gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

eHealth-Kartenterminal

Produkttyp Version:	1.2.1-3
Produkttyp Status:	freigegeben

Version:	1.0.1
Revision:	61038
Stand:	07.11.2018
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemProdT_KT_PTV_1.2.1-3

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.

Produkttyp-version	Beschreibung der Änderung	Referenz
1.0.0	Initiale Version auf Dokumentenebene	[gemProdT_KT_PTV1.0.0]
1.1.0	Losübergreifende Synchronisation	[gemProdT_KT_PTV1.1.0]
1.2.0	P11-Änderungsliste	[gemProdT_KT_PTV1.2.0]
1.2.0-1	Anpassung auf Releasestand 1.6.3	[gemProdT_KT_PTV1.2.0-1]
1.2.1-0	Anpassung auf Releasestand 1.6.4	[gemProdT_KT_PTV1.2.1-0]
1.2.1-1	Errata 1.6.4-2	[gemProdT_KT_PTV1.2.1-1]
1.2.1-2	Anpassung an Releasestand 2.1.2	[gemProdT_KT_PTV1.2.1-2]
1.2.1-3	Anpassung an Releasestand 2.1.3	[gemProdT_KT_PTV1.2.1-3]

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	26.10.18		freigegeben	gematik
1.0.1	07.11.18		redaktionelle Anpassung (Afos aus gemSpec_Net ergänzt)	gematik

Inhaltsverzeichnis

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an Herstellung und Betrieb von Produkten des Produkttyps eHealth-Kartenterminal oder verweist auf Dokumente, in denen verbindliche Anforderungen mit ggf. anderer Notation zu finden sind. Die Anforderungen 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 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 eHealth-Kartenterminal-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 Anforderungen, 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 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 wieder, 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 alle für den Produkttyp normativen Anforderungen.

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion

Dokumentenkürzel	Bezeichnung des Dokumentes	Version
gemSpec_PINPUK_TI	Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur	1.3.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.5.0
gemRL_TSL_SP_CP	Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL	2.2.0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.10.0
gemSpec_CVC_TSP	Spezifikation Trust Service Provider CVC	1.10.0
gemKPT_Test	Testkonzept der TI	2.1.0
gemSpec_Net	Übergreifende Spezifikation Netzwerk	1.14.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.11.0
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller	1.0.0
gemSpec_KSR	Spezifikation Konfigurationsdienst	2.2.0
gemSpec_KT	Spezifikation eHealth-Kartenterminal	3.9.0

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 für den Produkttypen normativen Anforderungen, die für die Herstellung und den Betrieb von Produkten des Produkttyps notwendig sind (Blattanforderungen). Die Anforderungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der Zulassung, Zertifizierung bzw. Bestätigung.

3.1 Anforderungen zur funktionalen Eignung

3.1.1 Produkttest/Produktübergreifender Test

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

Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1−A_2948	Definition SICCT/eHealth	gemSpec_KT
TIP1−A_2950	Mindestanforderung Display des eHealth-Kartenterminals	gemSpec_KT
TIP1−A_2951	eHealth-Kartenterminal: Eingabeeinheit	gemSpec_KT
TIP1−A_2952	eHealth-Kartenterminal: weitere Sensoren	gemSpec_KT
TIP1−A_2957	Behandlung Bedienungsfehler und ungültige Eingaben	gemSpec_KT
TIP1−A_2958	Sichtbarkeit MAC-Adresse des eHealth-Kartenterminals	gemSpec_KT
TIP1−A_2959	Lokale Terminalfunktion zur Anzeige der MAC-Adresse	gemSpec_KT
TIP1−A_2960	Unabhängigkeit Netzwerkanschluss bei lokaler Terminalfunktion zur Anzeige der MAC-Adresse	gemSpec_KT
TIP1−A_2961	Authentifizierung und MAC-Adressenabfrage	gemSpec_KT
TIP1−A_2962	Spezifizierung gematik-Prüfzeichen	gemSpec_KT
TIP1−A_2963	Prüfzeichen und inverse Form	gemSpec_KT
TIP1−A_2964	Anbringung gematik-Prüfzeichen	gemSpec_KT
TIP1−A_2966	eHealth-Kartenterminal und direkte Managementschnittstelle	gemSpec_KT
TIP1−A_2967	Aktivierung weiterer Managementschnittstellen	gemSpec_KT

TIP1−A_2968	Aktivieren und Deaktivieren von weiteren Managementschnittstellen	gemSpec_KT
TIP1−A_2969	Administration des eHealth-Kartenterminal	gemSpec_KT
TIP1−A_2970	Weitere Managementschnittstellen	gemSpec_KT
TIP1−A_2971	Über LAN-Netzwerk administrieren	gemSpec_KT
TIP1−A_2972	Anzeige Kartenzugriffe	gemSpec_KT
TIP1−A_2973	Anzeige Zugriffe	gemSpec_KT
TIP1−A_2979	Aktivierung und Erkennbarkeit sicherer PIN-Modus	gemSpec_KT
TIP1−A_2980	Managementschnittstellen zur Administrierung	gemSpec_KT
TIP1−A_2981	Rolle Administrator	gemSpec_KT
TIP1−A_2982	Rolle Benutzer und Administration	gemSpec_KT
TIP1−A_2983	Übertragung medizinischer und personenbezogener Daten	gemSpec_KT
TIP1−A_2984	Anzeige medizinischer und personenbezogener Daten	gemSpec_KT
TIP1−A_2985	Schlüsselmaterial des SM-KT	gemSpec_KT
TIP1−A_2986	Kein SM-KT vorhanden	gemSpec_KT
TIP1−A_2987	Aktivierung direkte Managementschnittstelle	gemSpec_KT
TIP1−A_2988	Administratorkennwort eingegeben an der direkten Managementschnittstelle	gemSpec_KT
TIP1−A_2989	Separates Setzen der Kennwörter	gemSpec_KT
TIP1−A_2990	Fehlerzähler bei falscher Kennworteingabe	gemSpec_KT
TIP1−A_2991	Fehlerzähler: Veränderung über Schnittstelle	gemSpec_KT
TIP1−A_2992	Fehlerzähler: Abfrage	gemSpec_KT
TIP1−A_2994	Sperrzeiten für direkte Managementschnittstelle bei Falscheingabe	gemSpec_KT
TIP1−A_2995	Fehlerzähler: spannungsloser Zustand	gemSpec_KT
TIP1−A_2996	Fehlerzähler: Speicherung verstrichener Sperrzeit im spannungslosem Zustand	gemSpec_KT
TIP1−A_2997	Fehlerzähler: Neustart Sperrzeit nach spannungslosem Zustand	gemSpec_KT
TIP1−A_2998	Sperrung weiterer Managementschnittstellen bei Falscheingabe	gemSpec_KT
TIP1−A_2999	Sperrung weiterer Managementschnittstellen für alle Benutzer bei Falscheingabe	gemSpec_KT

