, DE~~] In den Konnektor-Zertifikatsprofilen für C.NK.VPN, C.AK.AUT und C.SAK.AUT wird in den Zertifikatsprofiltabellen Tab_PKI_242, Tab_PKI_243 und Tab_PKI_244 jeweils der Eintrag für das Subject-Feld CountryName geändert: ALT: DE NEU: ~~DE~~ Herkunftsland des Konnektor-Herstellers In Kapitel 5.5.1: ALT: • countryName = [Herkunftsland des Kartenterminal-Herstellers, DE] NEU: • countryName = [Herkunftsland des Kartenterminal-Herstellers~~, DE~~] In Tab_PKI_241 C.SMKT.AUT gSMC-KT wird der Eintrag für das Subject-Feld CountryName geändert: ALT: DE NEU: ~~DE~~ Herkunftsland des Kartenterminal-Herstellers. In den Zertifikatsprofilen für C.FD.TLS-C, C.FD.TLS-S, C.ZD.TLS-S, und C.CM.TLS-CS wird in den Zertifikatsprofiltabellen Tab_PKI_249, Tab_PKI_250, Tab_PKI_247, und Tab_PKI_267 jeweils der Eintrag für das Subject-Feld CountryName geändert: ALT: DE NEU: ~~DE~~ Land der Anschrift des verantwortlichen Anbieters In den Zertifikatsprofilen für C.VPNK.VPN und C.VPNL.VPN-SIS.AUT wird in den Zertifikatsprofiltabellen Tab_PKI_245 und Tab_PKI_265 jeweils der Eintrag für das Subject-Feld CountryName geändert: ALT: DE NEU: ~~DE~~ Land der Anschrift des Zugangsdienstanbieters	gemSpec_PKI

Änderungsbedarf:

Vor der Kommunikation mit dem Konnektor holt sich ein Clientsystem über den Dienstverzeichnisdienst die SOAP-Endpunkte, über die das Clientsystem die einzelnen Dienstoperationen erreichen kann. Diese Schnittstellen werden vom Konnektor mit einer Version versehen und das Clientsystem kann anhand der Versionsnummer entscheiden, ob es mit der Dienstversion kompatibel ist.

Daher würde ein Clientsystem, das z.B. die Version 8.1.0 eines Dienstes unterstützt, die Kommunikation mit einem Konnektor ablehnen, der die Version 8.1.1 desselben Dienstes anbietet, obwohl die Version 8.1.1 per Definition abwärtskompatibel zur Version 8.1.0 ist.

Um diesem Problem zu begegnen wird in diesem Hotfix verlangt, in der Datei `connector.sds` für den CardService zwei Versionen aufzuführen.

Änderungen in gemSpec_Kon

4.1.3.1 Operationen an der Außenschnittstelle

⌦ **TIP1-A_4586 Basisanwendung Kartendienst**

Der Konnektor MUSS für Clients eine Basisanwendung Kartendienst mit den Operationen VerifyPin, ChangePin, UnblockPin, GetPinStatus an der Außenschnittstelle anbieten.

Tabelle 1: TAB_KON_038 Basisanwendung Karten- und Kartenterminaldienst

Name	`CardService`	
Version (KDV)	8.1.0 (WSDL- und XSD-Version) 8.1.1 (WSDL- und XSD-Version) Siehe Anhang D	
Namensraum	Siehe Anhang D	
Namensraum-Kürzel	`CARD` für Schema und `CARDW` für WSDL	
Operationen	**Name**	**Kurzbeschreibung**
	`VerifyPin`	PIN prüfen
	`ChangePin`	PIN ändern
	`UnblockPin`	PIN entsperren
	`GetPinStatus`	PIN-Status ermitteln
WSDL	`CardService.wsdl`	
Schema	`CardService.xsd`	

⌫

Anhang D - Übersicht über die verwendeten Versionen

Für den Fall, dass Schnittstellenversionen unterstützt werden müssen, die den gleichen TargetNamespace nutzen, kann der Konnektor zu diesen Schnittstellenversionen einheitlich einen SOAP-Endpunkt anbieten, der die höchste der Schnittstellenversionen implementiert.

Tabelle 2: TAB_KON_688 Version der Schemas aus dem Namensraum des Konnektors

Schemas aus dem Namensraum des Konnektors „http://ws.gematik.de/conn“		
	XSD Name	CardEvents.xsd
	XSD Schemaversion	6.0.0
	TargetNamespace	http://ws.gematik.de/conn/CardEvents/v6.0
	XSD Name	CardService.xsd
	XSD Schemaversion	8.1.1
	TargetNamespace	http://ws.gematik.de/conn/CardService/v8.1
	XSD Name	CardService.xsd
	XSD Schemaversion	8.1.0
	TargetNamespace	http://ws.gematik.de/conn/CardService/v8.1

(…)

