

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

eHealth-CardLink

Produkttyp Version: 1.0.0-0
Produkttyp Status: freigegeben

Version: 1.0.0
Revision: 867473
Stand: 19.03.2024
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemProdT_eHealth-CardLink_PTV_1.0.0-0

Historie Produkttypversion und Produkttypsteckbrief

Historie Produkttypversion

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

Produkttypversion	Beschreibung der Änderung	Referenz
1.0.0-0	Initiale Version	gemProdT_eHealth- CardLink_PTV_1.0.0-0

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	19.03.2024		freigegeben	gematik

Inhaltsverzeichnis

1 Einführung	4
1.1 Zielsetzung und Einordnung des Dokumentes	4
1.2 Zielgruppe	4
1.3 Geltungsbereich	4
1.4 Abgrenzung des Dokumentes	5
1.5 Methodik	5
2 Dokumente	6
3 Normative Festlegungen	8
3.1 Festlegungen zur funktionalen Eignung	8
3.1.1 Produkttest/Produktübergreifender Test.....	8
3.1.2 Herstellererklärung funktionale Eignung.....	12
3.2 Festlegungen zur sicherheitstechnischen Eignung	14
3.2.1 CC-Evaluierung.....	14
3.2.2 Zertifizierung nach Technischer Richtlinie.....	15
3.2.3 Produktgutachten.....	15
3.2.4 Sicherheitsgutachten.....	17
3.2.5 Herstellererklärung sicherheitstechnische Eignung.....	17
3.3 Festlegungen zur elektrischen, mechanischen und physikalischen Eignung	18
4 Produkttypspezifische Merkmale	19
5 Anhang - Verzeichnisse	20
5.1 Abkürzungen	20
5.2 Tabellenverzeichnis	20

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die normativen Festlegungen der gematik an Herstellung und Betrieb von Produkten des Produkttyps eHealth-CardLink oder verweist auf Dokumente, in denen verbindliche normative Festlegungen mit ggf. anderer Notation zu finden sind. Die normativen Festlegungen bilden die Grundlage für die Erteilung von Zulassungen, Zertifizierungen bzw. Bestätigungen durch die gematik. (Wenn im weiteren Dokument vereinfachend der Begriff „Zulassung“ verwendet wird, so ist dies der besseren Lesbarkeit geschuldet und umfasst übergreifend neben dem Verfahren der Zulassung auch Zertifizierungen und Bestätigungen der gematik-Zulassungsstelle.)

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

1.2 Zielgruppe

Der Produkttypsteckbrief richtet sich an eHealth-CardLink-Hersteller und -Anbieter sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Zulassungsverfahrens,
- dem Bundesamt für Sicherheit in der Informationstechnik (BSI),
- akkreditierten Materialprüflaboren,
- Auditoren.

Bei zentralen Diensten der TI-Plattform und fachanwendungsspezifischen Diensten beziehen sich normative Festlegungen, die sowohl an Anbieter als auch Hersteller gerichtet sind, jeweils auf den Anbieter als Zulassungsnehmer, bei dezentralen Produkten auf den Hersteller.

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

Dokumente zu den Zulassungsverfahren für den Anbietertyp sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können dem Fachportal der gematik (<https://fachportal.gematik.de/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen>) entnommen werden.

1.5 Methodik

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

ID: Identifiziert die normative Festlegung eindeutig im Gesamtbestand aller Festlegungen der gematik.

Bezeichnung: Gibt den Titel einer normativen Festlegung informativ wieder, um die thematische Einordnung zu erleichtern. Der vollständige Inhalt der normativen Festlegung ist dem Dokument zu entnehmen, auf das die Quellenangabe verweist.

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

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Produkttyp normativen Festlegungen.

Tabelle 1: Dokumente mit normativen Festlegungen

Dokumenten Kürzel	Bezeichnung des Dokumentes	Version
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.31.0
gemRL_TSL_SP_CP	Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL	2.12.0
gemSpec_Net	Übergreifende Spezifikation Netzwerk	1.27.0
gemSpec_KT	Spezifikation eHealth-Kartenterminal	3.17.0
gemKPT_Test	Testkonzept der TI	2.9.0
gemSpec_eHealth-CardLink	Spezifikation eHealth-CardLink	1.0.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.39.0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.16.0

Weiterhin sind die in folgender Tabelle aufgeführten Dokumente und Web-Inhalte normativ und gelten mit.