TIP1−A_3000	Mindestanforderungen Kennwort	gemSpec_KT
TIP1−A_3001	Zeichen für Kennwort	gemSpec_KT
TIP1−A_3002	Beschränkung für Kennwortauswahl	gemSpec_KT
TIP1−A_3003	Kennwörter und programmierbare Funktionstasten	gemSpec_KT
TIP1−A_3004	Kennwort und Klartextanzeige	gemSpec_KT
TIP1−A_3005	Zufallszahlen und Einmalschlüsseln	gemSpec_KT
TIP1−A_3006	Mindestanzahl Pairing-Block	gemSpec_KT
TIP1−A_3007	Empfohlene Anzahl Pairing-Blöcke	gemSpec_KT
TIP1−A_3012	Streichung "SICCT SELECT CT MODE"	gemSpec_KT
TIP1−A_3013	Einschränkungen CMD DO	gemSpec_KT
TIP1−A_3034	Display eines eHealth-Kartenterminals	gemSpec_KT
TIP1−A_3038	Vertrauenswürdiger Zustand	gemSpec_KT
TIP1−A_3039	Quelle für Zufallszahlen Zufallszahlengenerator des SM-KT	gemSpec_KT
TIP1−A_3040	Erzeugung von Zufallszahlen ohne vorhandenes SM-KT	gemSpec_KT
TIP1−A_3043	Speicherung Shared Secret	gemSpec_KT
TIP1−A_3044	Erstellung des Authentifizierungstokens	gemSpec_KT
TIP1−A_3045	Pairing-Information	gemSpec_KT
TIP1−A_3046	Pairing-Block	gemSpec_KT
TIP1−A_3048	Shared Secrets und Klartextanzeige	gemSpec_KT
TIP1−A_3049	Löschung Pairing-Blöcke	gemSpec_KT
TIP1−A_3050	Löschung öffentliche Schlüssel	gemSpec_KT
TIP1−A_3051	Löschen von Pairing-Informationen	gemSpec_KT
TIP1−A_3052	Funktionsfähigkeit der Karte bei Notentnahme	gemSpec_KT
TIP1−A_3053	Beschriftung/Bedruckung bei Notentnahme	gemSpec_KT
TIP1−A_3054	Hilfsmittel Notentnahme	gemSpec_KT
TIP1−A_3055	Bauform eHealth-Kartenterminal	gemSpec_KT
TIP1−A_3056	Notentnahme bei Stromausfall	gemSpec_KT
TIP1−A_3057	Benutzerdokumentation für Notentnahme	gemSpec_KT

TIP1−A_3058	Unterstützung kontaktbehaftete Chipkarten	gemSpec_KT
TIP1−A_3059	eHealth-Kartenterminal und Kontaktiereinheiten	gemSpec_KT
TIP1−A_3061	Format Kontaktiereinheiten	gemSpec_KT
TIP1−A_3062	Kommunikationsverhalten des Kartenterminals	gemSpec_KT
TIP1−A_3064	Kontext der verwalteten Chipkarten	gemSpec_KT
TIP1−A_3065	Verbindungsabbruch	gemSpec_KT
TIP1−A_3066	Mehrere Verbindungen zu ansteuernden Hosts	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_3071	Übergang Nutzungsrecht für Ressourcen	gemSpec_KT
TIP1−A_3072	Verbindung zum Kartenterminal aufgebaut, Ablehnung Konnektorverbindung	gemSpec_KT
TIP1−A_3073	Verbindung zum Kartenterminal aufgebaut, Abbruch Konnektorverbindung	gemSpec_KT
TIP1−A_3074	Verbindung zum eHealth-Kartenterminal aufbauen, Zurücksetzten gesteckter Karten	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_3079	SICCT OUTPUT und SICCT INPUT Displaynachricht	gemSpec_KT
TIP1−A_3080	SICCT OUTPUT und SICCT INPUT mindestens 48 Zeichen	gemSpec_KT
TIP1−A_3081	SICCT REQUEST ICC und SICCT EJECT ICC Displaynachricht	gemSpec_KT
TIP1−A_3082	SICCT REQUEST ICC und SICCT EJECT ICC mindestens 48 Zeichen	gemSpec_KT
TIP1−A_3083	SICCT PERFORM VERIFICATION: Parameter Displaynachricht und PIN-Prompt	gemSpec_KT
TIP1−A_3084	Displaynachrichten mittels SICCT PERFORM VERIFICATION	gemSpec_KT
TIP1−A_3085	Anzeige von PIN-Prompts mittels SICCT PERFORM VERIFICATION	gemSpec_KT
TIP1−A_3086	SICCT PERFORM VERIFICATION Kommando, Eingabe des 1. Zeichens	gemSpec_KT