Tabelle 328: TAB_KON_798 Schnittstellenversionen

Pro Dienst mit Operationen an der Außenschnittstelle: WSDLs des Konnektors und verwendete XSDs aus dem Namensraum der gematik http://ws.gematik.de		
Kartendienst (CardService)		
	WSDL Name	CardService.wsdl
	WSDL-Version	8.1.1
	TargetNamespace	http://ws.gematik.de/conn/CardService/WSDL/v8.1
	verwendete XSDs	CardService.xsd, CardServiceCommon.xsd, ConnectorCommon.xsd, ConnectorContext.xsd, ProductInformation.xsd, TelematikError.xsd
Kartendienst (CardService)		
	WSDL Name	CardService.wsdl
	WSDL-Version	8.1.0
	TargetNamespace	http://ws.gematik.de/conn/CardService/WSDL/v8.1
	verwendete XSDs	CardService.xsd, CardServiceCommon.xsd, ConnectorCommon.xsd, ConnectorContext.xsd, ProductInformation.xsd, TelematikError.xsd

(…)

Änderungsbedarf:

Mit der geplanten Einführung von G2.1-Karten wurde bei allen Zertifikatsprofilen der gematik die Unterstützung des Schlüsselalgorithmus ECDSA vorbereitet.

Im Rahmen der ersten Umsetzungsaktivitäten für EE-Zertifikate auf ECDSA-Basis wurde festgestellt, dass bezüglich der KeyUsage Anpassungen für die ECDSA-Ausprägungen der Zertifikatsprofile notwendig sind, um RFC-Konformität zu RFC 5480 gewährleisten.

Dabei wird ”KeyEncipherment” als KeyUsage nicht mehr für den Schlüsselalgorithmus ECDSA genutzt und dazu in den Zertifikatsprofilen fallweise in der ECDSA-Ausprägung entfernt oder durch ”KeyAgreement” ersetzt.

Die existierenden Zertifikatsprofile auf RSA-Basis (G2-Karten) werden nicht angepasst. Die Änderungen wirken sich nur auf die Zulassung von TSPs aus, die Zertifikate für G2.1-Karten ausgeben wollen.

Die Änderungen betreffen Zertifikatsprofile für ECDSA-EE-Zertifikate, die von den folgenden TSP-Produkttypen umgesetzt werden:

- TSP-X.509 nonQES (eGK)
- TSP-X.509 nonQES (HBA)
- TSP-X.509 nonQES (SMC-B)
- TSP-X.509 nonQES (Komp)

Die Spezifkation wird dahingehend wie folgt angepasst.

Änderungen in gemSpec_PKI

[…]

5.1.3.1 C.CH.AUT – Authentisierung eGK

⌦ GS-A_4595 Umsetzung Zertifikatsprofil C.CH.AUT

Der TSP-X.509 nonQES (eGK) MUSS C.CH.AUT gemäß Tab_PKI_232 umsetzen.⌫

Tabelle 22: Tab_PKI_232 C.CH.AUT Authentisierung eGK

Element				Inhalt	Kar.	
certificate				C.CH.AUT		
	tbsCertificate					
		…		2 (v3)		
		extensions				critical
			…			
			KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment	1 0-1	**TRUE**

Element				Inhalt	Kar.	
				Für Schlüsselgeneration ECDSA: digitalSignature	 1	
			…			
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature			Wert der Signatur		

5.1.3.2 C.CH.ENC – Verschlüsselung eGK

⌦ GS-A_4596 Umsetzung Zertifikatsprofil C.CH.ENC

Der TSP-X.509 nonQES (eGK) MUSS C.CH.ENC gemäß Tab_PKI_233 umsetzen.⌫

Tabelle 23: Tab_PKI_233 C.CH.ENC Verschlüsselung eGK

Element				Inhalt	Kar.	
certificate				C.CH.ENC		
	tbsCertificate					
		…		2 (v3)		
		extensions				critical
			…			
			KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* keyEncipherment dataEncipherment *Für Schlüsselgeneration ECDSA:* keyAgreement	 1 1 1	**TRUE**
			…			
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt# GS-A_4362]		
	signature			Wert der Signatur		

[…]

5.1.3.4 C.CH.AUTN - Technische Authentisierung eGK

⌦ GS-A_4598 Umsetzung Zertifikatsprofil C.CH.AUTN

Der TSP-X.509 nonQES (eGK) MUSS C.CH.AUTN gemäß Tab_PKI_235 umsetzen.⌫

Tabelle 25 Tab_PKI_235 C.CH.AUTN Technische Authentisierung eGK

Element			Inhalt	Kar.	
certificate			C.CH.AUTN		
	tbsCertificate				
		…	2 (v3)		
		extensions			critical

Element	Inhalt	Kar.	
…			
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 0-1 1	**TRUE**
…			
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature	Wert der Signatur		

5.1.3.5 C.CH.ENCV - Technische Verschlüsselung eGK

⌦ GS-A_4599 Umsetzung Zertifikatsprofil C.CH.ENCV

Der TSP-X.509 nonQES (eGK) MUSS C.CH.ENCV gemäß Tab_PKI_236 umsetzen.⌫

Tabelle 26: Tab_PKI_236 C.CH.ENCV Technische Verschlüsselung eGK

Element	Inhalt	Kar.	
certificate	C.CH.ENCV		
tbsCertificate			
…	2 (v3)		
extensions			critical
…			
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* keyEncipherment dataEncipherment *Für Schlüsselgeneration ECDSA:* keyAgreement	 1 1 1	**TRUE**
…			
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		
signature	Wert der Signatur		

