Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

Bestätigungsgegenstand Sicherheit für die Herausgabe- und Nutzungsprozesse der eGK

Produkttyp Version:	4.4.0-0
Produkttyp Status:	freigegeben

Version:	1.0.0
Revision:	111375
Stand:	15.05.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemProdT_eGK_Sich_G2_1_PTV_4.4.0-0

Historie Produkttypversion und Produkttypsteckbrief

Historie Produkttypversion

Die Produkttypversion ändert sich, wenn sich die Anforderungslage für den Produkttyp ändert und die Umsetzung durch Produktentwicklungen ebenfalls betroffen ist.

Produkttypversion	Beschreibung der Änderung	Referenz
4.0.0	Initial erstellt – Korrespondiert mit der Produkttypversion 4.0.0 der eGK	[gemProdT_eGK_SichPTV4.0.0]
4.0.1	PT-Version angepasst an PTV 4.0.1 der eGK	[gemProdT_eGK_SichPTV4.0.1]
4.1.0	Aktualisierung auf Releasestand 1.3.0	[gemProdT_eGK_SichPTV4.1.0]
4.2.0	Anpassungen für Online-Produktivbetrieb	[gemProdT_eGK_SichPTV4.2.0]
4.2.0-0	Anpassung auf Releasestand 1.6.3	[gemProdT_eGK_SichPTV4.2.0-0]
4.3.0-0	Kartengeneration 2.1	[gemProdT_eGK_SichPTV4.3.0-0]
4.3.0-1	Anpassung auf Releasestand 2.1.2	[gemProdT_eGK_SichPTV4.3.0-1]
4.4.0-0	Anpassung auf Releasestand 3.1.0	[gemProdT_eGK_SichPTV4.4.0-0]

Historie Produkttypsteckbrief

Die Dokumentenversion des Produkttypsteckbriefs ändert sich mit jeder inhaltlichen oder redaktionellen Änderung des Produkttypsteckbriefs und seinen referenzierten Dokumenten. Redaktionelle Änderungen haben keine Auswirkung auf die Produkttypversion.

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	15.05.2019		freigegeben	gematik

Inhaltsverzeichnis

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik bezüglich der Sicherheit der Herausgabe- und Nutzungsprozesse des Produkttyps eGK (personalisierte und bedruckte Karte) oder verweist auf Dokumente, in denen verbindliche Anforderungen mit ggf. anderer Notation zu finden sind. Die Anforderungen bilden die Grundlage für Bestätigungsverfahren der gematik.

Die Anforderungen werden über ihren Identifier, ihren Titel sowie die Dokumentenquelle referenziert. Die Anforderungen mit ihrem vollständigen, normativen Inhalt sind dem jeweils referenzierten Dokument zu entnehmen.

1.2 Zielgruppe

Der Produkttypsteckbrief richtet sich an eGK-Herausgeber, deren Dienstleister sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Bestätigungsverfahrens
- Sicherheitsgutachter/Auditoren

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Leistungsbeschreibung) festgelegt und bekannt gegeben.

1.4 Abgrenzung des Dokumentes

Dieses Dokument definiert den Anforderungsumfang an den Produkttypen eGK nicht umfassend, sondern lediglich in den Teilen, die für die Sicherheit innerhalb der Herausgabe- und Nutzungsprozesse relevant sind.

Dieses Dokument macht keine Aussagen zur Aufteilung der Produktentwicklung bzw. Produktherstellung auf verschiedene Hersteller und Anbieter.

Dokumente zu den Zulassungs- bzw. Bestätigungsverfahren für den Produkttyp sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können der Homepage der gematik entnommen werden.

1.5 Methodik

Die im Dokument verzeichneten Anforderungen werden tabellarisch dargestellt. Die Tabellenspalten haben die folgende Bedeutung:

Afo-ID: Identifiziert die Anforderung eindeutig im Gesamtbestand aller Festlegungen der gematik.

Afo-Bezeichnung: Gibt den Titel einer Anforderung informativ wider, um die thematische Einordnung zu erleichtern. Der vollständige Inhalt der Anforderung ist dem Dokument zu entnehmen, auf das die Quellenangabe verweist.

Quelle (Referenz): Verweist auf das Dokument, das die Anforderung definiert.

2 Dokumente

Die nachfolgenden Dokumente enthalten die im Zusammenhang mit der Sicherheit für die Herausgabe- und Nutzungsprozesse der eGK G2 normativen Anforderungen.