TIP1−A_3087	SICCT PERFORM VERIFICATION Kommando, Eingabe der weiteren Zeichen	gemSpec_KT
TIP1−A_3088	SICCT MODIFY VERIFICATION DATA Kommando, Eingabe des 1. Zeichens	gemSpec_KT
TIP1−A_3089	SICCT MODIFY VERIFICATION DATA Kommando, Eingabe der weiteren Zeichen	gemSpec_KT
TIP1−A_3090	PIN mit variabler oder fixer Länge	gemSpec_KT
TIP1−A_3091	PIN-Länge Kartenterminal bekannt	gemSpec_KT
TIP1−A_3095	Aufbau des SICCT-spezifischen TLS-Kanals bei nicht-gültigem Konnektorzertifikat	gemSpec_KT
TIP1−A_3096	Aufbau des SICCT-spezifischen TLS-Kanals, erlaubte Kommandos bei gültigem Konnektorzertifikat ohne Pairing	gemSpec_KT
TIP1−A_3097	Aufbau des SICCT-spezifischen TLS-Kanals, erlaubte Kommandos bei gültigem Konnektorzertifikat mit Pairing	gemSpec_KT
TIP1−A_3098	Aufbau des SICCT-spezifischen TLS-Kanals, zusätzlich erlaubtes Kommando bei gültigem Konnektorzertifikat ohne Pairing	gemSpec_KT
TIP1−A_3099	Auslieferungszustand Kennwörter	gemSpec_KT
TIP1−A_3100	Auslieferungszustand Pairing-Information	gemSpec_KT
TIP1−A_3101	Auslieferungszustand Managementschnittstelle	gemSpec_KT
TIP1−A_3102	Auslieferungszustand Direktkennwort	gemSpec_KT
TIP1−A_3103	Erstmaliges Setzen des Direktkennworts	gemSpec_KT
TIP1−A_3104	Definition Werksreset	gemSpec_KT
TIP1−A_3105	Mindestgröße gematik Prüfzeichen	gemSpec_KT
TIP1−A_3106	Benutzerführung und integriertes Display	gemSpec_KT
TIP1−A_3107	Optische Gestaltung des Prüfzeichens	gemSpec_KT
TIP1−A_3109	EPS-Datei „gematik Prüfzeichen“	gemSpec_KT
TIP1−A_3110	Gleichzeitige Kommunikation zu unterschiedlichen Karten	gemSpec_KT
TIP1−A_3111	Transiente bzw. überbrückbare Fehlerzustände bei der Kartenkommunikation	gemSpec_KT
TIP1−A_3112	Entnahme des SM-KT	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_3115	Zustand EHEALTH EXPECT CHALLENGE RESPONSE, Timeout	gemSpec_KT
TIP1−A_3116	SICCT-Modus und EHEALTH EXPECT CHALLENGE RESPONSE	gemSpec_KT
TIP1−A_3117	Protokollfehler spezifikationskonform behandeln	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	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_3129	TLS-Verbindungsaufbau: notwendiges kryptographisches Material	gemSpec_KT
TIP1−A_3131	Ergänzung der SICCT-Spezifikation	gemSpec_KT
TIP1−A_3132	Anzahl der während der PIN-Eingabe anzeigbaren Zeichen	gemSpec_KT
TIP1−A_3133	PIN-Länge mindestens 12 Zeichen ermöglichen	gemSpec_KT
TIP1−A_3134	Während der PIN-Eingabe	gemSpec_KT
TIP1−A_3135	Anzahl eingegebene Zeichen	gemSpec_KT
TIP1−A_3136	Aufbau des SICCT-spezifischen TLS-Kanals, erlaubte Kommandos bei ungültigem Konnektorzertifikat	gemSpec_KT
TIP1−A_3137	„Liste ausführbarer Kommandos ohne gültiges Konnektorzertifikat“	gemSpec_KT
TIP1−A_3144	SICCT-Terminalname	gemSpec_KT
TIP1−A_3145	Anzeige des SICCT-Terminalnamens	gemSpec_KT
TIP1−A_3146	Abfrage SICCT-Terminalnamen	gemSpec_KT

TIP1−A_3147	Übertragungsparameter PPS1	gemSpec_KT
TIP1−A_3148	TA1 Byte	gemSpec_KT
TIP1−A_3149	PPS-Verfahren und Wert ‚97'	gemSpec_KT
TIP1−A_3150	Zusammenarbeit mit einer Karte die im TA1 Byte des ATR der Wert ‚97' zurückliefert	gemSpec_KT
TIP1−A_3151	UNICast basierte Dienstanfragepakete	gemSpec_KT
TIP1−A_3152	KT: Update-Komponente innerhalb des LAN	gemSpec_KT
TIP1−A_3153	Update-Varianten für eHealth-Kartenterminals	gemSpec_KT
TIP1−A_3154	Authentisierung für weiteren Werksreset-Mechanismus	gemSpec_KT
TIP1−A_3158	TSP-Update-Mechanismus	gemSpec_KT
TIP1−A_3159	TSP-Update-Mechanismus für KT ohne Firmware-Update	gemSpec_KT
TIP1−A_3160	Mehrwertmodule auf KT	gemSpec_KT
TIP1−A_3161	Mehrwertmodule KT de-/aktivierbar	gemSpec_KT
TIP1−A_3162	Erkennbarkeit, ob Mehrwertmodul aktiv ist	gemSpec_KT
TIP1−A_3170	Ausführen eines zulässigen Downgrades	gemSpec_KT
TIP1−A_3177	Ausführung des Kommandos EHEALTH TERMINAL AUTHENTICATE	gemSpec_KT
TIP1−A_3180	Zugriff auf DF.KT	gemSpec_KT
TIP1−A_3181	Priorisierung DF.KT Zugriff	gemSpec_KT
TIP1−A_3184	KT-Unterstützung des anonymen Zugriffs für Rolle CT CONTROL	gemSpec_KT
TIP1−A_3188	Erhaltung Konfigurationen nach Update	gemSpec_KT
TIP1−A_3189	Unterstützung IPv4	gemSpec_KT
TIP1−A_3191	Definition anonyme Session	gemSpec_KT
TIP1−A_3192	Anforderungen an Slotsiegel	gemSpec_KT
TIP1−A_3227	Umsetzung der KT-Identität	gemSpec_KT
TIP1−A_3231	TLS-Verbindung: einseitige Authentisierung	gemSpec_KT
TIP1−A_3232	Sicherung administrativer TLS-Verbindung	gemSpec_KT
TIP1−A_3233	Einseitige Authentisierung während des Aufbaus der administrativen TLS-Verbindung	gemSpec_KT
TIP1−A_3236	Kennworteingabe bei der Aktivierung einer weiteren	gemSpec_KT