Tabelle 2: Mitgeltende Dokumente und Web-Inhalte

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag
[SICCT]	SICCT TeleTrusT, SICCT Secure Interoperable ChipCard Terminal, Version 1.2.3, 30. September 2016 Errata zu SICCT1.2.3, Version 1.0 vom 5. Mai 2021	
[gemRL_PruefSichEig_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung	2.2.0
[gemSpec_OID]	Spezifikation Festlegung von OIDs	3.14.0
Github	https://github.com/gematik/api-ehcl/blob/ehcl_1.0.0/ehcl/asyncapi.yaml	

Hinweis:

- Ist kein Herausgeber angegeben, wird angenommen, dass die gematik für Herausgabe und Veröffentlichung der Quelle verantwortlich ist.
- Ist keine Version angegeben, bezieht sich die Quellenangabe auf die aktuellste Version.
- Bei Quellen aus gitHub werden als Version Branch und / oder Tag verwendet.

3 Normative Festlegungen

Die folgenden Abschnitte verzeichnen alle für den Produkttypen normativen Festlegungen, die für die Herstellung und den Betrieb von Produkten des Produkttyps notwendig sind. Die Festlegungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der Zulassung, Zertifizierung bzw. Bestätigung.

3.1 Festlegungen zur funktionalen Eignung

3.1.1 Produkttest/Produktübergreifender Test

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Festlegungen an den technischen Teil des Produkttyps verzeichnet, deren Umsetzung im Zuge von Zulassungstests durch die gematik geprüft wird.

Tabelle 3: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

ID	Bezeichnung	Quelle (Referenz)
A_22450	TLS-Ciphersuiten	gemSpec_KT
A_22456	SICCT-spezifischer TLS-Kanal, Zustandsautomat	gemSpec_KT
A_22461	Erlaubte Kommandos für State_NoSicctTls	gemSpec_KT
A_22888	K_KT, CA-Zertifikat suchen	gemSpec_KT
A_22890	K_KT, erfolgreicher TLS-Handshake	gemSpec_KT
A_22891	K_KT, KEEP ALIVE Ereignisnachrichten	gemSpec_KT
A_24065	K_KT, netzwerkbasierte Managementschnittstelle, TLS-Verbindung	gemSpec_KT
A_24102	Schlüsselmaterial für netzwerkbasierte Managementschnittstellen	gemSpec_KT
TIP1-A_2948	Definition SICCT/eHealth	gemSpec_KT
TIP1-A_2971	Über LAN-Netzwerk administrieren	gemSpec_KT
TIP1-A_2983	Übertragung medizinischer und personenbezogener Daten	gemSpec_KT
TIP1-A_2984	Anzeige medizinischer und personenbezogener Daten	gemSpec_KT
TIP1-A_3005	Zufallszahlen und Einmalschlüsseln	gemSpec_KT
TIP1-A_3006	Mindestanzahl Pairing-Block	gemSpec_KT

TIP1-A_3012	Streichung "SICCT SELECT CT MODE"	gemSpec_KT
TIP1-A_3038	Vertrauenswürdiger Zustand	gemSpec_KT
TIP1-A_3039	Quelle für Zufallszahlen Zufallszahlengenerator des SM-KT	gemSpec_KT
TIP1-A_3044	Erstellung des Authentifizierungstokens	gemSpec_KT
TIP1-A_3045	Pairing-Information	gemSpec_KT
TIP1-A_3046-01	Pairing-Block	gemSpec_KT
TIP1-A_3049	Löschung Pairing-Blöcke	gemSpec_KT
TIP1-A_3050	Löschung öffentliche Schlüssel	gemSpec_KT
TIP1-A_3065	Verbindungsabbruch	gemSpec_KT
TIP1-A_3067	Anzahl Konnektorverbindungen	gemSpec_KT
TIP1-A_3068	Mehrere Verbindungen über SICCT-Port	gemSpec_KT
TIP1-A_3070	Ressourcen und unterschiedliche Kontexte	gemSpec_KT
TIP1-A_3075	SICCT-Kommandos über Netzwerk	gemSpec_KT
TIP1-A_3077	Kommandopuffer für APDUs	gemSpec_KT
TIP1-A_3078	Shared Secrets und die öffentlichen Schlüssel	gemSpec_KT
TIP1-A_3096-01	Erlaubte Kommandos für State_ClientWithoutPairing	gemSpec_KT
TIP1-A_3097-01	Erlaubte Kommandos für State_ClientWithPairing	gemSpec_KT
TIP1-A_3115	Zustand EHEALTH EXPECT CHALLENGE RESPONSE, Timeout	gemSpec_KT
TIP1-A_3118	Discretionary Data Data Object	gemSpec_KT
TIP1-A_3119	Kommandostruktur des EHEALTH TERMINAL AUTHENTICATE Kommandos	gemSpec_KT
TIP1-A_3120	Antwortstruktur des EHEALTH TERMINAL AUTHENTICATE Kommandos	gemSpec_KT
TIP1-A_3121	Allgemeine Status Codes gemäß SICCT-Spezifikation	gemSpec_KT
TIP1-A_3122	"Shared Secret Data Object Definition"	gemSpec_KT