[…]

5.2.1.1 C.HP.AUT – Authentisierung HBA

⌦ GS-A_5531 Umsetzung Zertifikatsprofil C.HP.AUT

Der TSP-X.509 nonQES MUSS C.HP.AUT gemäß Tab_PKI_268 umsetzen.⌫

Tabelle 27: Tab_PKI_268 C.HP.AUT Authentisierung HBA

Element	Inhalt	Kar.	
certificate	C.HP.AUT		

Element	Inhalt	Kar.	
tbsCertificate			
…	2 (v3)		
extensions			critical
…			
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature keyAgreement	 1 1 1 1	**TRUE**
…			
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
signature	Wert der Signatur		

**) Sektorspezifische Ausprägungen der HBA-Zertifikate sind dem Anhang C zu entnehmen.*

***) Kodierung in einem SET als einziges Multivalued Relative Distinguished Name Element (multivaluedRDN) (siehe Hinweis unten unter Zusatzinformationen)*

5.2.1.2 C.HP.ENC – Verschlüsselung HBA

⌦ GS-A_5532 Umsetzung Zertifikatsprofil C.HP.ENC

Der TSP-X.509 nonQES MUSS C.HP.ENC gemäß Tab_PKI_269 umsetzen.⌫

Tabelle 28: Tab_PKI_269 C.HP.ENC Verschlüsselung HBA

Element	Inhalt	Kar.	
certificate	C.HP.ENC		
tbsCertificate			
…	2 (v3)		
extensions			critical
…			
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* keyEncipherment dataEncipherment *Für Schlüsselgeneration ECDSA:* keyAgreement	 1 1 1	**TRUE**
…			
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt# GS-A_4357]		
signature	Wert der Signatur		

**) Sektorspezifische Ausprägungen der HBA-Zertifikate sind dem Anhang C zu entnehmen.*

***) Kodierung in einem SET als einziges Multivalued Relative Distinguished Name Element (multivaluedRDN) (siehe Hinweis unten unter Zusatzinformationen)*

[…]

5.3.4.1 C.HCI.AUT – Authentisierung SMC- B

⌦ GS-A_4600 Umsetzung Zertifikatsprofil C.HCI.AUT

Der TSP-X.509 nonQES MUSS C.HCI.AUT gemäßTab_PKI_238 umsetzen.⌫

Tabelle 30: Tab_PKI_238 C.HCI.AUT Authentisierung SMC-B

Element	Inhalt	Kar.	
certificate	C.HCI.AUT		
tbsCertificate			
…	2 (v3)		
extensions			critical
…			
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
…			
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature	Wert der Signatur		

**) Sektorspezifische Ausprägungen der SMC-B Zertifikate sind dem Anhang A zu entnehmen*

5.3.4.2 C.HCI.ENC – Verschlüsselung SMC-B

⌦ GS-A_4601 Umsetzung Zertifikatsprofil C.HCI.ENC

Der TSP-X.509 nonQES MUSS C.HCI.ENC gemäß Tab Tab_PKI_239 umsetzen.⌫

Tabelle 31: Tab_PKI_239 C.HCI.ENC Verschlüsselung SMC-B

Element	Inhalt	Kar.	
certificate	C.HCI.ENC		
tbsCertificate			
…	2 (v3)		
extensions			critical
…			
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* keyEncipherment dataEncipherment *Für Schlüsselgeneration ECDSA:* keyAgreement	 1 1 1	**TRUE**
…			
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		
signature	Wert der Signatur		

**) Sektorspezifische Ausprägungen der SMC-B Zertifikate sind dem Anhang A zu entnehmen*

[…]

5.5.2.1 C.SMKT.AUT – Identität der gSMC-KT

⌦ GS-A_4604 Umsetzung Zertifikatsprofil C.SMKT.AUT

Der TSP-X.509 nonQES MUSS C.SMKT.AUT gemäß Tab_PKI_241 umsetzen.⌫

Tabelle 33: Tab_PKI_241 C.SMKT.AUT gSMC-KT

Element	Inhalt	Kar.	
certificate	C.SMKT.AUT		
tbsCertificate			
…	2 (v3)		
extensions			critical
…			
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
…			
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature	Wert der Signatur		

[…]

5.6.4.1 C.NK.VPN – VPN-Authentisierung Netzkonnektor

[…]

⌦ GS-A_4609 Umsetzung Zertifikatsprofil C.NK.VPN

Der TSP-X.509 nonQES MUSS C.NK.VPN gemäß Tab_PKI_242 umsetzen.⌫

Tabelle 35: Tab_PKI_242 Zertifikatsprofil C.NK.VPN VPN-Authentisierung Netzkonnektor

Element	Inhalt	Kar.	
certificate	C.NK.VPN		
tbsCertificate			
…	2 (v3)		
extensions			critical
…			
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
…			

Element		Inhalt	Kar.	
	signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]		
	signature	Wert der Signatur		