	Managementschnittstelle	
TIP1−A_3241	Abweichung von [gemSpec_Krypt#2.2]	gemSpec_KT
TIP1−A_3242	Nicht SICCT-spezifische TLS-Verbindungen und [gemSpec_Krypt#2.2]	gemSpec_KT
TIP1−A_3243	Initiales Pairing	gemSpec_KT
TIP1−A_3244	Außerbetriebnahme eines eHealth-Kartenterminals	gemSpec_KT
TIP1−A_3245	Keine Veränderung bei fehlerhafter oder nicht authentischer Übertragung	gemSpec_KT
TIP1−A_3246	Port der netzwerkbasierten Managementschnittstellen	gemSpec_KT
TIP1−A_3247	Statusmeldung der Chipkarte	gemSpec_KT
TIP1−A_3248	Notentnahme vor Ort	gemSpec_KT
TIP1−A_3249	Zugriff auf die Plug-In-Karte	gemSpec_KT
TIP1−A_3250	Deadlock während Kartenkommunikation	gemSpec_KT
TIP1−A_3251	„CONTROL COMMAND“-Kommando	gemSpec_KT
TIP1−A_3253	Kommunikation gemäß SICCT-Protokoll	gemSpec_KT
TIP1−A_3255	CA-Zertifikate der relevanten TSP speichern	gemSpec_KT
TIP1−A_3258	Beendigung SICCT-spezifische TLS-Verbindung, resetten der Karten	gemSpec_KT
TIP1−A_3260	Netzwerkbasierten Managementschnittstellen	gemSpec_KT
TIP1−A_3263	Dokumentation der Konfiguration	gemSpec_KT
TIP1−A_3264	Return Code Control Command	gemSpec_KT
TIP1−A_3265	Ergänzung Sicherheitsprotokolle	gemSpec_KT
TIP1−A_3266	Kartenkommandos ablehnen bei nicht vorhandenem Pairing	gemSpec_KT
TIP1−A_3412	Nähere Beschreibung Rolle Administrator	gemSpec_KT
TIP1−A_3413	Prüfung Authentizität und Integrität bei Inbetriebnahme	gemSpec_KT
TIP1−A_3415	Sicherung der Netzwerkkommunikation	gemSpec_KT
TIP1−A_3417	Möglichkeit zum Werksreset	gemSpec_KT
TIP1−A_3418	Werksreset nicht dauerhaft unausführbar	gemSpec_KT
TIP1−A_3420	Weiterer Mechanismus für Werksreset	gemSpec_KT
TIP1−A_3421	PUK-Verfahren	gemSpec_KT

TIP1−A_3422	PUK-Eingabe bei Inbetriebnahme	gemSpec_KT
TIP1−A_3423	Fehlerzähler PUK	gemSpec_KT
TIP1−A_3424	Werksreset Administrator	gemSpec_KT
TIP1−A_3425	Dokumentation Werksreset Mechanismus	gemSpec_KT
TIP1−A_3926	Karten-Kompatibilität	gemSpec_KT
TIP1−A_3934	Ermittlung Zertifikatsrolle	gemSpec_KT
TIP1−A_3935	Vergleich Zertifikatsrolle	gemSpec_KT
TIP1−A_3938	Darstellung Selbstauskunft	gemSpec_KT
TIP1−A_3939	Darstellung Firmware-Gruppen-Version	gemSpec_KT
TIP1−A_3940	Zertifikat prüfen	gemSpec_KT
TIP1−A_3947	Dokumentation Einbringung Serverzertifikat	gemSpec_KT
TIP1−A_3948	CTM Festlegung für eHealth	gemSpec_KT
TIP1−A_5083	Anforderungen PUK	gemSpec_KT
TIP1−A_5424	Ausführung eines Werksreset ohne Authentisierung	gemSpec_KT
TIP1−A_5425	Aktivierung/Deaktivierung des Werksreset ohne Authentisierung	gemSpec_KT
TIP1−A_5426	Standardeinstellung Werksreset ohne Authentisierung	gemSpec_KT
TIP1−A_5656	Unterstützung Auto-IP-Protokoll optional	gemSpec_KT
TIP1−A_6483	SICCT MODIFY VERIFICATION DATA Displaynachricht und PIN-Prompt	gemSpec_KT
TIP1−A_6541	Benutzerfreundlichkeit und weitere Kennwort-/PIN-Eingaben	gemSpec_KT
TIP1−A_6718	Bezugsquellen gSMC-KT	gemSpec_KT
TIP1−A_6719	Prüfung von Authentizität und Integrität der gSMC-KT	gemSpec_KT
GS−A_4359	X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	gemSpec_Krypt
GS−A_4361	X.509-Identitäten für die Erstellung und Prüfung digitaler Signaturen	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_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_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
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
GS-A_4865	Versionierte Liste zulässiger Firmware-Versionen	gemSpec_OM
GS-A_4867	Übernahme Firmware-Gruppe	gemSpec_OM
GS-A_4868	Aufsteigende Nummerierung der Firmware-Gruppen	gemSpec_OM
GS-A_4869	Firmware-Gruppe mindestens eine Firmware-Version	gemSpec_OM
GS-A_4870	Wechsel zu jeder Firmware-Version der aktuellen Firmware-Gruppe	gemSpec_OM
GS-A_4871	Upgrade nur auf höhere Firmware-Gruppen-Version	gemSpec_OM
GS-A_4872	Kein Downgrade der Firmware-Gruppe	gemSpec_OM
GS-A_4941	Betriebsdokumentation der dezentralen Produkte der TI-Plattform	gemSpec_OM
GS-A_5034	Inhalte der Betriebsdokumentation der dezentralen Produkte der TI-Plattform	gemSpec_OM
GS-A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM
GS-A_4154	Performance – Kartenterminal – Bearbeitungszeit	gemSpec_Perf
GS-A_5329	eHealth-KT Performance – TLS-Handshake I	gemSpec_Perf
GS-A_5330	eHealth-KT Performance – TLS-Handshake II	gemSpec_Perf

3.1.2 Herstellererklärung funktionale Eignung

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

Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)

