

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

HBA

Zulassungsobjekt HBA- Objektsystem

Produkttyp Version: 4.6.1-0
Produkttyp Status: freigegeben

Version: 1.1.0
Revision: 73549
Stand: 18.12.2018
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemProdT_HBA_ObjSys_G2_1_PTV_4.6.1-0

Historie Produkttypversion und Produkttypsteckbrief

Historie Produkttypversion

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

Produkttypversion	Beschreibung der Änderung	Referenz
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_ObjSys_PTV2.0.2]
4.0.0	Anpassung an G2 Iteration 2	[gemProdT_HBA_ObjSys_PTV4.0.0]
4.0.1	Anpassung an G2 Iteration 2b	[gemProdT_HBA_ObjSys_PTV4.0.1]
4.1.0	Anpassung an G2 Iteration 3	[gemProdT_HBA_ObjSys_PTV4.1.0]
4.2.0	Anpassung an G2 Iteration 4	[gemProdT_HBA_ObjSys_PTV4.2.0]
4.3.1	Einarbeitung der Errata R1.4.1 bis R1.4.7	[gemProdT_HBA_ObjSys_PTV4.3.1]
4.3.1-1	Anpassung auf Releasestand 1.6.3	[gemProdT_HBA_ObjSys_PTV4.3.1-1]
4.4.0-0	Kartengeneration 2.1	[gemProdT_HBA_ObjSys_PTV4.4.0-0]
4.4.1-0	Errata 1.6.4-2	[gemProdT_HBA_ObjSys_PTV4.4.1-0]
4.5.0-0	Anpassung an Releasestand	[gemProdT_HBA_ObjSys_PTV4.5.0-0]

	2.1.2	
4.6.0-0	Anpassung an Releasestand 2.1.3	[gemProdT_HBA_ObjSys_PTV4.6.0-0]
4.6.1-0	Anpassung an Releasestand 2.1.3-1	[gemProdT_HBA_ObjSys_PTV4.6.1-0]

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	28.11.18		freigegeben	gematik
1.1.0	18.12.18	2	Aktualisierung	gematik

Inhaltsverzeichnis

1	Einführung.....	5
1.1	Zielsetzung und Einordnung des Dokumentes	5
1.2	Zielgruppe	5
1.3	Geltungsbereich	5
1.4	Abgrenzung des Dokumentes	6
1.5	Methodik.....	6
2	Dokumente	7
3	Blattanforderungen	9
3.1	Anforderungen zur funktionalen Eignung	9
3.1.1	Produkttest/Produktübergreifender Test	9
3.1.2	Herstellereklärung funktionale Eignung	15
3.2	Anforderungen zur sicherheitstechnischen Eignung	17
3.2.1	Sicherheitstechnische Eignung: Zertifizierung nach Technischer Richtlinie 17	
3.2.2	Zertifizierung als Signaturerstellungseinheit.....	23
3.2.3	Herstellereklärung sicherheitstechnische Eignung.....	23
3.3	Anforderungen zur elektrischen, mechanischen und physikalischen Eignung.....	24
4	Umsetzungsanforderungen	26
5	Produkttypspezifische Merkmale	27
5.1	Angaben zu EF.Version2.....	27
5.2	Optionale Ausprägungen	27
5.3	Variationen	27
5.3.1	Festlegung des Wertes für das Attribut „transportStatus“ der PIN.AUTO und der PIN.SO des HBA	27
6	Anhang A – Verzeichnisse	28
6.1	Abkürzungen.....	28
6.2	Tabellenverzeichnis.....	28
6.3	Referenzierte Dokumente.....	28

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an Herstellung von Produkten des Zulassungsobjektes HBA-Objektsystem 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 für das Zulassungsobjekt HBA-Objektsystem richtet sich an HBA-Objektsystem-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 das Zulassungsobjekt HBA-Objektsystem 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 das Zulassungsobjekt HBA-Objektsystem normativen Anforderungen.