TIP1-A_3123	“Shared Secret Data Object Challenge Definition”	gemSpec_KT
TIP1-A_3124	“Shared Secret Data Object Response Definition”	gemSpec_KT
TIP1-A_3125-03	Kommando mit P2='01' (CREATE)	gemSpec_KT
TIP1-A_3126	Kommando mit P2='02' (VALIDATE)	gemSpec_KT
TIP1-A_3127	P2='03' (ADD Phase 1)	gemSpec_KT
TIP1-A_3128	P2='04' (ADD Phase 2)	gemSpec_KT
TIP1-A_3131	Ergänzung der SICCT-Spezifikation	gemSpec_KT
TIP1-A_3136-01	Erlaubte Kommandos für State_InvalidClient	gemSpec_KT
TIP1-A_3151	UNICast basierte Dienstanfragepakete	gemSpec_KT
TIP1-A_3177	Ausführung des Kommandos EHEALTH TERMINAL AUTHENTICATE	gemSpec_KT
TIP1-A_3184	KT-Unterstützung des anonymen Zugriffs für Rolle CT CONTROL	gemSpec_KT
TIP1-A_3189	Unterstützung IPv4	gemSpec_KT
TIP1-A_3191	Definition anonyme Session	gemSpec_KT
TIP1-A_3227	Umsetzung der KT-Identität	gemSpec_KT
TIP1-A_3243	Initiales Pairing	gemSpec_KT
TIP1-A_3244	Außerbetriebnahme eines eHealth-Kartenterminals	gemSpec_KT
TIP1-A_3250	Deadlock während Kartenkommunikation	gemSpec_KT
TIP1-A_3251	„CONTROL COMMAND“-Kommando	gemSpec_KT
TIP1-A_3264	Return Code Control Command	gemSpec_KT
TIP1-A_3265	Ergänzung Sicherheitsprotokolle	gemSpec_KT
TIP1-A_3266-01	Kartenkommandos für State_ClientWithPairing	gemSpec_KT
TIP1-A_3948	CTM Festlegung für eHealth	gemSpec_KT
TIP1-A_6719	Prüfung von Authentizität und Integrität der gSMC-KT	gemSpec_KT
A_17090-01	eHealth-Kartenterminals: Signaturverfahren beim initialen Pairing zwischen Konnektor und eHealth-Kartenterminal (ECC-Migration)	gemSpec_Krypt

A_17183	CA-Zertifikate der relevanten TSP speichern (ECC-Migration)	gemSpec_Krypt
A_22451	ClientHello ohne akzeptable Cipher-Suite	gemSpec_Krypt
A_22453	ServerHello, Cipher-Suite	gemSpec_Krypt
A_22454	CertificateRequest	gemSpec_Krypt
A_22455	ClientCertificate	gemSpec_Krypt
GS-A_4359-02	X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	gemSpec_Krypt
GS-A_4361-02	X.509-Identitäten für die Erstellung und Prüfung digitaler Signaturen	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	gemSpec_Krypt
GS-A_5524	TLS-Renegotiation eHealth-KT	gemSpec_Krypt
GS-A_3700	Versionierung von Produkten auf Basis von dezentralen Produkttypen der TI-Plattform durch die Produktidentifikation	gemSpec_OM
GS-A_3702	Inhalt der Selbstauskunft von Produkten außer Karten	gemSpec_OM
A_24810	Performance - eHealth-CardLink - Bearbeitungszeit unter Last	gemSpec_Perf
A_24811	Performance - eHealth-CardLink - Robustheit gegenüber Lastspitzen	gemSpec_Perf
A_24769	eHealth-CardLink - Schnittstelle Konnektor - eHealth-CardLink	gemSpec_eHealth-CardLink
A_25159	eHealth-CardLink - Card Communication Interface, Websocket-Verbindungen	gemSpec_eHealth-CardLink
A_25160	eHealth-CardLink - Card Communication Interface, API-Dokumentation	gemSpec_eHealth-CardLink
A_25161	eHealth-CardLink - SICCT „Slot-Ereignis - Karte eingesteckt“ an Konnektor senden	gemSpec_eHealth-CardLink
A_25162	eHealth-CardLink - Command APDU INTERNAL AUTHENTICATE an nutzendes System weiterleiten	gemSpec_eHealth-CardLink