A_15593	Ersatz bei defekten dezentralen Produkten	gemKPT_Test
A_15594	Vorhalten testbereiter dezentraler Komponenten	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 Echtdaten 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	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	Eigenverantwortlicher Test: TBV	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	Testdokumentation gemäß Vorlagen	gemKPT_Test
TIP1-A_6526	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
TIP1−A_7358	Qualität des Produktmusters	gemKPT_Test
TIP1−A_3314	Inhalt Update-Paket – Hersteller-Update-Informationen	gemSpec_KSR
TIP1−A_3315	Inhalt Update-Paket – DokumentationFiles	gemSpec_KSR
TIP1−A_3316	Firmware-Gruppenkonzept Informationen für den Konfigurationsdienst	gemSpec_KSR
TIP1−A_3317	Firmware-Gruppenkonzept – Lieferung mit Firmware	gemSpec_KSR
TIP1−A_3897	Keine Signatur der Update-Informationen durch Kartenterminalhersteller	gemSpec_KSR
TIP1−A_5158	Inhalt Update-Paket – Kartenterminal FirmwareFiles	gemSpec_KSR
TIP1−A_5159	Inhalt Update-Paket – Firmware-Gruppen-Information	gemSpec_KSR
TIP1−A_6108	FirmwareGroupInfo.xml Signatur	gemSpec_KSR
TIP1−A_6112	Name des Update-Paketes	gemSpec_KSR
TIP1−A_6113	Definition Update-Paket-Struktur	gemSpec_KSR
TIP1−A_6114	Passwort des Update-Paketes	gemSpec_KSR
TIP1−A_6115	Größe des Update-Paketes	gemSpec_KSR
TIP1−A_6116	Update-Paket - Dateinamen und Unterverzeichnisse	gemSpec_KSR
TIP1−A_6117	Referenzierungen des Update-Paketes	gemSpec_KSR
TIP1−A_6118	Zusätzliche Dateien im Update-Paket	gemSpec_KSR
TIP1−A_6120	Update-Paket – Dateinamen der UpdateInformation Detached-Signatur	gemSpec_KSR
TIP1−A_6121	Update-Paket – Dateinamen der FirmwareGroupInfo Detached-Signatur	gemSpec_KSR
TIP1−A_6122	Pfadreferenz	gemSpec_KSR
TIP1−A_6123	Update-Paket – Signatur	gemSpec_KSR
TIP1−A_6124	Bereitstellung KSR Update-Paket Zertifikat	gemSpec_KSR
TIP1−A_6131	FirmwareGroupInfo.xml und UpdateInfo.xml - Format	gemSpec_KSR

TIP1−A_6132	Detached-Signature der FirmwareGroupInfo.xml	gemSpec_KSR
TIP1−A_6133	FirmwareGroupInfo.xml - Element „FirmwareGroupSignature“	gemSpec_KSR
TIP1−A_3190	Unterstützung IPv6	gemSpec_KT
TIP1−A_6481	Firmwarelieferung via P_KSRS_Upload Schnittstelle	gemSpec_KT
TIP1−A_6482	Anzahl CA-Zertifikate	gemSpec_KT
TIP1−A_6717	gSMC-KT Verantwortung durch den Hersteller	gemSpec_KT
TIP1−A_6720	Verwendung zugelassener Gerätekarten gSMC-KT	gemSpec_KT
TIP1−A_7016	Prüfung der personalisierten gSMC-KT	gemSpec_KT
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_3696	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM
GS−A_3697	Anlass der Erhöhung von Versionsnummern	gemSpec_OM
GS−A_3813	Datenschutzvorgaben Fehlermeldungen	gemSpec_OM
GS−A_4541	Nutzung der Produkttypversion zur Kompatibilitätsprüfung	gemSpec_OM
GS−A_4875	Einschränkung der Firmware-Gruppe bei Verlust Zulassung	gemSpec_OM
GS−A_4876	Einschränkung der Firmware-Gruppe bei Verlust SigG-Bestätigung oder CC-Sicherheitszertifikat	gemSpec_OM
GS−A_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS−A_5039	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 CC-Evaluierung

Der Produkttyp erfordert eine Zertifizierung nach Common Criteria [CC] auf der Grundlage des Protection Profiles.

Für die Evaluierung sind die Inhalte der Schutzprofile normativ führend. Der Nachweis der im Folgenden aufgeführten Anforderungen erfolgt implizit durch die Vorlage des IT-Sicherheitszertifikats bei der gematik.

Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "CC-Evaluierung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4330	Einbringung des Komponentenzertifikats	gemRL_TSL_SP_CP
TIP1-A_2965	Sichere Updatemöglichkeit KT-Firmware	gemSpec_KT
TIP1-A_2966	eHealth-Kartenterminal und direkte Managementschnittstelle	gemSpec_KT
TIP1-A_2967	Aktivierung weiterer Managementschnittstellen	gemSpec_KT
TIP1-A_2968	Aktivieren und Deaktivieren von weiteren Managementschnittstellen	gemSpec_KT
TIP1-A_2969	Administration des eHealth-Kartenterminal	gemSpec_KT
TIP1-A_2970	Weitere Managementschnittstellen	gemSpec_KT
TIP1-A_2971	Über LAN-Netzwerk administrieren	gemSpec_KT
TIP1-A_2976	Prüfung Integrität/Authentizität einer neuen Firmware	gemSpec_KT
TIP1-A_2977	Fehlerhafte oder nicht authentische Übertragung abweisen	gemSpec_KT
TIP1-A_2978	Übernahme als aktive Firmware	gemSpec_KT
TIP1-A_2980	Managementschnittstellen zur Administrierung	gemSpec_KT
TIP1-A_2981	Rolle Administrator	gemSpec_KT
TIP1-A_2982	Rolle Benutzer und Administration	gemSpec_KT
TIP1-A_2983	Übertragung medizinischer und personenbezogener Daten	gemSpec_KT
TIP1-A_2984	Anzeige medizinischer und personenbezogener Daten	gemSpec_KT
TIP1-A_2985	Schlüsselmaterial des SM-KT	gemSpec_KT
TIP1-A_2986	Kein SM-KT vorhanden	gemSpec_KT
TIP1-A_2987	Aktivierung direkte Managementschnittstelle	gemSpec_KT
TIP1-A_2990	Fehlerzähler bei falscher Kennworteingabe	gemSpec_KT
TIP1-A_2991	Fehlerzähler: Veränderung über Schnittstelle	gemSpec_KT
TIP1-A_2993	Geschütze Speicherung der Kennwörter	gemSpec_KT
TIP1-A_2994	Sperrzeiten für direkte Managementschnittstelle bei Falscheingabe	gemSpec_KT
TIP1-A_2995	Fehlerzähler: spannungsloser Zustand	gemSpec_KT
TIP1-A_2997	Fehlerzähler: Neustart Sperrzeit nach spannungslosem Zustand	gemSpec_KT