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion

Dokumenten Kürzel	Bezeichnung des Dokumentes	Version
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.12.0
gemSpec_Karten_Fach_TIP_G2_1	Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	3.0.0
gemSpec_eGK_Opt	Spezifikation der elektronischen Gesundheitskarte – Äußere Gestaltung	3.7.0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.11.0
gemKPT_Test	Testkonzept der TI	2.2.0
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller	1.0.0
gemSpec_HBA_ObjSys_G2_1	Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem	4.4.0
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.4.0

Tabelle 2: Mitgeltende Dokumente

Dokumenten Kürzel	Bezeichnung des Dokuments	Version
gemSpec_TK	Spezifikation für Testkarten gematik, (eGK, HBA, (g)SMC) der Generation 2	3.7.0
gemSpec_TLK_COS_G2	gematik: Spezifikation der Testlaborkarte COS / Objektsysteme	1.6.0
gemSpec_OID	gematik: Spezifikation Festlegung von OIDs	2.9.0
TR-03143	BSI: eHealth G2-COS Konsistenz-Prüf tool	1.0

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.

Dokumenten Kürzel	Bezeichnung des Dokuments	Version
gemErrata_R2.1.3-1	Errata zu Release 2.1.3-1	1.0.0

3 Blattanforderungen

Die folgenden Abschnitte verzeichnen alle für das Zulassungsobjekt HBA-Objektsystem normativen Anforderungen, die für die Herstellung des Zulassungsobjektes 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 Zulassungsobjektes HBA-Objektsystem verzeichnet, deren Umsetzung im Zuge von Zulassungstests durch die gematik geprüft wird.

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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_15220	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.R2048	gemSpec_HBA_ObjSys_G2.1
A_15222	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.E256	gemSpec_HBA_ObjSys_G2.1
A_15224	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.R2048	gemSpec_HBA_ObjSys_G2.1
A_15226	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2033-01	K_Initialisierung: Ordnerattribute	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2035	K_Initialisierung: Zugriffsregeln für besondere Kommandos	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2036	K_Initialisierung Anzahl logischer Kanäle	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2039	K_Initialisierung: Wert des Attributes root	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_2042-01	K_Initialisierung: Inhalt persistentPublicKeyList	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_2047	K_Initialisierung: Initialisierte Attribute von MF	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2048-01	K_Initialisierung: Initialisierte Attribute von MF / EF.ATR	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2055-01	K_Initialisierung: Initialisierte Attribute von MF / EF.DIR	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2057	K_Initialisierung: Initialisierte Attribute von MF / EF.GDO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2059-01	K_Initialisierung: Attribute von MF / EF.Version2	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2061	K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_HPC.CS.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2064	K_Initialisierung: Initialisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2067	K_Initialisierung: Initialisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2069	K_Initialisierung: Initialisierte Attribute von MF / PIN.CH	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2072	K_Initialisierung: Initialisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2075	K_Initialisierung: Initialisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2078-01	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2080-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2081-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2082	K_Initialisierung: Initialisierte Attribute von MF / DF.HPA	gemSpec_HBA_ObjSys_G2.1

Card-G2-A_2083	K_Initialisierung: Initialisierte Attribute von MF / DF.HPA / EF.HPD	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2084	K_Initialisierung: Initialisierte Attribute von MF / DF.QES	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2085-01	K_Initialisierung: Initialisierte Attribute von MF / DF.QES / PrK.HP.QES.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2088-01	K_Initialisierung: Initialisierte Attribute von MF / DF.QES / PIN.QES	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2089	K_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.SSEC	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2090-01	K_Initialisierung: Inhalt von EF.SSEC	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2091-01	K_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2097	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2098-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2101	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2107	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2110-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2117	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2118	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2119-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.CIA.CIAInfo	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2120-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.OD (Object Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2121-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.AOD (Authentication Object Directory)	gemSpec_HBA_ObjSys_G2.1

Card-G2-A_2122-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.PrKD (Private Key Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2123-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.CD(Certificate Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2124	K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2125-01	K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2128	K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / PIN.AUTO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2129	K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / PIN.SO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2130-01	K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2131-01	K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072	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_2867	K_HBA: Vorhandensein einer USB-Schnittstelle	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2868	K_Initialisierung: Initialisierte Attribute von MF / SK.CAN	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3006	K_HBA: USB-Schnittstelle	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3007	K_HBA: Kontaktlose Schnittstelle	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3009	K_HBA: Zusatzanforderungen für kontaktlose Schnittstelle	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_3011	K_Initialisierung: Kontaktlose Schnittstelle im COS nicht vorhanden	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3014	K_HBA: Vorhandensein Kryptobox	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3015	K_Personalisierung und K_Initialisierung: Historical Bytes im ATR	gemSpec_HBA_ObjSys_G2.1