A_25163	eHealth-CardLink - Webschnittstelle, Fehlerfälle bei registerEgk	gemSpec_eHealth-CardLink
A_25182	eHealth-CardLink - Ausschließliche Anbindung von Karten des Typs eGK	gemSpec_eHealth-CardLink
A_25185	eHealth-CardLink - Response APDU INTERNAL AUTHENTICATE an Konnektor weiterleiten	gemSpec_eHealth-CardLink
A_25189	eHealth-CardLink - correlationId zur Korrelation von Command- und Response-APDU	gemSpec_eHealth-CardLink

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Festlegungen an den technischen Teil des Produkttyps verzeichnet, deren durchgeführte bzw. geplante Umsetzung und Beachtung der Hersteller bzw. der Anbieter durch eine Herstellererklärung bestätigt bzw. zugesagt.

Tabelle 4: Festlegungen zur funktionalen Eignung "Herstellererklärung"

ID	Bezeichnung	Quelle (Referenz)
A_15593	Ersatz bei defekten dezentralen Produkten	gemKPT_Test
A_15594	Vorhalten testbereiter dezentraler Komponenten	gemKPT_Test
A_20065	Nutzung der Dokumententemplates der gematik	gemKPT_Test
GS-A_2162	Kryptographisches Material in Entwicklungs- und Testumgebungen	gemKPT_Test
TIP1-A_2775	Performance in RU	gemKPT_Test
TIP1-A_4191	Keine Echtdateien in RU und TU	gemKPT_Test
TIP1-A_5052	Dauerhafte Verfügbarkeit in der RU	gemKPT_Test
TIP1-A_6079	Updates von Referenzobjekten	gemKPT_Test
TIP1-A_6080	Softwarestand von Referenzobjekten	gemKPT_Test
TIP1-A_6081	Bereitstellung der Referenzobjekte	gemKPT_Test
TIP1-A_6082-01	Versionen der Referenzobjekte	gemKPT_Test
TIP1-A_6086	Unterstützung bei Anbindung eines Produktes	gemKPT_Test
TIP1-A_6087	Zugang zur Adminschnittstelle bei dezentralen Produkten	gemKPT_Test
TIP1-A_6088	Unterstützung bei Fehlernachstellung	gemKPT_Test
TIP1-A_6093	Ausprägung der Referenzobjekte	gemKPT_Test

TIP1-A_6517-01	Eigenverantwortlicher Test: TBI	gemKPT_Test
TIP1-A_6518	Eigenverantwortlicher Test: TDI	gemKPT_Test
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6523	Zulassungstest: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6524-01	Testdokumentation gemäß Vorlagen	gemKPT_Test
TIP1-A_6526-01	Produkttypen: Bereitstellung	gemKPT_Test
TIP1-A_6527	Testkarten	gemKPT_Test
TIP1-A_6529	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	gemKPT_Test
TIP1-A_6532	Zulassung eines neuen Produkts: Aufgaben der TDI	gemKPT_Test
TIP1-A_6533	Zulassung eines neuen Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1-A_6536	Zulassung eines geänderten Produkts: Aufgaben der TDI	gemKPT_Test
TIP1-A_6537	Zulassung eines geänderten Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1-A_6538	Durchführung von Produkttests	gemKPT_Test
TIP1-A_6539	Durchführung von Produktübergreifenden Tests	gemKPT_Test
TIP1-A_6772	Partnerprodukte bei Interoperabilitätstests	gemKPT_Test
TIP1-A_7333	Parallelbetrieb von Release oder Produkttypversion	gemKPT_Test
TIP1-A_7334	Risikoabschätzung bezüglich der Interoperabilität	gemKPT_Test
TIP1-A_7335	Bereitstellung der Testdokumentation	gemKPT_Test
A_20956	Codierung des SICCT-Terminalnamens	gemSpec_KT
TIP1-A_3005	Zufallszahlen und Einmalschlüsseln	gemSpec_KT
TIP1-A_3039	Quelle für Zufallszahlen Zufallszahlengenerator des SM-KT	gemSpec_KT
TIP1-A_3049	Löschung Pairing-Blöcke	gemSpec_KT
TIP1-A_3050	Löschung öffentliche Schlüssel	gemSpec_KT
TIP1-A_6482	Anzahl CA-Zertifikate	gemSpec_KT

