Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

HBA

Produkttyp Version:	4.6.1-1
Produkttyp Status:	freigegeben
Version:	1.0.0
Revision:	380716
Stand:	01.07.2021
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemProdT_HBA_G2_1_PTV_4.6.1-1

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
2.0.0	Initiale Version G2-Karten für Vergabeverfahren	[gemProdT_HBA_PTV2.0.0]
2.0.1	Anpassung Produkttypversion auf Stand ORS1 vom 22.04.13	[gemProdT_HBA_PTV2.0.1]
2.0.2	Anpassung an G2 Iteration 1 und Iteration 2a	[gemProdT_HBA_PTV2.0.2]
4.0.1	Anpassung an G2 Iteration 2b	[gemProdT_HBA_PTV4.0.1]
4.1.0	Anpassung an G2 Iteration 3 und Releasestand 1.3.0	[gemProdT_HBA_PTV4.1.0]
4.2.0	Anpassung an G2 Iteration 4 und Releasestand 1.4.0	[gemProdT_HBA_PTV4.2.0]
4.2.1	Anpassung Produkttypversion auf Stand OPB1 vom 25.04.16	[gemProdT_HBA_PTV4.2.1]
4.2.1-1	Anpassung an Releasestand 1.6.3	[gemProdT_HBA_PTV4.2.1-1]
4.3.0-0	Kartengeneration 2.1	[gemProdT_HBA_PTV4.3.0-0]
4.4.0-0	Anpassung an Releasestand 2.1.2	[gemProdT_HBA_PTV4.4.0-0]
4.5.0-0	Anpassung an Releasestand 2.1.3	[gemProdT_HBA_PTV4.5.0-0]
4.5.1-0	Anpassung an Releasestand 3.0.0	[gemProdT_HBA_PTV4.5.1-0]
4.6.0-0	Anpassung an Releasestand 3.1.0	[gemProdT_HBA_PTV4.6.0-0]
4.6.1-0	Anpassung an Releasestand 4.0.0 Hotfix 1	[gemProdT_HBA_PTV4.6.1-0]
4.6.1-1	Anpassung an Releasestand Smartcards_Maintenance_21.1	[gemProdT_HBA_PTV4.6.1-1]

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	01.07.21		freigegeben	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 HBA 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 HBA-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. gemPTV_ATV_Festlegungen, 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_gematikHBA_Opt	Spezifikation Optische Gestaltung des von der gematik herausgegebenen HBA	2.0.0
gemRL_TSL_SP_CP	Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL	2.~~6~~9.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.1~~7~~9.~~0~~1
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.14.0
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.~~9~~10.~~0~~2
gemSpec_eGK_Opt	Spezifikation der elektronischen Gesundheitskarte – Äußere Gestaltung	3.10.0
gemSpec_CAN_TI	Übergreifende Spezifikation CAN-Policy	1.0.0
gemSpec_CVC_TSP	Spezifikation Trust Service Provider CVC	1.1~~3~~4.0
gemSpec_Karten_Fach_TIP_G2_1	Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	3.0.0
gemKPT_Test	Testkonzept der TI	2.~~7~~8.0
gemSpec_HBA_ObjSys_G2_1	Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem	5.~~0~~1.0
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	1.~~2~~3.0
gemSpec_PINPUK_TI	Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur	1.3.0

Tabelle 2: Mitgeltende Dokumente

Dokumentenkürzel	Bezeichnung des Dokuments	Version
BAEK_HBA_Opt	BÄK: Handbuch zur optischen Gestaltung des eArztausweises	2.4.0
BAEK_HBA_Holo	BÄK: Anforderungen an Kartenkörper und Hologramm des eArztausweises	2.3.4