TIP1−A_3000	Mindestanforderungen Kennwort	gemSpec_KT
TIP1−A_3002	Beschränkung für Kennwortauswahl	gemSpec_KT
TIP1−A_3003	Kennwörter und programmierbare Funktionstasten	gemSpec_KT
TIP1−A_3004	Kennwort und Klartextanzeige	gemSpec_KT
TIP1−A_3005	Zufallszahlen und Einmalschlüsseln	gemSpec_KT
TIP1−A_3036	Mehrwertmodule: keine Störungen der eHealth-Anwendungen	gemSpec_KT
TIP1−A_3039	Quelle für Zufallszahlen Zufallszahlengenerator des SM-KT	gemSpec_KT
TIP1−A_3040	Erzeugung von Zufallszahlen ohne vorhandenes SM-KT	gemSpec_KT
TIP1−A_3041	Zufallszahlengenerator geringerer Güte	gemSpec_KT
TIP1−A_3043	Speicherung Shared Secret	gemSpec_KT
TIP1−A_3044	Erstellung des Authentifizierungstokens	gemSpec_KT
TIP1−A_3047	Zugriff auf Shared Secrets	gemSpec_KT
TIP1−A_3048	Shared Secrets und Klartextanzeige	gemSpec_KT
TIP1−A_3049	Löschung Pairing-Blöcke	gemSpec_KT
TIP1−A_3050	Löschung öffentliche Schlüssel	gemSpec_KT
TIP1−A_3051	Löschen von Pairing-Informationen	gemSpec_KT
TIP1−A_3064	Kontext der verwalteten Chipkarten	gemSpec_KT
TIP1−A_3065	Verbindungsabbruch	gemSpec_KT
TIP1−A_3069	Verbindungen und eHealth-Kartenterminal	gemSpec_KT
TIP1−A_3070	Ressourcen und unterschiedliche Kontexte	gemSpec_KT
TIP1−A_3071	Übergang Nutzungsrecht für Ressourcen	gemSpec_KT
TIP1−A_3072	Verbindung zum Kartenterminal aufgebaut, Ablehnung Konnektorverbindung	gemSpec_KT
TIP1−A_3073	Verbindung zum Kartenterminal aufgebaut, Abbruch Konnektorverbindung	gemSpec_KT
TIP1−A_3074	Verbindung zum eHealth-Kartenterminal aufbauen, Zurücksetzten gesteckter Karten	gemSpec_KT
TIP1−A_3092	Aktualisierung der Kartenterminal-Firmware	gemSpec_KT
TIP1−A_3093	Neu einzuspielende Firmware-Version	gemSpec_KT
TIP1−A_3094	Aktualisierung von CA-Zertifikaten der Komponenten-PKI	gemSpec_KT

TIP1−A_3095	Aufbau des SICCT-spezifischen TLS-Kanals bei nicht-gültigem Konnektorzertifikat	gemSpec_KT
TIP1−A_3096	Aufbau des SICCT-spezifischen TLS-Kanals, erlaubte Kommandos bei gültigem Konnektorzertifikat ohne Pairing	gemSpec_KT
TIP1−A_3097	Aufbau des SICCT-spezifischen TLS-Kanals, erlaubte Kommandos bei gültigem Konnektorzertifikat mit Pairing	gemSpec_KT
TIP1−A_3098	Aufbau des SICCT-spezifischen TLS-Kanals, zusätzlich erlaubtes Kommando bei gültigem Konnektorzertifikat ohne Pairing	gemSpec_KT
TIP1−A_3099	Auslieferungszustand Kennwörter	gemSpec_KT
TIP1−A_3100	Auslieferungszustand Pairing-Information	gemSpec_KT
TIP1−A_3101	Auslieferungszustand Managementschnittstelle	gemSpec_KT
TIP1−A_3102	Auslieferungszustand Direktkennwort	gemSpec_KT
TIP1−A_3103	Erstmaliges Setzen des Direktkennworts	gemSpec_KT
TIP1−A_3104	Definition Werksreset	gemSpec_KT
TIP1−A_3108	Prüfung der einzuspielenden Firmware-Version	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_3125	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_3129	TLS-Verbindungsaufbau: notwendiges kryptographisches Material	gemSpec_KT
TIP1−A_3136	Aufbau des SICCT-spezifischen TLS-Kanals, erlaubte Kommandos bei ungültigem Konnektorzertifikat	gemSpec_KT
TIP1−A_3137	„Liste ausführbarer Kommandos ohne gültiges Konnektorzertifikat“	gemSpec_KT
TIP1−A_3153	Update-Varianten für eHealth-Kartenterminals	gemSpec_KT
TIP1−A_3154	Authentisierung für weiteren Werksreset-Mechanismus	gemSpec_KT
TIP1−A_3158	TSP-Update-Mechanismus	gemSpec_KT
TIP1−A_3159	TSP-Update-Mechanismus für KT ohne Firmware-Update	gemSpec_KT