5.6.4.2 C.AK.AUT - Authentisierung Anwendungskonnektor

[…]

⌦ GS-A_4610 Umsetzung Zertifikatsprofil C.AK.AUT

Der TSP-X.509 nonQES MUSS C.AK.AUT gemäß Tab_PKI_243 umsetzen.⌫

Tabelle 36: Tab_PKI_243 Zertifikatsprofil C.AK.AUT Authentisierung Anwendungskonnektor

Element			Inhalt	Kar.	
certificate			C.AK.AUT		
	tbsCertificate				
		…	2 (v3)		
		extensions			critical
		…			
		KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
		…			
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature		Wert der Signatur		

5.6.4.3 C.SAK.AUT - Authentisierung SAK

[…]

⌦ GS-A_4611 Umsetzung Zertifikatsprofil C.SAK.AUT

Der TSP-X.509 nonQES MUSS C.SAK.AUT gemäß Tab_PKI_244 umsetzen.⌫

Tabelle 37: Tab_PKI_244 Zertifikatsprofil C.SAK.AUT Authentisierung SAK

Element			Inhalt	Kar.	
certificate			C.SAK.AUT		
	tbsCertificate				
		…	2 (v3)		
		extensions			critical
		…			
		KeyUsage	*Für Schlüsselgeneration RSA:*		**TRUE**

Element				Inhalt	Kar.	
			{2 5 29 15}	digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	1 1 1	
			…			
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature			Wert der Signatur		

[…]

5.7.3.1 C.VPNK.VPN - VPN-Authentisierung Zugangsdienst TI

⌦ GS-A_4613 Umsetzung Zertifikatsprofil C.VPNK.VPN

Der TSP-X.509 nonQES MUSS C.VPNK.VPN gemäß Tab_PKI_245 umsetzen.⌫

Tabelle 38: Tab_PKI_245 Zertifikatsprofil C.VPNK.VPN VPN-Authentisierung Zugangsdienst TI

Element				Inhalt	Kar.	
certificate				C.VPNK.VPN		
	tbsCertificate					
		…		2 (v3)		
		extensions				critical
			…			
			KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
			…			
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]		
	signature			Wert der Signatur		

5.7.3.2 C.VPNK.VPN-SIS - VPN-Authentisierung Zugangsdienst Sicherer Internetzugang

⌦ GS-A_4830 Umsetzung Zertifikatsprofil C.VPNK.VPN-SIS

Der TSP-X.509 nonQES MUSS C.VPNK.VPN-SIS gemäß Tab_PKI_265 umsetzen.⌫

Tabelle 39: Tab_PKI_265 Zertifikatsprofil C.VPNK.VPN-SIS VPN-Authentisierung Zugangsdienst Sicherer Internetzugang

Element	Inhalt	Kar.	

Element			Inhalt	Kar.	
certificate			C.VPNK.VPN-SIS		
	tbsCertificate				
		…	2 (v3)		
		extensions			critical
		…			
		KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
		…			
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]		
	signature		Wert der Signatur		

[…]

5.8.3.1 C.ZD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S)

⌦ GS-A_4615 Umsetzung Zertifikatsprofil C.ZD.TLS-S

Der TSP-X.509 nonQES MUSS C.ZD.TLS-S gemäß Tab_PKI_247 umsetzen.⌫

Tabelle 40: Tab_PKI_247 C.ZD.TLS-S Server-Authentisierung Zentrale Dienste

Element			Inhalt	Kar.	
certificate			C.ZD.TLS-S		
	tbsCertificate				
		…	2 (v3)		
		extensions			critical
		…			
		KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
		…			
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature		Wert der Signatur		

[…]

5.9.3.1 C.FD.TLS-C Client-Authentisierung (ehemals C.SF.SSL-C)

⌦ GS-A_4617 Umsetzung Zertifikatsprofil C.FD.TLS-C

Der TSP-X.509 nonQES MUSS C.FD.TLS-C gemäß Tab_PKI_249 umsetzen.⌫

Tabelle 41: Tab_PKI_249 C.FD.TLS-C Client-Authentisierung Fachanwendungsspezifische Dienste

Element	Inhalt	Kar.	
certificate	C.FD.TLS-C		
tbsCertificate			
…	2 (v3)		
extensions			critical
…			
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
…			
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature	Wert der Signatur		

5.9.3.2 C.FD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S)

⌦ **GS-A_4618 Umsetzung Zertifikatsprofil C.FD.TLS-S**

Der TSP-X.509 nonQES MUSS C.FD.TLS-S gemäß Tab_PKI_250 umsetzen.⌫

Tabelle 42: Tab_PKI_250 C.FD.TLS-S Server-Authentisierung Fachanwendungsspezifische Dienste

Element	Inhalt	Kar.	
certificate	C.FD.TLS-S		
tbsCertificate			
…	2 (v3)		
extensions			critical
…			
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
…			
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature	Wert der Signatur		

[…]

5.10.3.1 C.CM.TLS-CS Clientmodul-Authentisierung

⌦ GS-A_5280 Umsetzung Zertifikatsprofil C.CM.TLS-CS

Der TSP-X.509 nonQES MUSS C.CM.TLS-CS gemäß Tab_PKI_267 umsetzen.⌫

Tabelle 43: Tab_PKI_267 C.CM.TLS-CS Clientmodul-Authentisierung

Element	Inhalt	Kar.	
certificate	C.CM.TLS-CS		
tbsCertificate			
…	2 (v3)		
extensions			critical
…			
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
…			
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature	Wert der Signatur		

[…]

Änderungsbedarf:

Die Schreibweise des Parameterbezeichners ”Value” soll vereinheitlicht werden.

