

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikanstruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

## Änderungsbedarf in PTSB [gemProdT\_Kon\_PTV3]

### 3.2.3 Sicherheitsgutachten

Die in diesem Abschnitt verzeichneten Anforderungen sind Gegenstand der Prüfung der Sicherheitseignung gemäß [gemRL\_PruefSichEig]. Das entsprechende Sicherheitsgutachten ist der gematik vorzulegen.

Die Anforderungen in diesem Kapitel sind durch den Personalisierer der Gerätekarte gSMC-K für den Konnektor zu erfüllen. betreffen die Herausgabe der gSMC-K. Das Sicherheitsgutachten muss entsprechend die Schlüsselerzeugung, den Zertifikatbezug und die Personalisierung der Daten auf die gSMC-K umfassen.

Werden alle Aufgaben vom Personalisierer der gSMC-K erfüllt, ist vom Hersteller ein Sicherheitsgutachten des Personalisierers erforderlich.

Wenn der Hersteller des Konnektors die Schlüssel für die gSMC-K jedoch selber erzeugt oder von einem Dritten (der nicht der Personalisierer ist) erzeugen lässt, ist neben dem Sicherheitsgutachten vom Personalisierer auch vom Hersteller oder dem von ihm beauftragten Dritten ein entsprechendes Sicherheitsgutachten, das die Schlüsselerzeugung umfasst, einzureichen.

Erzeugt der Hersteller oder ein von ihm beauftragter Dritter ausschließlich „Herstellerspezifische Schlüssel“ sowie Schlüssel zur Kartenadministration (konkret Schlüssel für Objekte der Abschnitte 5.3.20, 5.3.22 und 5.3.23 der Objektsystemspezifikation der gSMC-K G2.0 [gemSpec\_gSMC-K\_ObjSys]), ist neben dem Sicherheitsgutachten vom Personalisierer eine Herstellererklärung über die Umsetzung der Anforderungen in Tabelle 10 zur Zulassung ausreichend.

**Tabelle 10: Anforderungen zur Herstellererklärung für die Erzeugung herstellereigener Schlüssel und Admin-Schlüssel durch den Hersteller des Konnektors selbst**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3593	Schlüsselspeicherung	gemSpec_gSMC-K_ObjSys
GS-A_4366	CV-CA-Zertifikate G2	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_5021	Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung	gemSpec_Krypt
TIP1-A_7225	Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung	gemSpec_Kon
TIP1-A_5703	Geschützte Übertragung von Daten zum Kartenpersonalisierer	gemSpec_Kon

Zusätzlich ist stets vom Personalisierer und, falls dieser nicht die Schlüssel erzeugt, auch vom Hersteller oder dem von ihm beauftragten Dritten die Herstellererklärung zur Erfüllung der Anforderungen in Kapitel 3.2.4, Tabelle 13 zu erbringen.

[...]

### 3.2.4 Herstellererklärung sicherheitstechnische Eignung

Sofern in diesem Abschnitt Anforderungen verzeichnet sind, muss der Hersteller bzw. der Anbieter deren Umsetzung und Beachtung zum Nachweis der sicherheitstechnischen Eignung durch eine Herstellererklärung bestätigen bzw. zusagen.

**Tabelle 12: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
[...]	[...]	[...]

**Tabelle 13: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung" spezifisch für die Herausgabe der gSMC-K**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4233	Zertifikatsuspendierung für Kartenzertifikate	gemRL_TSL_SP_CP
GS-A_4479	kDSM: Meldung von Kontaktinformationen zum Datenschutzmanagement	gemSpec_DSM
Card-G2-A_3593	Schlüsselspeicherung	gemSpec_gSMC-K_ObjSys
GS-A_4523	Bereitstellung Kommunikationsschnittstelle für Informationssicherheit	gemSpec_ISM
GS-A_4524	Meldung von Kontaktinformationen zum Informationssicherheitsmanagement	gemSpec_ISM
GS-A_4528	Meldung von lokalen Sicherheitsvorfällen	gemSpec_ISM
GS-A_4362	X.509-Identitäten für Verschlüsselungszertifikate	gemSpec_Krypt
GS-A_4365	CV-Zertifikate G2	gemSpec_Krypt
GS-A_4366	CV-CA-Zertifikate G2	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_5021	Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung	gemSpec_Krypt
GS-A_4380	Card-to-Server (C2S) Authentisierung und Trusted Channel G2	gemSpec_Krypt
GS-A_4381	Schlüssellängen Algorithmus AES	gemSpec_Krypt
GS-A_4963	Deaktivierung von Chipkarten nach Gültigkeitsende	gemSpec_PKI
GS-A_4965	Suspendierung von X.509-Zertifikaten (außer für eGK)	gemSpec_PKI
GS-A_4972	Bezug des CV-Zertifikat	gemSpec_PKI
GS-A_4973	Ausstellung aller CV-Zertifikate einer Karte durch gleiche CVC-	gemSpec_PKI