TIP1−A_3170	Ausführen eines zulässigen Downgrades	gemSpec_KT
TIP1−A_3180	Zugriff auf DF.KT	gemSpec_KT
TIP1−A_3181	Priorisierung DF.KT Zugriff	gemSpec_KT
TIP1−A_3182	Erkennung von Übertragungsfehlern und nicht authentischen Übertragungen während eines Firmware-Updates	gemSpec_KT
TIP1−A_3183	selbständige Übertragungsfehlererkennung bei KT-Firmware-Updates	gemSpec_KT
TIP1−A_3185	Ablage des Sicherheitsankers in einem schreibgeschützten Bereich des KT	gemSpec_KT
TIP1−A_3227	Umsetzung der KT-Identität	gemSpec_KT
TIP1−A_3229	Schutz vor Auslesen des Shared Secrets	gemSpec_KT
TIP1−A_3231	TLS-Verbindung: einseitige Authentisierung	gemSpec_KT
TIP1−A_3232	Sicherung administrativer TLS-Verbindung	gemSpec_KT
TIP1−A_3233	Einseitige Authentisierung während des Aufbaus der administrativen TLS-Verbindung	gemSpec_KT
TIP1−A_3234	Private Schlüssel zur Sicherung des administrativen TLS-Kanals	gemSpec_KT
TIP1−A_3235	Öffentliche Schlüssel und Zertifikate zur Sicherung des administrativen TLS-Kanals	gemSpec_KT
TIP1−A_3239	Persistente Speicherung im Kartenterminal	gemSpec_KT
TIP1−A_3241	Abweichung von [gemSpec_Krypt#2.2]	gemSpec_KT
TIP1−A_3242	Nicht SICCT-spezifische TLS-Verbindungen und [gemSpec_Krypt#2.2]	gemSpec_KT
TIP1−A_3245	Keine Veränderung bei fehlerhafter oder nicht authentischer Übertragung	gemSpec_KT
TIP1−A_3253	Kommunikation gemäß SICCT-Protokoll	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_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_3260	Netzwerkbasierten Managementschnittstellen	gemSpec_KT
TIP1−A_3261	alleinige KT-Kontrolle über Anzeigemechanismus Diensttypaktivität	gemSpec_KT
TIP1−A_3262	SM-KT-Identität für Mehrwertmodule nutzbar	gemSpec_KT
TIP1−A_3266	Kartenkommandos ablehnen bei nicht vorhandenem Pairing	gemSpec_KT
TIP1−A_3412	Nähere Beschreibung Rolle Administrator	gemSpec_KT
TIP1−A_3413	Prüfung Authentizität und Integrität bei Inbetriebnahme	gemSpec_KT
TIP1−A_3415	Sicherung der Netzwerkkommunikation	gemSpec_KT
TIP1−A_3416	Prüfung Stellen des Kennwortes	gemSpec_KT
TIP1−A_3417	Möglichkeit zum Werksreset	gemSpec_KT
TIP1−A_3420	Weiterer Mechanismus für Werksreset	gemSpec_KT
TIP1−A_3421	PUK-Verfahren	gemSpec_KT
TIP1−A_3422	PUK-Eingabe bei Inbetriebnahme	gemSpec_KT
TIP1−A_3423	Fehlerzähler PUK	gemSpec_KT
TIP1−A_3424	Werksreset Administrator	gemSpec_KT
TIP1−A_3933	Mathematische Prüfung Zertifikat	gemSpec_KT
TIP1−A_3934	Ermittlung Zertifikatsrolle	gemSpec_KT
TIP1−A_3935	Vergleich Zertifikatsrolle	gemSpec_KT
TIP1−A_3936	Durchsuchen CA-Zertifikate	gemSpec_KT
TIP1−A_3937	Einbringen CA-Zertifikate	gemSpec_KT
TIP1−A_3940	Zertifikat prüfen	gemSpec_KT
TIP1−A_3941	Update von TSP-Zertifikaten	gemSpec_KT
TIP1−A_4115	Sicherstellung CA Berechtigung	gemSpec_KT
TIP1−A_5083	Anforderungen PUK	gemSpec_KT
TIP1−A_5424	Ausführung eines Werksreset ohne Authentisierung	gemSpec_KT
TIP1−A_5425	Aktivierung/Deaktivierung des Werksreset ohne Authentisierung	gemSpec_KT
TIP1−A_5426	Standardeinstellung Werksreset ohne Authentisierung	gemSpec_KT
GS−A_4359	X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	gemSpec_Krypt

GS-A_4361	X.509-Identitäten für die Erstellung und Prüfung digitaler Signaturen	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	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_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
GS-A_5524	TLS-Renegotiation eHealth-KT	gemSpec_Krypt
GS-A_4865	Versionierte Liste zulässiger Firmware-Versionen	gemSpec_OM
GS-A_4866	Integritäts- und Authentizitätsschutz der Firmware-Versionsinformationen	gemSpec_OM
GS-A_4867	Übernahme Firmware-Gruppe	gemSpec_OM
GS-A_4868	Aufsteigende Nummerierung der Firmware-Gruppen	gemSpec_OM
GS-A_4869	Firmware-Gruppe mindestens eine Firmware-Version	gemSpec_OM
GS-A_4870	Wechsel zu jeder Firmware-Version der aktuellen Firmware-Gruppe	gemSpec_OM
GS-A_4871	Upgrade nur auf höhere Firmware-Gruppen-Version	gemSpec_OM
GS-A_4872	Kein Downgrade der Firmware-Gruppe	gemSpec_OM
GS-A_4873	Speicherung der Firmware-Gruppe	gemSpec_OM
GS-A_4874	Firmware-Gruppen-Updates nur über herstellereigenen Update-Mechanismus	gemSpec_OM
GS-A_4941	Betriebsdokumentation der dezentralen Produkte der TI-Plattform	gemSpec_OM

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.

Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" spezifisch für die Herausgabe der gSMC-KT

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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 Chipkarte	gemSpec_CVC_TSP
TIP1-A_2583	Zuordnung des privaten Schlüssels zu Identitäten	gemSpec_CVC_TSP
TIP1-A_2584	Schlüsselpaare und CV-Zertifikate	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_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_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_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_5551	Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR	gemSpec_DS_Anbieter
GS-A_5557	Security Monitoring	gemSpec_DS_Anbieter
GS-A_5558	Aktive Schwachstellenscans	gemSpec_DS_Anbieter
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_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_5386	kartenindividuelle geheime und private Schlüssel G2-Karten	gemSpec_Krypt
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

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)
GS-A_2330-02	Hersteller: Schwachstellen-Management	gemSpec_DS_Hersteller
GS-A_2350-01	Produktunterstützung der Hersteller	gemSpec_DS_Hersteller
GS-A_2354-01	Produktunterstützung mit geeigneten Sicherheitstechnologien	gemSpec_DS_Hersteller
GS-A_2524-01	Produktunterstützung: Nutzung des Problem-Management-Prozesses	gemSpec_DS_Hersteller
GS-A_2525-01	Hersteller: Schließen von Schwachstellen	gemSpec_DS_Hersteller
GS-A_4944-01	Produktentwicklung: Behebung von Sicherheitsmängeln	gemSpec_DS_Hersteller
GS-A_4945-01	Produktentwicklung: Qualitätssicherung	gemSpec_DS_Hersteller
GS-A_4946-01	Produktentwicklung: sichere Programmierung	gemSpec_DS_Hersteller

GS-A_4947-01	Produktentwicklung: Schutz der Vertraulichkeit und Integrität	gemSpec_DS_Hersteller
TIP1-A_3318	Firmware-Gruppenkonzept – Lieferung ohne Firmware	gemSpec_KSR
TIP1-A_3322	Firmware-Gruppenkonzept – Integritäts- und Authentizitätsschutz	gemSpec_KSR
TIP1-A_3908	Firmware-Gruppenkonzept – Streichung Firmware	gemSpec_KSR
TIP1-A_6119	Update-Paket – Übertragung „Firmware-Gruppen-Information“	gemSpec_KSR
TIP1-A_3192	Anforderungen an Slotsiegel	gemSpec_KT