Card-G2-A_3016-01	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3182	K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs, kein konkretes SE genannt	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3184	K_Initialisierung: Verhalten der Objekte, konkretes SE genannt	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3185	K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs, konkretes SE genannt	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3199	K_Initialisierung: Initialisierte Attribute von MF / EF.CardAccess	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3266-01	K_Initialisierung: Wert von pointInTime	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_3278	K_Initialisierung: Initialisiertes Attribut numberOfOctet von MF / EF.ATR	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3293-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3295-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3320-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CIA.CIAInfo	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3321-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.OD (Object Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3322-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3323-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3324-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CD (Certificate Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3626	K_Initialisierung: Herstellerspezifischer FileIdentifier	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_3628	K_Initialisierung: Inhalt der Records von EF.DIR	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3629-01	K_Initialisierung: Initialisierte Attribute von MF / DF.QES / PrK.HP.QES.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3631	K_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3639-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3641-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3643	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3645	K_Initialisierung: Initialisierte 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_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_3483-01	K_Initialisierung: Inhalt body von EF.Version2	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3484	K_Initialisierung: Reihenfolge der Datenobjekte in body von EF.Version2	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3485	K_Initialisierung: Datenobjekte in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3486	K_Initialisierung: DO_BufferSize in EF.ATR	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_3488	K_Initialisierung: DO_PT_COS in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3489	K_Initialisierung: DO_PI_CHIP in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1

Card-G2-A_3490	K_Initialisierung: DO_PI_COS in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3491	K_Initialisierung: DO_PI_InitialisiertesObjSys in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3493	K_Initialisierung DO_PI_Kartenkörper in EF.ATR-Initialisierung	gemSpec_Karten_Fach_TIP_G2.1
GS-A_4377	Card-to-Card-Authentisierung G1	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_4559	Versionierung der Karten der TI	gemSpec_OM
GS-A_5026	Versionierung von Karten durch die Produktidentifikation	gemSpec_OM
GS-A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM
GS-A_5140	Inhalt der Selbstauskunft von Karten	gemSpec_OM
GS-A_4668	Prüfung der mathematischen Korrektheit bei CV-Zertifikaten der Generation G1	gemSpec_PKI
Card-G2-A_2232	Größe Chip-Modul	gemSpec_eGK_Opt

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Zulassungsobjektes HBA-Objektsystem 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)
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	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_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
Card-G2-A_2675-01	K_Initialisierung: Initialisierte: Wert von PrK.HP.AUTO.R3072	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3270	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.AUTO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3271	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für 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_3625	K_Initialisierung: Fehlender FileIdentifier	gemSpec_HBA_ObjSys_G2.1
GS-A_3697	Anlass der Erhöhung von Versionsnummern	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

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 Sicherheitstechnische Eignung: Zertifizierung nach Technischer Richtlinie

In diesem Abschnitt sind Anforderungen verzeichnet, deren Umsetzung im Zuge einer Prüfung gemäß Technischer Richtlinie TR-03144 nachgewiesen werden muss. Der Nachweis erfolgt durch die Vorlage des Zertifikates nach TR-03144.

Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sich.techn. Eignung: Zertifizierung nach Technischer Richtlinie"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_15220	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.R2048	gemSpec_HBA_ObjSys_G2.1
A_15222	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.E256	gemSpec_HBA_ObjSys_G2.1
A_15224	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.R2048	gemSpec_HBA_ObjSys_G2.1
A_15226	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2032	K_Initialisierung: Änderung von Zugriffsregeln	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2033-01	K_Initialisierung: Ordnerattribute	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2034	K_Initialisierung: Dateiattribut	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2035	K_Initialisierung: Zugriffsregeln für besondere Kommandos	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2036	K_Initialisierung Anzahl logischer Kanäle	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2039	K_Initialisierung: Wert des Attributes root	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_2042-01	K_Initialisierung: Inhalt persistentPublicKeyList	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_2047	K_Initialisierung: Initialisierte Attribute von MF	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2048-01	K_Initialisierung: Initialisierte Attribute von MF / EF.ATR	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2055-01	K_Initialisierung: Initialisierte Attribute von MF / EF.DIR	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2057	K_Initialisierung: Initialisierte Attribute von MF / EF.GDO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2059-01	K_Initialisierung: Attribute von MF / EF.Version2	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2061	K_Initialisierung: Initialisierte Attribute von MF / EF.C.CA_HPC.CS.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2064	K_Initialisierung: Initialisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2067	K_Initialisierung: Initialisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2069	K_Initialisierung: Initialisierte Attribute von MF / PIN.CH	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2072	K_Initialisierung: Initialisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2075	K_Initialisierung: Initialisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2078-01	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2080-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES128	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2081-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2082	K_Initialisierung: Initialisierte Attribute von MF / DF.HPA	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2083	K_Initialisierung: Initialisierte Attribute von MF / DF.HPA / EF.HPD	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2084	K_Initialisierung: Initialisierte Attribute von MF / DF.QES	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2085-01	K_Initialisierung: Initialisierte Attribute von MF / DF.QES /	gemSpec_HBA_ObjSys_G2.1

	PrK.HP.QES.R2048	
Card-G2-A_2088-01	K_Initialisierung: Initialisierte Attribute von MF / DF.QES / PIN.QES	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2089	K_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.SSEC	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2091-01	K_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2097	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2098-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2101	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2107	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2110-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2117	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2118	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2119-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.CIA.CIAInfo	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2120-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.OD (Object Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2121-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.AOD (Authentication Object Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2122-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.PrKD (Private Key Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2123-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.CD(Certificate Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2124	K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO	gemSpec_HBA_ObjSys_G2.1

Card-G2-A_2125-01	K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2128	K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / PIN.AUTO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2129	K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / PIN.SO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2130-01	K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2131-01	K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072	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_2675-01	K_Initialisierung: Initialisierte: Wert von PrK.HP.AUTO.R3072	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_2868	K_Initialisierung: Initialisierte Attribute von MF / SK.CAN	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3009	K_HBA: Zusatzanforderungen für kontaktlose Schnittstelle	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3015	K_Personalisierung und K_Initialisierung: Historical Bytes im ATR	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3016-01	K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3181	K_Initialisierung: Größe persistentPublicKeyList	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3182	K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs, kein konkretes SE genannt	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3183	K_Initialisierung: Eigenschaften der Objekte in anderen SEs, kein konkretes SE genannt	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3184	K_Initialisierung: Verhalten der Objekte, konkretes SE genannt	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3185	K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs, konkretes SE genannt	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3186	K_Initialisierung: Eigenschaften der Objekte in anderen SEs, konkretes SE	gemSpec_HBA_ObjSys_G2.1

	genannt	
Card-G2-A_3199	K_Initialisierung: Initialisierte Attribute von MF / EF.CardAccess	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3266-01	K_Initialisierung: Wert von pointInTime	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3270	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.AUTO	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3271	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.SO	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_3278	K_Initialisierung: Initialisiertes Attribut numberOfOctet von MF / EF.ATR	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3293-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3295-01	K_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3320-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CIA.CIAInfo	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3321-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.OD (Object Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3322-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3323-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory)	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3324-01	K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CD (Certificate Directory)	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_3629-01	K_Initialisierung: Initialisierte Attribute von MF / DF.QES / PrK.HP.QES.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3631	K_Initialisierung: Initialisierte Attribute von MF / DF.QES /	gemSpec_HBA_ObjSys_G2.1