TIP1-A_6720	Verwendung zugelassener Gerätekarten gSMC-KT	gemSpec_KT
TIP1-A_7016	Prüfung der personalisierten gSMC-KT	gemSpec_KT
A_17183	CA-Zertifikate der relevanten TSP speichern (ECC-Migration)	gemSpec_Krypt
A_17207	Signaturen binärer Daten (ECC-Migration)	gemSpec_Krypt
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	gemSpec_Krypt
GS-A_5542	TLS-Verbindungen (fatal Alert bei Abbrüchen)	gemSpec_Krypt
GS-A_4009	Übertragungstechnologie auf OSI-Schicht LAN	gemSpec_Net
GS-A_4831	Standards für IPv4	gemSpec_Net
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_3697	Anlass der Erhöhung von Versionsnummern	gemSpec_OM
GS-A_3813	Datenschutzvorgaben Fehlermeldungen	gemSpec_OM
GS-A_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS-A_5039-01	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM
GS-A_5040-01	Änderung der Produktversion bei Produktänderungen außerhalb von Produkttypänderungen	gemSpec_OM

3.2 Festlegungen zur sicherheitstechnischen Eignung

3.2.1 CC-Evaluierung

Eine Zertifizierung nach Common Criteria [CC] ist nicht erforderlich.

Tabelle 5: Festlegungen zur sicherheitstechnischen Eignung "CC-Evaluierung"

ID	Bezeichnung	Quelle (Referenz)
	Es liegen keine Festlegungen vor	

3.2.2 Zertifizierung nach Technischer Richtlinie

Eine Zertifizierung nach Technischer Richtlinie ist nicht erforderlich.

Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Zertifizierung nach Technischer Richtlinie"

ID	Bezeichnung	Quelle (Referenz)
	Es liegen keine Festlegungen vor	

3.2.3 Produktgutachten

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

Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Produktgutachten"

ID	Bezeichnung	Quelle (Referenz)
GS-A_4330	Einbringung des Komponentenzertifikats	gemRL_TSL_SP_CP
A_22889	K_Hersteller-KT, Liste zulässiger CA-Zertifikate	gemSpec_KT
TIP1-A_2983	Übertragung medizinischer und personenbezogener Daten	gemSpec_KT
TIP1-A_2984	Anzeige medizinischer und personenbezogener Daten	gemSpec_KT
TIP1-A_3047	Zugriff auf Shared Secrets	gemSpec_KT
TIP1-A_3070	Ressourcen und unterschiedliche Kontexte	gemSpec_KT
TIP1-A_3094	Aktualisierung von CA-Zertifikaten der Komponenten-PKI	gemSpec_KT
TIP1-A_3239	Persistente Speicherung im Kartenterminal	gemSpec_KT
TIP1-A_3255	CA-Zertifikate der relevanten TSP speichern	gemSpec_KT
TIP1-A_3256	CA-Zertifikate in Kartenterminal und anschließende Speicherung	gemSpec_KT
TIP1-A_3257	Schutz CA-Zertifikate	gemSpec_KT
TIP1-A_3941	Update von TSP-Zertifikaten	gemSpec_KT
A_17090-01	eHealth-Kartenterminals: Signaturverfahren beim initialen Pairing zwischen Konnektor und eHealth-Kartenterminal (ECC-Migration)	gemSpec_Krypt
A_17207	Signaturen binärer Daten (ECC-Migration)	gemSpec_Krypt
A_18464	TLS-Verbindungen, nicht Version 1.1	gemSpec_Krypt
A_18467	TLS-Verbindungen, Version 1.3	gemSpec_Krypt