BAEK_TelematikID	Identity Management Konzept der eArztausweise und Telematik-ID	2.3.1
BAEK_HBA_Opt_Vorlagen	BÄK: Dateivorlagen zu BÄK_HBA_Opt	
BPtK_HBA_Opt	BPtK: Handbuch zur optischen Gestaltung des elektronischen Heilberufsausweises für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Stand vom 29.06.2015	
BPtK_TelematikID	BPtK: Spezifikation Telematik-ID	1.1
BZÄK_HBA_Opt	BZÄK: Vorgaben an inhaltliche Gestaltung Antragsprozess, Layout und Zertifikate elektronischer Zahnarztausweis	1.2
BZÄK_HBA_Layout	Layout des elektronischen Zahnarztausweises	2.1
BZÄK_HBA_Opt_Vorlagen	BZÄK: Dateivorlagen zu BZÄK_HBA_Opt	
ABDA_HBA_Opt	ABDA: Handbuch für den Apothekerausweis / HBA Stand von Oktober 2018	

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 der gematik gegenüber nachzuweisen ist.

Die Anforderungen werden als Teil der Personalisierungsvalidierung anhand von Echtkarten geprüft.

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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5020	Einbringung des Komponentenzertifikats durch den Kartenherausgeber	gemRL_TSL_SP_CP
TIP1-A_2578	Korrekte ICCSN der Chipkarte	gemSpec_CVC_TSP
TIP1-A_2589	Personalisierung des CVC-CA-Zertifikats	gemSpec_CVC_TSP
Card-G2-A_2038	K_Personalisierung: Druck der CAN auf den HBA bei Verwendung der optionalen kontaktlosen Schnittstelle	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2040-01	K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2041	K_Personalisierung: Wert des Attributes iccsn8	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2043	K_Personalisierung und K_Initialisierung: ATR-Kodierung	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2044-01	K_Personalisierung und K_Initialisierung: TC1 Byte im ATR	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2045	K_Personalisierung und K_Initialisierung: Vorgaben für Historical Bytes	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2058-01	K_Personalisierung: Personalisiertes Attribut von EF.GDO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2673	K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile“	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2869	K_Personalisierung: Generierung der CAN bei Verwendung der optionalen kontaktlosen Schnittstelle des HBA	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3009	K_HBA: Zusatzanforderungen für kontaktlose Schnittstelle	gemSpec_HBA_ObjSys_G2.1

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3015	K_Personalisierung und K_Initialisierung: Historical Bytes im ATR	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3282	K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_HPC.CS.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3284	K_Personalisierung: Personalisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3285	K_Personalisierung: Personalisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3297	K_Personalisierung: Personalisierte Attribute von MF / SK.CAN	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3301-01	K_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3307-01	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3308-01	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3317-02	K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3318-02	K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3327-01	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3386	K_Personalisierung: Festlegung von CHR in MF / EF.C.HPC.AUTR_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3387	K_Personalisierung: Festlegung von CHR in MF / EF.C.HPC.AUTD_SUK_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3395	K_Personalisierung: personalisierter Wert von pointInTime	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3627	K_Personalisierung und K_Initialisierung: T0 Byte im ATR	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3630	K_Personalisierung: Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3632-01	K_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3640	K_Personalisierung: Personalisierte MF / DF.ESIGN / PrK.HP.AUT.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3642	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3644-01	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3646-01	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3848	K_Personalisierung und K_Initialisierung: Unterstützung Onboard-RSA-Schlüsselgenerierung	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3479	Kodierung von Versionskennungen	gemSpec_Karten_Fach_TIP