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Sub-CA	
GS-A_3784	Nachweis durch ISO27001 Zertifikat	gemSpec_SiBetrUmg
GS-A_2356	ISM der Beteiligten: Nutzung des Incident-Management-Prozesses	gemSpec_Sich_DS
GS-A_2524	Produktunterstützung: Nutzung des Problem-Management-Prozesses	gemSpec_Sich_DS
GS-A_2525	Hersteller: Schließen von Schwachstellen	gemSpec_Sich_DS
GS-A_2354	Produktunterstützung mit geeigneten Sicherheits-Technologien	gemSpec_Sich_DS
GS-A_2350	Produktunterstützung der Hersteller	gemSpec_Sich_DS

## Änderungsbedarf in PTSB [gemProdT\_eHealth\_KT]

### 3.2.2 Sicherheitsgutachten

Die in diesem Abschnitt verzeichneten Anforderungen sind Gegenstand der Prüfung der Sicherheitseignung gemäß [gemRL\_PruefSichEig]. Das entsprechende Sicherheitsgutachten ist der gematik vorzulegen.

Die Anforderungen in diesem Kapitel sind durch den Personalisierer der Gerätekarte gSMC-KT für das eHealth-Kartenterminal zu erfüllen.

Zusätzlich ist stets vom Personalisierer die Herstellererklärung zur Erfüllung der Anforderungen in Kapitel 3.2.3, Tabelle 7 zu erbringen.

[...]

### 3.2.3 Herstellererklärung sicherheitstechnische Eignung

Sofern in diesem Abschnitt Anforderungen verzeichnet sind, muss der Hersteller bzw. der Anbieter deren Umsetzung und Beachtung zum Nachweis der sicherheitstechnischen Eignung durch eine Herstellererklärung bestätigen bzw. zusagen.

**Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
[...]	[...]	[...]

**Tabelle 7: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung" spezifisch für die Herausgabe der gSMC-KT**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4233	Zertifikatsuspendierung für Kartenzertifikate	gemRL_TSL_SP_CP
GS-A_4479	kDSM: Meldung von Kontaktinformationen zum Datenschutzmanagement	gemSpec_DSM
GS-A_4523	Bereitstellung Kommunikationsschnittstelle für Informationssicherheit	gemSpec_ISM
GS-A_4524	Meldung von Kontaktinformationen zum Informationssicherheitsmanagement	gemSpec_ISM
GS-A_4528	Meldung von lokalen Sicherheitsvorfällen	gemSpec_ISM
GS-A_4365	CV-Zertifikate G2	gemSpec_Krypt
GS-A_4366	CV-CA-Zertifikate G2	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_5021	Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung	gemSpec_Krypt
GS-A_4380	Card-to-Server (C2S) Authentisierung und Trusted Channel G2	gemSpec_Krypt
GS-A_4381	Schlüssellängen Algorithmus AES	gemSpec_Krypt

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4963	Deaktivierung von Chipkarten nach Gültigkeitsende	gemSpec_PKI
GS-A_4965	Suspendierung von X.509-Zertifikaten (außer für eGK)	gemSpec_PKI
GS-A_4972	Bezug des CV-Zertifikat	gemSpec_PKI
GS-A_4973	Ausstellung aller CV-Zertifikate einer Karte durch gleiche CVC-Sub-CA	gemSpec_PKI
GS-A_3784	Nachweis durch ISO27001 Zertifikat	gemSpec_SiBetrUmg
GS-A_2356	ISM der Beteiligten: Nutzung des Incident-Management-Prozesses	gemSpec_Sich_DS
GS-A_2524	Produktunterstützung: Nutzung des Problem-Management-Prozesses	gemSpec_Sich_DS
GS-A_2525	Hersteller: Schließen von Schwachstellen	gemSpec_Sich_DS
GS-A_2354	Produktunterstützung mit geeigneten Sicherheits-Technologien	gemSpec_Sich_DS
GS-A_2350	Produktunterstützung der Hersteller	gemSpec_Sich_DS