Die Schreibweise des Parameterbezeichners ”CtID” soll vereinheitlicht werden.

Änderungen in gemSpec_Kon

3.3 Betriebszustand
(...)

⌦ **TIP1-A_4512 Ereignis bei Änderung des Betriebszustandes**

Der Konnektor MUSS per Ereignisdienst TUC_KON_256 über Änderungen des Betriebszustandes (Tabelle TAB_KON_503 Betriebszustand_Fehlerzustandsliste) informieren.

Der Konnektor muss dazu für jeden Fehlerzustand $EC mit Error Condition $EC.errorcondition mit verändertem Wert $EC.value den technischen Anwendungsfall TUC_KON_256 „Systemereignis absetzen“ mit folgenden Parametern aufrufen:

TUC_KON_256{ "OPERATIONAL_STATE/$EC.errorcondition ";
$EC.type;
$EC.severity;
{~~¥~~Value=$EC.value; $EC.parameterlist}
} ⌫

Tabelle 3 TAB_KON_503 Betriebszustand_Fehlerzustandsliste

ErrorCondition[1]	Beschreibung	Type	Severity	max. Feststellungs-zeit	Parameterlist[2]
EC_CardTerminal_Software_Out_Of_Date ($ctId)	Software auf Kartenterminal($ctId) ist nicht aktuell	Op	Info	1 day	CtIDd=$ctId; Bedeutung=$EC.description
(...)					
EC_CardTerminal_Not_Available ($ctId)	Kartenterminal($ctId) ist nicht verfügbar. Dieser Betriebszustand bezieht sich auf die als „aktiv“ gekennzeichneten KTs.	Op	Error	1 sec	CtIDd=$ctId; Bedeutung=$EC.description

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

[2] EC.description referenziert den Text, der in der Spalte „Beschreibung“ des Zustandes spezifiziert wurde.

Anhang F - Übersicht Events

Tabelle 330 – TAB_KON_777 Events Interne Mechanismen

Topic Ebene1	Topic Ebene2	Topic Ebene3	Typ	Schwere	Prot	An Clients	Parameter	Bedeutung	Auslöser (TUC/Op)
Interne Mechanismen									
BOOTUP	BOOTUP_COMPLETE		Op	Info	x	x		Änderung des Betriebszustandes	
OPERATIONAL_STATE	EC_CardTerminal_Software_Out_Of_Date($ctId)		Op	Info	x	x	Value=true/false; CtIDd=$ctId; Bedeutung=$EC.description	Änderung des Betriebszustandes durch Änderung im Fehlerzustand (Änderung im vValue).	
(…)									
OPERATIONAL_STATE	EC_CardTerminal_Not_Available($CtId)		Op	Error	x	x	Value=true/false; CtIDd=$ctId; Bedeutung=$EC.description	"	
(…)									
Kartenterminaldienst									
CT	ERROR		$ErrorType	$Severity	x	x	CtTID=$CT.ID; Name=$CT.HOSTNAME; Error=$Fehlercode; Bedeutung=$Fehlertext	Bei der Kommunikation mit dem KT ist ein Fehler aufgetreten	TUC_KON_051 TUC_KON_053
(…)									
CT	TLS_ESTABLISHMENT_FAILURE		$ErrorType	$Severity	x	x	CtTID=$CT.ID; Name=$CT.HOSTNAME; Error=$Fehlercode; Bedeutung=$Fehlertext	Im Rahmen des Verbindungsaufbaus sind Fehler aufgetreten	TUC_KON_050
Software-Aktualisierungsdienst (KSR-Client)									
(…)									
KSR	ERROR		$ErrorType	$Severity	x	x	Target=KT; Name=<KT-FriendlyName>; CtTID=$ctID;	Während einer Kartenterminalaktualisierung ist ein Fehler aufgetreten	TUC_KON_281

							Error=$Fehlercode; Bedeutung=$Fehlertext		
(...)									
KSR	UPDATE	START	Sec	Info	x	x	für TUC_KON_280 Target=Konnektor; Name=<MGM_KONN_HOSTNAME> für TUC_KON_281 Target=KT; CtID=$CtID	Ein Updateprozess im Konnektor wird gestartet, Ziel Konnektor oder Kartenterminal	TUC_KON_280 TUC_KON_281
KSR	UPDATE	SUCCESS	Sec	Info	x	x	für TUC_KON_280 Target=Konnektor; Name=<MGM_KONN_HOSTNAME>; NewFirmwareversion=<UpdateInformation.FirmwareVersion>; ConfigurationChanged=<Ja/Nein>; ManualInputNeeded=<Ja/Nein> für TUC_KON_281 Target=KT; Name=<KT-FriendlyName>; CtID=$ctID; NewFirmwareversion=<UpdateInformation.FirmwareVersion>	Die Firmware des Konnektors / eines Kartenterminals wurde erfolgreich aktualisiert	TUC_KON_280 TUC_KON_281
KSR	UPDATE	END	Sec	Info	x	x	für TUC_KON_280 Target=Konnektor; Name=<MGM_KONN_HOSTNAME> für TUC_KON_281 Target=KT; CtID=$CtID	Ein Updateprozess im Konnektor wurde beendet	TUC_KON_280 TUC_KON_281