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_3480	Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP
Card-G2-A_3481	Ausschluss für die Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP
Card-G2-A_3487	K_Initialisierung und K_Personalisierung: DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3492	K_Personalisierung: DO_PT_Pers in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3494	K_Personalisierung: DO_PI_Kartenkörper in EF.ATR-Personalisierung	gemSpec_Karten_Fach_TIP
Card-G2-A_3495	K_Personalisierung: DO_PI_Personalisierung in EF.ATR-Personalisierung	gemSpec_Karten_Fach_TIP
Card-G2-A_3496	K_Initialisierung: Weitere Datenobjekte in DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3497	K_Personalisierung: Vollständige Befüllung von EF.ATR	gemSpec_Karten_Fach_TIP
Card-G2-A_3498	K_Personalisierung: DO_ICCSN in EF.GDO	gemSpec_Karten_Fach_TIP
Card-G2-A_3479	Kodierung von Versionskennungen	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3480	Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3481	Ausschluss für die Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3487	K_Initialisierung und K_Personalisierung: DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3492	K_Personalisierung: DO_PT_Pers in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3494	K_Personalisierung: DO_PI_Kartenkörper in EF.ATR-Personalisierung	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3495	K_Personalisierung: DO_PI_Personalisierung in EF.ATR-Personalisierung	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3496	K_Initialisierung: Weitere Datenobjekte in DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3497	K_Personalisierung: Vollständige Befüllung von EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3498	K_Personalisierung: DO_ICCSN in EF.GDO	gemSpec_Karten_Fach_TIP_G2.1
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_4559	Versionierung der Karten der TI	gemSpec_OM
GS-A_4560	Versionierung von Datenstrukturen der Karten der TI	gemSpec_OM
GS-A_5026	Versionierung von Karten durch die Produktidentifikation	gemSpec_OM
GS-A_5140	Inhalt der Selbstauskunft von Karten	gemSpec_OM
GS-A_4583	Berufsgruppenkennzeichen für HBA	gemSpec_PKI
GS-A_4587	Gesamtlänge der Telematik-ID	gemSpec_PKI

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4621	Zugriffsprofil von HBA und SM-B (SMC-B, HSM-B)	gemSpec_PKI
GS-A_4623	Zugriffsprofil eines HBA	gemSpec_PKI
GS-A_4710	Präfix der Telematik-ID	gemSpec_PKI
GS-A_4711	Separator der Telematik-ID	gemSpec_PKI
GS-A_4974	CV-Ausstattung von Smartcards der TI	gemSpec_PKI
~~Card-G2-A_3005~~	~~Absicherung der Kartenadministration~~	~~gemSpec_HBA_ObjSys~~

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 4: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_20065	Nutzung der Dokumententemplates der gematik	gemKPT_Test
GS-A_2162	Kryptographisches Material in Entwicklungs- und Testumgebungen	gemKPT_Test
TIP1-A_4191	Keine Echtdaten in RU und TU	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	Produkttypen: Bereitstellung	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_2575	Zugelassenes Zugriffsprofil im CV-Rollen-Zertifikat	gemSpec_CVC_TSP
A_21549	K_Personalisierung, Option_Personalisierung_Admin_Schlüssel:	gemSpec_HBA_ObjSys_G2.1

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_2676-01	K_Personalisierung: Wert von PIN.AUTO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2677	K_Personalisierung: Wert von PUK für PIN.AUTO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2678-01	K_Personalisierung: Wert von PIN.SO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2679	K_Personalisierung: Wert von PUK für PIN.SO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2680-02	K_Personalisierung: Inhalt von EF.C.HP.AUTO1.R3072	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2681-02	K_Personalisierung: Inhalt von EF.C.HP.AUTO2.R3072	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2682	K_Personalisierung: Unterbindung der Nutzung von DF.AUTO – PIN.AUTO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2856	K_Personalisierung: Unterbindung der Nutzung von DF.AUTO – PIN.SO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3010	K_Initialisierung und K_Personalisierung: Kontaktlose Schnittstelle wird nicht genutzt	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3277	K_Personalisierung und K_Initialisierung: Konformität kontaktlose Schnittstelle	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3286	K_Personalisierung: Personalisierte Attribute von MF / PIN.CH	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3288	K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3289	K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3290-01	K_Personalisierung, Option_Personalisierung_Admin_Schlüssel: MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3291-01	K_Personalisierung, Option_Personalisierung_Admin_Schlüssel: MF / SK.CMS.AES128	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3292-01	K_Personalisierung, Option_Personalisierung_Admin_Schlüssel: MF / SK.CMS.AES256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3294-01	K_Personalisierung, Option_Personalisierung_Admin_Schlüssel: MF / SK.CUP.AES128	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3296-01	K_Personalisierung, Option_Personalisierung_Admin_Schlüssel: MF / SK.CUP.AES256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3298	K_Personalisierung: Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3299	K_Personalisierung: Personalisierte Attribute von MF / DF.QES / PIN.QES	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3305	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048	gemSpec_HBA_ObjSys_G2.1