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion

Dokumentenkürzel	Bezeichnung des Dokumentes	Version
gemSpec_SMC_OPT	Gemeinsame optische Merkmale der SMC	3.7.0
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	1.1.0
gemSpec_SMC-B_ObjSys_G2_1	Spezifikation der Security Module Card SMC-B Objektsystem	4.4.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.13.0
gemSpec_CVC_TSP	Spezifikation Trust Service Provider CVC	1.12.0
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.5.0
gemSpec_CAN_TI	Übergreifende Spezifikation CAN-Policy	1.0.0
gemSpec_eGK_Fach_VSDM	Speicherstrukturen der eGK für die Fachanwendung VSDM	1.2.0
gemSpec_PINPUK_TI	Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur	1.3.0
gemRL_TSL_SP_CP	Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL	2.3.0
gemSpec_eGK_ObjSys_G2_1	Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem (G2.1)	4.3.0
gemKPT_Test	Testkonzept der TI	2.3.0
gemSpec_eGK_Opt	Spezifikation der elektronischen Gesundheitskarte – Äußere Gestaltung	3.8.0
gemSpec_Karten_Fach_TIP_G2_1	Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	3.0.0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.12.0

Errata

Neben den vorgenannten Dokumenten werden auf der Internetseite der gematik bei Bedarf Errata-Dokumente mit normativen Ergänzungen bzw. Korrekturen zu den Spezifikationsdokumenten veröffentlicht. Sofern in den Errata der vorliegende Produkttyp benannt wird, sind diese bei der Umsetzung des Produkttyps entsprechend der Vorgabe in der Dokumentenlandkarte zu berücksichtigen. Dabei kann eine abweichende Produkttypversion festgelegt werden.

3 Blattanforderungen

Die folgenden Abschnitte verzeichnen alle im Zusammenhang mit der Sicherheit für die Herausgabe- und Nutzungsprozesse der eGK G2 normativen Anforderungen, (Blattanforderungen).

3.1 Anforderungen zur sicherheitstechnischen Eignung: Sicherheitsgutachten

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

Dieser Produkttypsteckbrief richtet sich an den Kartenherausgeber insgesamt. Sofern die Rollen im eGK-Herausgabeprozess (CAMS Betreiber, Personalisierer) von verschiedenen Parteien ausgefüllt werden, so muss der Sicherheitsgutachter eigenständig entscheiden, an welcher Stelle die relevanten Anforderungen zu prüfen sind. Darüber hinaus muss er zusätzliche Sicherheitsanforderungen berücksichtigen, die ggf. aufgrund dieser Trennung an den Schnittstellen zwischen den Rollen entstehen.

Tabelle 2: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5115	Schutzbedarf der CAN	gemSpec_CAN_TI
GS-A_5116	Zufällige CAN-Erzeugung	gemSpec_CAN_TI
GS-A_5117	Anforderungen an Zufallsgenerator für CAN-Erzeugung	gemSpec_CAN_TI
GS-A_5118	CAN-Speicherung nur für die Personalisierung der Karte	gemSpec_CAN_TI
GS-A_5119	Sicherer Transport und Speicherung der CAN beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_CAN_TI
GS-A_5120	Verteilung der CAN auf das erforderliche Maß beschränken	gemSpec_CAN_TI
GS-A_5121	Karteninhaber über Umgang mit CAN informieren	gemSpec_CAN_TI
TIP1-A_2579	Korrekter privater Schlüssel in der Chipkarte	gemSpec_CVC_TSP
TIP1-A_2580	Erzeugung des privaten Schlüssels der Chipkarte	gemSpec_CVC_TSP
TIP1-A_2582	Vertraulichkeit des privaten Schlüssels der	gemSpec_CVC_TSP

	Chipkarte	
TIP1-A_2583	Zuordnung des privaten Schlüssels zu Identitäten	gemSpec_CVC_TSP
TIP1-A_2590	Vernichtung fehlerhafter Chipkarten vor deren Ausgabe	gemSpec_CVC_TSP
TIP1-A_2591	Ausgabe fehlerfreier Chipkarten	gemSpec_CVC_TSP
TIP1-A_4222	Authentizität des öffentlichen Root-Schlüssels	gemSpec_CVC_TSP
GS-A_2076-01	kDSM: Datenschutzmanagement nach BSI	gemSpec_DS_Anbieter
GS-A_2158-01	Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen	gemSpec_DS_Anbieter
GS-A_2328-01	Pflege und Fortschreibung des Sicherheitskonzeptes und Notfallkonzeptes	gemSpec_DS_Anbieter
GS-A_2329-01	Umsetzung der Sicherheitskonzepte	gemSpec_DS_Anbieter
GS-A_2331-01	Sicherheitsvorfalls-Management	gemSpec_DS_Anbieter
GS-A_2332-01	Notfallmanagement	gemSpec_DS_Anbieter
GS-A_2345-01	regelmäßige Reviews	gemSpec_DS_Anbieter
GS-A_2355-01	Meldung von erheblichen Schwachstellen und Bedrohungen	gemSpec_DS_Anbieter
GS-A_3737-01	Sicherheitskonzept	gemSpec_DS_Anbieter
GS-A_3753-01	Notfallkonzept	gemSpec_DS_Anbieter
GS-A_3772-01	Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen	gemSpec_DS_Anbieter
GS-A_4473-01	kDSM: Unverzügliche Benachrichtigung bei Verstößen gemäß Art. 34 DSGVO	gemSpec_DS_Anbieter
GS-A_4479-01	kDSM: Meldung von Änderungen der Kontaktinformationen zum Datenschutzmanagement	gemSpec_DS_Anbieter
GS-A_4523-01	Bereitstellung Kontaktinformationen für Informationssicherheit	gemSpec_DS_Anbieter
GS-A_4524-01	Meldung von Änderungen der Kontaktinformationen für Informationssicherheit	gemSpec_DS_Anbieter
GS-A_4980-01	Umsetzung der Norm ISO/IEC 27001	gemSpec_DS_Anbieter
GS-A_4981-01	Erreichen der Ziele der Norm ISO/IEC 27001 Annex A	gemSpec_DS_Anbieter