4.1.4.3.1 TUC_KON_050 „Beginne Kartenterminalsitzung“

⌧ TIP1-A_4545 TUC_KON_050 „BeginneKartenterminalsitzung“

Der Konnektor MUSS den technischen Use Case “Beginne Kartenterminalsitzung” gemäß TUC_KON_050 umsetzen.

Tabelle 29: TAB_KON_039 - TUC_KON_050 „Beginne Kartenterminalsitzung“

Element	Beschreibung
(…)	
Fehlerfälle	Fehler in den folgenden Schritten des Ablaufs führen zu: Aufruf von TUC_KON_256 mit folgenden Parametern {"CT/TLS_ESTABLISHMENT_FAILURE"; $ErrorType; $Severity; „CtID=$CT.ID; Name=$CT.HOSTNAME; Error=$Fehlercode; Bedeutung=$Fehlertext“} Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes (→1): Admin-Rolle für logische KTs nicht möglich (hätte bei korrekter Implementierung nicht stattfinden dürfen), Fehlercode: 4032 (→1): Verbindungsaufbau zu HSM fehlgeschlagen, Fehlercode: 4032 (→3): Fehler im TLS-Verbindungsaufbau bzw. Zertifikatsprüfung, Fehlercode: 4028 und setze CT.CONNECTED auf „Nein“ (→3): TLS-Verbindung konnte nicht innerhalb von CTM_TLS_HS_TIMEOUT Sekunden aufgebaut werden , Fehlercode: 4028 und setze CT.CONNECTED auf „Nein“ (→5): Präsentiertes Zertifikat nicht das aus dem Pairing, Fehlercode: 4029 und setze CT.CORRELATION auf „gepairt“ und setze CT.CONNECTED auf „Nein“ und terminiere TLS-Verbindung (→6b): Hinterlegte KT-Admin-Credentials fehlerhaft, Fehlercode: 4030 und in die User-Session zurückzuwechseln (damit das KT für den normalen Fachbetrieb weiterhin zur Verfügung steht) (→8): Prüfung auf Nachweis SharedSecret fehlgeschlagen, Fehlercode 4029 und setze CT.CORRELATION auf „gepairt“ und setze CT.CONNECTED auf „Nein“ und terminiere TLS-Verbindung

4.3.9.3.2 TUC_KON_281 „Kartenterminalaktualisierung anstoßen“

Im Vergleich zur Durchführung des Konnektor-Update (TUC_KON_280), werden die Updates der Kartenterminals nur durch den Konnektor initiiert. Der Konnektor liefert dem Kartenterminal das Updatefile, der eigentliche Updatevorgang (inklusive der Prüfung des Updatepakets auf Integrität und Authentizität) erfolgt ausschließlich und eigenverantwortlich auf Seiten des Kartenterminals.

⌧ TIP1-A_4833 TUC_KON_281 „Kartenterminalaktualisierung anstoßen“

Der Konnektor MUSS den technischen Use Case TUC_KON_281 „Kartenterminal-aktualisierung anstoßen“ umsetzen.

Tabelle 314: TAB_KON_666 - TUC_KON_281 „Kartenterminalaktualisierung anstoßen“

Element	Beschreibung
Name	TUC_KON_281 „Kartenterminalaktualisierung anstoßen“
Beschreibung	Dieser TUC fordert ein Kartenterminal auf einen Update durchzuführen, dessen Update-Dateien entweder direkt übergeben oder per UpdateInformation (vom KSRS bezogen) referenziert werden
Auslöser	Der Administrator hat UpdateInformation für ein Kartenterminal zur Anwendung ausgewählt und bestätigt bzw. ein lokales Updatepaket für ein Kartenterminal bezogen und zur Anwendung übergeben.
Vorbedingungen	• Der Administrator hat bewusst das übergebene Paket für eine Installation ausgewählt • CT(ctID).IS_PHYSICAL=Ja • CT(ctID).CORRELATION>=”gepairt”
Eingangsdaten	• ctID (ID des Ziel-KTs) • UpdateInformation (gemäß [gemSpec_KSR]) oder • Updatepaket (herstellerspezifisch, von lokaler Datenquelle, mit enthaltenen FirmwareFiles)
Komponenten	Konnektor, Kartenterminal
Ausgangsdaten	Keine
Nachbedingungen	Das Kartenterminal arbeitet basierend auf der übergebenen, im Updatepaket enthaltenen neuen Version.
Standardablauf	Der Konnektor MUSS die zur Anwendung übergebene UpdateInformation wie folgt anwenden: 1. Download der in UpdateInformation/FirmwareFiles gelisteten Datei (für KT-Updates darf nur genau ein FirmwareFile angegeben werden) 2. TUC_KON_256{"KSR/UPDATE/START"; Sec; Info; „Target=KT; CtID=$ctID“} 3. Durchführen des KT-Updates durch: a) Wechsel in eine Admin-Session durch TUC_KON_050 „Beginne Kartenterminalsitzung“{Admin; ctID} b) Senden der SICCT Kommandos: SICCT CT Download INIT, SICCT CT Download DATA (Übermittlung des UpdateFiles) und SICCT CT Download FINISH an ctID c) TUC_KON_256{"KSR/UPDATE/SUCCESS"; Sec; Info; „Target=KT; Name= $CT.HOSTNAME;CtID=$ctID; NewFirmwareversion=<UpdateInformation.FirmwareVersion>“} Der TUC endet in jedem Fall mit: • TUC_KON_256{"KSR/UPDATE/END"; Sec; Info; „Target=KT;CtID=$ctID“}
Varianten/Alternativen	Sofern direkt ein Updatepaket (mit enthaltenem FirmwareFile)