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
TIP1-A_2581	Evaluierung von HSMs	gemSpec_CVC_TSP
GS-A_2355-01	Meldung von erheblichen Schwachstellen und Bedrohungen	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_4526-01	Aufbewahrungsvorgaben an die Nachweise zu Sicherheitsmeldungen	gemSpec_DS_Anbieter
GS-A_4530-01	Maßnahmen zur Behebung von erheblichen Sicherheitsvorfällen und Notfällen	gemSpec_DS_Anbieter
GS-A_4532-01	Nachweis der Umsetzung von Maßnahmen in Folge eines erheblichen Sicherheitsvorfalls oder Notfalls	gemSpec_DS_Anbieter
GS-A_5017-01	Meldung und Behandlung von Schwachstellen	gemSpec_DS_Anbieter
GS-A_5324-01	Teilnahme des Anbieters an Sitzungen des kISMS	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_5559	Bereitstellung Ergebnisse von Schwachstellenscans	gemSpec_DS_Anbieter
GS-A_5560	Entgegennahme und Prüfung von Meldungen der gematik	gemSpec_DS_Anbieter

GS-A_5561	Bereitstellung 24/7-Kontaktpunkt	gemSpec_DS_Anbieter
GS-A_5562	Bereitstellung Produktinformationen	gemSpec_DS_Anbieter
GS-A_5563	Jahressicherheitsbericht	gemSpec_DS_Anbieter
GS-A_5624	Auditrechte der gematik zur Informationssicherheit	gemSpec_DS_Anbieter
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_5021	Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung	gemSpec_Krypt
GS-A_4963	Deaktivierung von Chipkarten nach Gültigkeitsende	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

3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

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

Tabelle 8: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_2953	Zuverlässigkeitsprognose eHealth-Kartenterminals	gemSpec_KT
TIP1-A_2954	Zuverlässigkeitsprognose eHealth-Kartenterminal	gemSpec_KT
TIP1-A_2955	Dauerhafte Stromversorgung der im eHealth-Kartenterminal gesteckten Chipkarte(n)	gemSpec_KT
TIP1-A_2956	Kurzzeitig höherer Strombedarf von Chipkarten (Spike)	gemSpec_KT

TIP1−A_2962	Spezifizierung gematik-Prüfzeichen	gemSpec_KT
TIP1−A_3008	Unterstützung Kartenkontakte	gemSpec_KT
TIP1−A_3009	Elektrischer Anschluss Kartenkontakte	gemSpec_KT
TIP1−A_3010	„Card-In“-Schalter	gemSpec_KT
TIP1−A_3011	Anpressdruck der Kontakte	gemSpec_KT
TIP1−A_3035	Zuverlässigkeit des eHealth-Kartenterminals im Betrieb	gemSpec_KT
TIP1−A_3062	Kommunikationsverhalten des Kartenterminals	gemSpec_KT
TIP1−A_3063	Synchrone und asynchrone Übertragungsprotokolle	gemSpec_KT
TIP1−A_3130	Kartenkontakte und Umschalten in andere Betriebsmodi	gemSpec_KT
TIP1−A_3138	Kartenkontakte und Umschalten Betriebsmodi	gemSpec_KT
TIP1−A_3147	Übertragungsparameter PPS1	gemSpec_KT
TIP1−A_3148	TA1 Byte	gemSpec_KT
TIP1−A_3149	PPS-Verfahren und Wert ‚97’	gemSpec_KT
TIP1−A_3150	Zusammenarbeit mit einer Karte die im TA1 Byte des ATR der Wert ‚97’ zurückliefert	gemSpec_KT
TIP1−A_3927	Kontaktschonende Kontaktiereinheiten	gemSpec_KT
TIP1−A_3929	Landende Kontakte	gemSpec_KT
TIP1−A_3930	Physikalische Sicherheit-Klima	gemSpec_KT
TIP1−A_3932	Physikalische Sicherheit-Vibration	gemSpec_KT
TIP1−A_3942	Belastbarkeit des Netzteils	gemSpec_KT
TIP1−A_3944	Einführung oder Entnahme der Chipkarte	gemSpec_KT

4 Produkttypspezifische Merkmale

4.1 Optionale Ausprägungen

Es liegen die folgenden optionalen Ausprägungen des Produkttyps vor.

Im Rahmen der Zulassung muss der Hersteller verbindlich erklären, welche der gelisteten Optionen sein eHealth-Kartenterminal umsetzt. Im Rahmen der Zulassung muss die Erfüllung der zu diesen Optionen gehörenden Anforderungen nachgewiesen werden.

In diesem Kapitel erfolgt lediglich die inhaltliche Zuordnung der bereits in Kapitel 3 gelisteten Anforderungen zu den Optionen.

4.1.1 Umsetzung des Werksreset ohne Authentisierung

Die Anforderungen in Tab_Afos_WerksresetOhneAuth gelten nur für ein eHealth-Kartenterminal, das den Werksreset ohne Authentisierung gemäß [TIP1-A_5424] umsetzt.

Tabelle 9: Tab_Afos_WerksresetOhneAuth - Anforderung an das eHealth-Kartenterminal bei Umsetzung des Werksreset ohne Authentisierung

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_5424	Ausführung eines Werksreset ohne Authentisierung	gemSpec_KT
TIP1-A_5425	Aktivierung/Deaktivierung des Werksreset ohne Authentisierung	gemSpec_KT
TIP1-A_5426	Standardeinstellung Werksreset ohne Authentisierung	gemSpec_KT

4.2 Kompatibilitätsanforderungen an Kartenversionen

Die durch den Produkttyp eHealth-Kartenterminal zu unterstützenden Kartenversionen werden in der Dokumentenlandkarte zum aktuellen Release festgelegt.

4.3 Festlegung EHEALTH Schnittstellenversion (VER)

In „Tabelle 9: Tab_VER - EHEALTH Schnittstellenversion (VER)“ erfolgt für den Produkttyp eHealth-Kartenterminal in der Version 1.2.1-0 die Festlegung der EHEALTH Schnittstellenversion (VER).

Tabelle 10: Tab_VER - EHEALTH Schnittstellenversion (VER)

Parameter	Wert

EHEALTH Schnittstellenversion (VER)	1.0.0

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

5.2 Tabellenverzeichnis

5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[CC]	Internationaler Standard: Common Criteria for Information Technology Security Evaluation https://www.commoncriteriaportal.org/cc/

[gemRL_PruefSichEig]	gematik: Richtlinie zur Prüfung der Sicherheitseignung