GS-A_4982-01	Umsetzung der Maßnahmen der Norm ISO/IEC 27002	gemSpec_DS_Anbieter
GS-A_4983-01	Umsetzung der Maßnahmen aus dem BSI-Grundschutz	gemSpec_DS_Anbieter
GS-A_4984-01	Befolgen von herstellerspezifischen Vorgaben	gemSpec_DS_Anbieter
GS-A_5555	Unverzügliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_5556	Unverzügliche Behebung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_5564	kDSM: Ansprechpartner für Datenschutz	gemSpec_DS_Anbieter
GS-A_5565	kDSM: Unverzügliche Behebung von Verstößen gemäß Art. 34 DSGVO	gemSpec_DS_Anbieter
GS-A_5626	kDSM: Auftragsverarbeitung	gemSpec_DS_Anbieter
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_4380	Card-to-Server (C2S) Authentisierung und Trusted Channel G2	gemSpec_Krypt
GS-A_4381	Schlüssellängen Algorithmus AES	gemSpec_Krypt
GS-A_4384	TLS-Verbindungen	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4386	TLS-Verbindungen, optional Version 1.1	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_4391	MAC im Rahmen der Personalisierung der eGK	gemSpec_Krypt
GS-A_4392	Algorithmus im Rahmen der Bildung der pseudonymisierten Versichertenidentität	gemSpec_Krypt
GS-A_5021	Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt

GS-A_5386	kartenindividuelle geheime und private Schlüssel G2-Karten	gemSpec_Krypt
GS-A_2227	Keine Kartendubletten	gemSpec_PINPUK_TI
GS-A_2228	Trennung von Karte und PIN/PUK-Brief	gemSpec_PINPUK_TI
GS-A_2229	Prozesse und Maßnahmen zur Aushändigung von Karte und PIN/PUK-Brief	gemSpec_PINPUK_TI
GS-A_2230	PIN/PUK-Erzeugung: Länge PIN/PUK (Kartenherausgeber)	gemSpec_PINPUK_TI
GS-A_2232	PIN/PUK-Erzeugung: Verfahren für PIN/PUK-Auswahl	gemSpec_PINPUK_TI
GS-A_2234	PIN/PUK-Erzeugung: Zufallsgenerator für PIN/PUK	gemSpec_PINPUK_TI
GS-A_2235	PIN/PUK-Erzeugung: Ableitung von PIN	gemSpec_PINPUK_TI
GS-A_2236	PIN/PUK-Erzeugung: Ableitung der PIN aus eindeutig dem Versicherten zugeordneten Daten	gemSpec_PINPUK_TI
GS-A_2237	PIN/PUK-Erzeugung: kein Rückschluss von PIN/PUK auf Schlüssel	gemSpec_PINPUK_TI
GS-A_2238	PIN/PUK-Erzeugung: Informationen an Karteninhaber bei selbstständiger Wahl der PIN	gemSpec_PINPUK_TI
GS-A_2239	PIN/PUK-Erzeugung: Ableitung von PIN im Sicherheitsmodul	gemSpec_PINPUK_TI
GS-A_2240	PIN/PUK-Speicherung: Verschlüsselung der PIN außerhalb von Sicherheitsmodulen	gemSpec_PINPUK_TI
GS-A_2242	PIN/PUK-Speicherung: Integrität der PIN außerhalb von Sicherheitsmodulen	gemSpec_PINPUK_TI
GS-A_2244	PIN/PUK-Speicherung: Verschlüsselung unterschiedlicher PINs mit unterschiedlichen Schlüsseln	gemSpec_PINPUK_TI
GS-A_2246	PIN/PUK-Speicherung: Verschlüsselung gleicher PINs führt zu unterschiedlichen verschlüsselten Werten	gemSpec_PINPUK_TI
GS-A_2247	PIN/PUK-Speicherung: Wiederholte Verschlüsselung der PIN führt zu unterschiedlichen Werten	gemSpec_PINPUK_TI
GS-A_2248	PIN/PUK-Speicherung: unterschiedliche Schlüssel für unterschiedliche Zwecke	gemSpec_PINPUK_TI
GS-A_2249	PIN/PUK-Speicherung: Dokumentation der Zwecke	gemSpec_PINPUK_TI