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card−G2−A_3306	K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048	gemSpec_HBA_ObjSys_G2.1
Card−G2−A_3314−01	K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072	gemSpec_HBA_ObjSys_G2.1
Card−G2−A_3315	K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PIN.AUTO	gemSpec_HBA_ObjSys_G2.1
Card−G2−A_3316	K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PIN.SO	gemSpec_HBA_ObjSys_G2.1
Card−G2−A_3325	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_HBA_ObjSys_G2.1
Card−G2−A_3523	K_Personalisierung: Schlüsselgenerierung auf der Karte	gemSpec_HBA_ObjSys_G2.1
GS−A_3696	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM
GS−A_3697	Anlass der Erhöhung von Versionsnummern	gemSpec_OM
GS−A_3700	Versionierung von Produkten auf Basis von dezentralen Produkttypen der TI-Plattform durch die Produktidentifikation	gemSpec_OM
GS−A_3813	Datenschutzvorgaben Fehlermeldungen	gemSpec_OM
GS−A_4542	Spezifikationsgrundlage für Produkte	gemSpec_OM
GS−A_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS−A_5039	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM
GS−A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM
~~Card−G2−A_3590~~	~~Symmetrische Kartenadministration~~	~~gemSpec_HBA_ObjSys~~
~~Card−G2−A_3292~~	~~K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256~~	~~gemSpec_HBA_ObjSys~~
~~Card−G2−A_3290~~	~~K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256~~	~~gemSpec_HBA_ObjSys~~
~~Card−G2−A_3291~~	~~K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128~~	~~gemSpec_HBA_ObjSys~~
~~Card−G2−A_3294~~	~~K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES128~~	~~gemSpec_HBA_ObjSys~~
~~Card−G2−A_3296~~	~~K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES256~~	~~gemSpec_HBA_ObjSys~~

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 CC-Evaluierung

Eine Zertifizierung nach Common Criteria [CC] ist nicht erforderlich

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.

Tabelle 5: 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 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_2585	Personalisierung von CV-Zertifikaten für einen HBA	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_2214-01	kDSM: Anbieter müssen jährlich die Auftragsverarbeiter kontrollieren	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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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_5626	kDSM: Auftragsverarbeitung	gemSpec_DS_Anbieter
GS−A_4384	TLS-Verbindungen	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_5338	HBA/SMC-B – Erzeugung asymmetrischer Schlüsselpaare auf der jeweiligen Karte selbst	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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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. Kartenpersonalisierer	gemSpec_PINPUK_TI
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
~~Card-G2-A_3591~~	~~Schlüsselspeicherung~~	~~gemSpec_HBA_ObjSys~~

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_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_4468-02	kDSM: Jährlicher Datenschutzbericht der TI	gemSpec_DS_Anbieter
GS-A_4473-01	kDSM: Unverzügliche Benachrichtigung bei Verstößen gemäß Art. 34 DSGVO	gemSpec_DS_Anbieter
GS-A_4478-01	kDSM: Nachweis der Umsetzung von Maßnahmen in Folge eines gravierenden Datenschutzverstoßes	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_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_5324-02	kDSM: Teilnahme des Anbieters an Sitzungen des kDSM	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_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_5566	kDSM: Sicherstellung der Datenschutzanforderungen in Unterbeauftragungsverhältnissen	gemSpec_DS_Anbieter
GS-A_5624	Auditrechte der gematik zur Informationssicherheit	gemSpec_DS_Anbieter