A_21275-01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	gemSpec_Krypt
A_24779-01	TI-Gateway-Zugangsmodule und eHealth-CardLink - TLS-Cipher-Suiten	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_5207	Signaturverfahren beim initialen Pairing zwischen Konnektor und eHealth-Kartenterminal	gemSpec_Krypt
GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	gemSpec_Krypt
A_24593	eHealth-CardLink - Keine PIN-Verifikation	gemSpec_eHealth-CardLink
A_24594	eHealth-CardLink - Keine Card-to-Card-Freischaltung	gemSpec_eHealth-CardLink
A_24595	eHealth-CardLink - Kryptographisch geschützte Anbindung des Clients des Nutzers	gemSpec_eHealth-CardLink
A_24596	eHealth-CardLink - Erkennung und Abwehr von Angriffen über den TLS-Kanal	gemSpec_eHealth-CardLink
A_24601	eHealth-CardLink - EV-TLS-Zertifikat	gemSpec_eHealth-CardLink
A_24602	eHealth-CardLink - OCSP-Stapling	gemSpec_eHealth-CardLink
A_24606	eHealth-CardLink - Sichere Speicherung der Pairing-Geheimnisse	gemSpec_eHealth-CardLink
A_24855	eHealth-CardLink - Geschützte Speicherung kritischer persistenter Daten	gemSpec_eHealth-CardLink
A_24929	eHealth-CardLink - Anwendungsfall VSDM - Prüfung ICCSN	gemSpec_eHealth-CardLink
A_25182	eHealth-CardLink - Ausschließliche Anbindung von Karten des Typs eGK	gemSpec_eHealth-CardLink
A_25193	eHealth-CardLink - Abgleich Ablaufdatum C.CH.AUT und C.eGK.AUT_CVC	gemSpec_eHealth-CardLink
A_25199	eHealth-CardLink - Keine Speicherung von Versicherten- und eGK-Daten	gemSpec_eHealth-CardLink

3.2.4 Sicherheitsgutachten

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

Tabelle 8: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

ID	Bezeichnung	Quelle (Referenz)
	Es liegen keine Festlegungen vor	

3.2.5 Herstellererklärung sicherheitstechnische Eignung

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

Tabelle 9: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_3004	Kennwort und Klartextanzeige	gemSpec_KT
TIP1-A_3043	Speicherung Shared Secret	gemSpec_KT
TIP1-A_3051	Löschen von Pairing-Informationen	gemSpec_KT
TIP1-A_3064	Kontext der verwalteten Chipkarten	gemSpec_KT
TIP1-A_3113	Zustand EHEALTH EXPECT CHALLENGE RESPONSE, Abbruch durch anderes Kommando	gemSpec_KT
TIP1-A_3114	Zustand EHEALTH EXPECT CHALLENGE RESPONSE, Einnehmen des Zustands	gemSpec_KT
TIP1-A_3180	Zugriff auf DF.KT	gemSpec_KT
TIP1-A_3181	Priorisierung DF.KT Zugriff	gemSpec_KT
TIP1-A_3258	Beendigung SICCT-spezifische TLS-Verbindung, resetten der Karten	gemSpec_KT
TIP1-A_3259	Beendigung SICCT-spezifische TLS-Verbindung, Verlust der Sicherheitszustände	gemSpec_KT
TIP1-A_3412	Nähere Beschreibung Rolle Administrator	gemSpec_KT
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	gemSpec_Krypt

3.3 Festlegungen zur elektrischen, mechanischen und physikalischen Eignung

Der Produkttyp erfordert den Nachweis der elektrischen, mechanischen und physikalischen Eignung. Sofern dabei spezifische Festlegungen der gematik zu beachten sind, werden diese nachfolgend aufgeführt. Der Nachweis erfolgt durch die Vorlage des Prüfberichts.

Tabelle 10: Festlegungen zur elektrischen, mechanischen und physikalischen Eignung

ID	Bezeichnung	Quelle (Referenz)
	Es liegen keine Festlegungen vor	

4 Produktypspezifische Merkmale

Es liegen keine optionalen Ausprägungen des Produktyps vor.

5 Anhang - Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
ID	Identifikation
CC	Common Criteria

5.2 Tabellenverzeichnis

Tabelle 1: Dokumente mit normativen Festlegungen.....	6
Tabelle 2: Mitgeltende Dokumente und Web-Inhalte.....	6
Tabelle 3: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test".....	8
Tabelle 4: Festlegungen zur funktionalen Eignung "Herstellererklärung".....	12
Tabelle 5: Festlegungen zur sicherheitstechnischen Eignung "CC-Evaluierung".....	14
Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Zertifizierung nach Technischer Richtlinie".....	15
Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Produktgutachten".....	15
Tabelle 8: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten".....	17
Tabelle 9: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung".....	17
Tabelle 10: Festlegungen zur elektrischen, mechanischen und physikalischen Eignung. .	18