Element	Beschreibung
	übergeben wurde beginnt der Ablauf ab Nummer 2 mit Signalisierung des Beginns des KT-Updates
Fehlerfälle	Fehler in den folgenden Schritten des Ablaufs führen zu: a) Aufruf von TUC_KON_256 mit folgenden Parametern {"KSR/ERROR"; $ErrorType; $Severity; „Target=KT; Name=$CT.HOSTNAME;CtID=$ctID; Error=$Fehlercode; Bedeutung=$Fehlertext“} b) Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes (→1) Download fehlgeschlagen, Fehlercode: 4186 (→3b) SICCT-Download fehlgeschlagen, Fehlercode: 4187

Änderungsbedarf in gemSpec_Net

In Abschnitt ”2.3.3 Adresskonzepz IPv4

⌦ GS-A_4029 IPv4-Adresskonzept Produktivumgebung

Der Anbieter Zentrales Netz TI MUSS den Adressbereich 100.64.0.0/10 nach dem in der Tab_Adrkonzept_Produktiv definierten Schema zur Vergabe von IPv4-Adressen an Produkttypen der TI in der Produktivumgebung verwenden.

Tabelle 1: Tab_Adrkonzept_Produktiv, Adressräume IPv4 TI Produktivumgebung

Netzbereich	Adressen	Netz	Nutzung	Verantwortlich
TI-Produktivumgebung	4M	100.64.0.0/10	TI Produktiv	Anbieter Zentrales Netz TI und GBV
TI_Dezentral (TI_Dezentral_SIS) (siehe Erläuterung)	1M	100.64.0.0/11	Dezentral (Dezentral SIS)	Anbieter Zentrales Netz TI
Konnektoren	2M	100.64.0.0/11	Konnektoren TI (Konnektoren SIS)	Anbieter Zugangsdienst
~~TI_Dezentral~~	~~1M~~	~~100.80.0.0/12~~	~~Dezentral~~	~~Anbieter Zentrales Netz TI~~
~~Konnektoren~~	~~1M~~	~~100.80.0.0/12~~	~~Konnektoren TI~~	~~Anbieter Zugangsdienst~~
TI_Zentral	256K	100.96.0.0/14	Zentrale Dienste	Anbieter Zentrales Netz TI
Zentrale Dienste	64K	100.96.0.0/16	Zentrale Dienste	Anbieter Zentraler Dienste
	Der Anbieter Zentrales Netz TI weist jedem zentralen Dienst ein /26 Adressblock aus dem Bereich 100.96.0.0/16 zu.			
VPN-Zugangsdienst	64K	100.97.0.0/16	Anschluss VPN-Konzentratoren an die TI	Anbieter Zugangsdienst
	Der Anbieter Zentrales Netz TI weist jedem VPN-Zugangsdienstprovider ein /26 Adressblock aus dem Bereich 100.97.0.0/16 zu.			
Reserveblöcke	128K	100.98.0.0/15	Reserve	Anbieter Zentrales Netz TI
TI_Fachdienste	256K	100.100.0.0/14	Fachdienste	Anbieter Zentrales Netz TI

Netzbereich	Adressen	Netz	Nutzung	Verantwortlich
Offene Fachdienste	64K	100.102.0.0/16	Offene Fachdienste	Anbieter Offene Fachdienste
	Der Anbieter Zentrales Netz TI weist jedem Offenen Fachdienst ein /26 Adressblock aus dem Bereich 100.102.0.0/16 zu			
Gesicherte Fachdienste	64K	100.100.0.0/16	Gesicherte Fachdienste	Anbieter Gesicherte Fachdienste
	Der Anbieter Zentrales Netz TI weist jedem Gesicherten Fachdienst ein /26 Adressblock aus dem Bereich 100.100.0.0/16 zu			
Reserveblöcke	128K	100.101.0.0/16 100.103.0.0/16	Reserve	Anbieter Zentrales Netz TI
TI_Dezentral_SIS (siehe Erläuterung)	256k	100.104.0.0/14	Dezentral SIS	Anbieter Zentrales Netz TI
Konnektoren	128k	100.104.0.0/15	Konnektoren SIS	Anbieter Zugangsdienst
Reserveblock	128k	100.106.0.0/15	Reserve	Anbieter Zentrales Netz TI
TI_Betriebsreserve	1.5M	100.108.0.0/14 100.112.0.0/12	Reserve	Anbieter Zentrales Netz TI