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5625	kDSM: Auditrechte der gematik zum Datenschutz	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_5021	Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung	gemSpec_Krypt
GS-A_4712	Definition und Eindeutigkeit der Telematik-ID	gemSpec_PKI
GS-A_4958	Neue Telematik-ID bei Folgekarten	gemSpec_PKI
GS-A_4961	Verwendung zugewiesener Berufs- und Rollenattribute	gemSpec_PKI
GS-A_4962	Verhalten bei Kartenverlust und Änderung persönlicher Daten	gemSpec_PKI
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
~~Card-G2-A_3594~~	~~Schlüsselspeicherung~~	~~gemSpec_HBA_ObjSys~~

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 7: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card-G2-A_2319	Abriebfestigkeit der Personalisierung	gemSpec_eGK_Opt
Card-G2-A_2320	Untersuchungsverfahren Abriebfestigkeit der Personalisierung	gemSpec_eGK_Opt
Card-G2-A_2321	Haltbarkeit des Layouts/Artworks	gemSpec_eGK_Opt
Card-G2-A_2322	Schweiß- und Speicheltest	gemSpec_eGK_Opt
Card-G2-A_2323	Vorgaben zum Test Beschreibbarkeit und Wischfestigkeit	gemSpec_eGK_Opt

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
Card−G2−A_2324	Test Beschreibbarkeit und Wischfestigkeit: Zeitpunkt	gemSpec_eGK_Opt
Card−G2−A_2325	Test Beschreibbarkeit und Wischfestigkeit: Ergebnis	gemSpec_eGK_Opt

4 Produkttypspezifische Merkmale

4.1 Angaben zu EF.Version2

Die detaillierte Versionskennzeichnung des HBA wird im Dokument [gemSpec_Karten_Fach_TIP] festgelegt.

4.2 Optionale Ausprägungen

In diesem Kapitel werden die optionalen Ausprägungen des Produkttyps HBA beschrieben Die Spezifikationen des COS und des HBA-Objektsystems lassen folgende Optionen zu:

- Bereitstellung einer USB-Schnittstelle gemäß [gemSpec_HBA_ObjSys#4.2.1]
- Bereitstellung einer kontaktlosen Schnittstelle gemäß [gemSpec_HBA_ObjSys#4.2.2]
- Bereitstellung der Funktion Kryptobox gemäß [gemSpec_HBA_ObjSys #4.2.3]
- Falls der HBA administriert werden soll (z.B. falls die Option „Kurzläuferzertifikate" für CV-Zertifikate genutzt werden soll) müssen bei der Personalisierung
  - entweder symmetrische Schlüssel für die Authentisierung mit einem CMS/CUpS gemäß [gemSpec_HBA_ObjSys#2]
  - oder asymmetrische Schlüssel für die Authentisierung mit einem CMS/CUpS [gemSpec_HBA_ObjSys#2]

  in die entsprechenden Objekte der Karte eingebracht werden.

Der HBA kann gemäß [gemSpec_HBA_ObjSys#2] als Testkarte ausgestaltet werden.

4.3 Variationen

4.3.1 Festlegung des Wertes für das Attribut „transportStatus" der PIN.AUTO und der PIN.SO des HBA

Gemäß Card-G2-A_2128 und Card-G2-A_2129 gibt es für den Produkttyp HBA zwei verschiedene Möglichkeiten, den Wert für das Attribut „transportStatus" der PIN.AUTO und der PIN.SO festzulegen: „Leer-PIN" oder „Transport-PIN". Der Wert "Transport-PIN" kann bei der Personalisierung in "regularPassword" mit der Zuordnung eines konkreten PIN-Wertes geändert werden. Beide PINs müssen mit demselben Wert für „transportStatus" belegt werden.

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