GS-A_2250	PIN/PUK-Speicherung: Entschlüsselung nur durch berechtigten Empfänger	gemSpec_PINPUK_TI
GS-A_2252	PIN/PUK-Löschung: Löschung von PIN/PUK nach Ablauf der Speicherdauer	gemSpec_PINPUK_TI
GS-A_2253	PIN/PUK-Transport: Sicherer PIN-Transport beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_2254	PIN/PUK-Transport: Schutz außerhalb geschützter Hardware beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_2255	PIN/PUK-Transport: Verteilung beschränken	gemSpec_PINPUK_TI
GS-A_2256	PIN/PUK-Transport: einmalige PIN-Erstellung beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_2260	PIN/PUK-Transport: Transport außerhalb eines Sicherheitsmoduls	gemSpec_PINPUK_TI
GS-A_2261	PIN/PUK-Transport: Transport außerhalb eines Sicherheitsmoduls - kein Klartext	gemSpec_PINPUK_TI
GS-A_2264	PIN/PUK-Transport: elektronische PIN-Verteilung	gemSpec_PINPUK_TI
GS-A_2266	PIN/PUK-Transport: Verschlüsselung gleicher PINs muss zu unterschiedlichen Werten führen	gemSpec_PINPUK_TI
GS-A_2270	PIN/PUK-Transport: Unterschiedliche verschlüsselte Werte auch bei gleichen PINs	gemSpec_PINPUK_TI
GS-A_2271	PIN/PUK-Transport: kein Rückschluss auf vorher benutzte Schlüssel	gemSpec_PINPUK_TI
GS-A_2274	PIN/PUK-Transport: Löschung der PIN nach Transport	gemSpec_PINPUK_TI
GS-A_2276	PIN/PUK-Transport: Aktivitäten im Vier-Augen-Prinzip bei der Zuordnung einer PIN/PUK zu einer Karte	gemSpec_PINPUK_TI
GS-A_2277	PIN/PUK-Transport: Aktivitäten im Vier-Augen-Prinzip beim Rücksetzen des Fehlbedienungszählers	gemSpec_PINPUK_TI
GS-A_2284	PIN/PUK-Änderung: Änderungen durch Kartenpersonalisierer im Vier-Augen-Prinzip	gemSpec_PINPUK_TI
GS-A_2285	PIN/PUK-Änderung: Prozess bei Kompromittierung beim Kartenherausgeber bzw.	gemSpec_PINPUK_TI

	Kartenpersonalisierer	
GS-A_2287	PIN/PUK-Löschung: Nachweis der Löschung nicht mehr gebrauchter PIN beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_2291	PIN/PUK-Löschung: Löschen von nicht mehr benötigten Klartext-PIN	gemSpec_PINPUK_TI
GS-A_2292	PIN/PUK-Löschung: Außerbetriebnahme der PIN und Karte	gemSpec_PINPUK_TI
GS-A_2295	Schutz der Schlüssel für PIN/PUK gemäß Hierarchiestufe 4	gemSpec_PINPUK_TI
GS-A_5085	PIN/PUK-Änderung: Prozess bei Kompromittierungsmeldung durch Karteninhaber	gemSpec_PINPUK_TI
GS-A_5209	PIN/PUK-Speicherung: PIN/PUK unverzüglich löschen	gemSpec_PINPUK_TI
GS-A_5387	Beachten von Vorgaben bei der Kartenpersonalisierung	gemSpec_PINPUK_TI
GS-A_4578	eGK hs-ZW Bildungsregel	gemSpec_PKI
GS-A_4579	eGK hs-ZW Verwendung/Wechsel	gemSpec_PKI
GS-A_4580	eGK hs-ZW Archivierung	gemSpec_PKI
Card-G2-A_3335-01	K_Personalisierung: Option des PIN-Brief-Versands für MF / PIN.AMTS_REP	gemSpec_eGK_ObjSys_G2.1

4 Anhang A – Verzeichnisse

4.1 Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

4.2 Tabellenverzeichnis

4.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[gemRL_PruefSichEig]	gematik: Richtlinie zur Prüfung der Sicherheitseignung