⌫

Erläuterung:

Aus dem Netzbereich 100.64.0.0/11 sollen nur noch IP-Adressblöcke für den dezentralen Zugang zur TI (TI_Dezentral) zugeteilt werden. Die IP-Adressblöcke, die schon für den Zugang SIS eingeteilt wurden, bleiben bestehen und müssen nicht verändert werden.

Für den dezentralen SIS-Zugang muss dem Anbieter des VPN-Zugangsdienstes der IP-Adressblock 100.104.0.0/15 zugewiesen werden. Somit ist der IP-Adressblock TI_Dezentral_SIS ist für jeden VPN-Zugangsdienstanbieter identisch.

⌦ **GS-A_4850 IPv4-Adresskonzept Testumgebung**

Der Anbieter Zentrales Netz TI MUSS den Adressbereich 172.16.0.0/12 nach dem in Tab_Adrkonzept_Test definierten Schema zur Vergabe von IPv4-Adressen an Produkttypen der TI in der Testumgebung verwenden.

Tabelle 2: Tab_Adrkonzept_Test, Adressräume IPv4 TI-Testumgebung

Netzbereich	Adressen	Netz	Nutzung	Verantwortlich
TI-Testumgebung	1M	172.16.0.0/12	TI Test	Anbieter Zentrales Netz TI
TI_Test_Dezentral (TI_Test_Dezentral_SIS) (siehe Erläuterung)	512K	172.16.0.0/13	Dezentral TI (Dezentral SIS)	Anbieter Zentrales Netz TI
Konnektoren	512K	172.16.0.0/13	Konnektoren TI (SIS)	Anbieter Zugangsdienst
~~TI_Test_Dezentral~~	~~256K~~	~~172.20.0.0/14~~	~~Dezentral~~	~~Anbieter Zentrales Netz TI~~
~~Konnektoren~~	~~256K~~	~~172.20.0.0/14~~	~~Konnektoren TI~~	~~Anbieter Zugangsdienst~~
TI_Test_Zentral	256K	172.24.0/14	Zentrale Dienste	Anbieter Zentrales Netz TI
Zentrale Dienste	64K	172.24.0.0/16	Zentrale Dienste	Anbieter Zentraler Dienste
	Der Anbieter Zentrales Netz TI weist jedem zentralen Dienst ein /26 Adressblock aus dem Bereich 172.24.0.0/15 zu.			
VPN-Zugangsdienst	64K	172.25.0.0/16	Anschluss VPN-Konzentratoren an die TI	Anbieter Zugangsdienst
	Der Anbieter Zentrales Netz TI weist jedem VPN-Zugangsdienstprovider ein /26 Adressblock aus dem Bereich 172.25.0.0/16 zu.			
Reserveblöcke	128K	172.26.0.0/15	Reserve	Anbieter Zentrales Netz TI
TI_Test_Fachdienste	256K	172.28.0.0/14	Fachdienste	Anbieter Zentrales Netz TI
Offene Fachdienste	64K	172.30.0.0/16	Offene Fachdienste	Anbieter Offene Fachdienste
	Der Anbieter Zentrales Netz TI weist jedem Offenen Fachdienst ein /26 Adressblock aus dem Bereich 172.30.0.0/16 zu			
Gesicherte Fachdienste	64K	172.28.0.0/16	Gesicherte Fachdienste	Anbieter Gesicherte Fachdienste
	Der Anbieter Zentrales Netz TI weist jedem Gesicherten Fachdienst ein /26 Adressblock aus dem Bereich 172.28.0.0/16 zu			
(TI_Test_Dezentral_SIS) (siehe Erläuterung)	172.29.0.0/16		Dezentral SIS	Anbieter Zentrales Netz TI
Konnektoren	64K	172.29.0.0/16	Konnektoren	Anbieter

Netzbereich	Adressen	Netz	Nutzung	Verantwortlich
			SIS	Zugangsdienst
Reserveblöcke	128K	172.31.0.0/16	Reserve	Anbieter Zentrales Netz TI

⌫

Erläuterung:
Aus dem Netzbereich 172.16.0.0/14 sollen nur noch IP-Adressblöcke für den dezentralen Zugang zur TI (TI_Dezentral) zugeteilt werden. Die IP-Adressblöcke, die schon für den Zugang SIS eingeteilt wurden, bleiben bestehen und müssen nicht verändert werden.
Für den dezentralen SIS-Zugang muss dem Anbieter des VPN-Zugangsdienstes der IP-Adressblock 172.29.0.0/16 fest zugewiesen werden. Somit ist der IP-Adressblock TI_Dezentral_SIS für jeden VPN-Zugangsdienstanbieter identisch.