	EF.C.HP.QES.E256	
Card-G2-A_3639-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3641-01	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3643	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256	gemSpec_HBA_ObjSys_G2.1
Card-G2-A_3645	K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256	gemSpec_HBA_ObjSys_G2.1
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_3483-01	K_Initialisierung: Inhalt body von EF.Version2	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3484	K_Initialisierung: Reihenfolge der Datenobjekte in body von EF.Version2	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3485	K_Initialisierung: Datenobjekte in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3486	K_Initialisierung: DO_BufferSize in EF.ATR	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_3488	K_Initialisierung: DO_PT_COS in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3489	K_Initialisierung: DO_PI_CHIP in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3490	K_Initialisierung: DO_PI_COS in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3491	K_Initialisierung: DO_PI_InitialisiertesObjSys in EF.ATR	gemSpec_Karten_Fach_TIP_G2.1
Card-G2-A_3493	K_Initialisierung DO_PI_Kartenkörper in EF.ATR-Initialisierung	gemSpec_Karten_Fach_TIP_G2.1
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM

GS-A_3696	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM
GS-A_3700	Versionierung von Produkten auf Basis von dezentralen Produkttypen der TI-Plattform durch die Produktidentifikation	gemSpec_OM
GS-A_4559	Versionierung 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

3.2.2 Zertifizierung als Signaturerstellungseinheit

Der Produkttyp (HBA) erfordert eine Zertifizierung als qualifizierte elektronische Signaturerstellungseinheit gemäß Art. 30 [eIDAS-VO] auf Grundlage der in [(EU) 2016/650] festgelegten Standards.

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
GS-A_4362	X.509-Identitäten für Verschlüsselungszertifikate	gemSpec_Krypt

GS-A_4363	CV-Zertifikate G1	gemSpec_Krypt
GS-A_4364	CV-CA-Zertifikate G1	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

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_2230	Kartenformat	gemSpec_eGK_Opt
Card-G2-A_2231	Toleranzen Kartenkörper	gemSpec_eGK_Opt
Card-G2-A_2309	Material Kartenkörper	gemSpec_eGK_Opt
Card-G2-A_2310	Physikalische Eigenschaften des Kartenkörpers	gemSpec_eGK_Opt
Card-G2-A_2311	Überprüfung physikalische Eigenschaften	gemSpec_eGK_Opt
Card-G2-A_2312	Biegefestigkeit	gemSpec_eGK_Opt
Card-G2-A_2313	Torsionsfestigkeit	gemSpec_eGK_Opt
Card-G2-A_2314	Weichmacherstabilität: Biege- und Torsionsprüfung	gemSpec_eGK_Opt
Card-G2-A_2315	Weichmacherstabilität: Verblockungen/Ablösungen	gemSpec_eGK_Opt
Card-G2-A_2316	Untersuchungsverfahren Weichmacherstabilität	gemSpec_eGK_Opt
Card-G2-A_2317	Haftfestigkeit Chipmodul	gemSpec_eGK_Opt

Card-G2-A_2318	Untersuchungsverfahren Haftfestigkeit Chipmodul	gemSpec_eGK_Opt
----------------	---	-----------------

4 Umsetzungsanforderungen

Für die folgenden dargestellten Anforderungen (Umsetzungsanforderungen) ist eine Verfeinerung und Konkretisierung zu Blattanforderungen erforderlich, bevor die konkrete und vollständige Herstellung und der Betrieb von Produkten des Zulassungsobjektes HBA-Objektsystem möglich ist. Die Umsetzungsanforderungen werden in einer zukünftigen Version des Produkttypsteckbriefs durch neue verfeinerte und konkretisierte Blattanforderungen in Kapitel 3 ersetzt.

Tabelle 8: Offene Umsetzungsanforderungen an das Zulassungsobjekt

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Es liegen keine Anforderungen vor.	

5 Produktypspezifische Merkmale

5.1 Angaben zu EF.Version2

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

5.2 Optionale Ausprägungen

In diesem Kapitel werden die optionalen Ausprägungen des Zulassungsobjektes HBA-Objektsystem 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]

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

5.3 Variationen

5.3.1 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 das Zulassungsobjekt HBA Objektsystem zwei verschiedene Möglichkeiten, den Wert für das Attribut „transportStatus“ der PIN.AUTO und der PIN.SO eines HBA festzulegen: „Leer-PIN“ oder „Transport-PIN“. Beide PINs müssen mit demselben Wert für „transportStatus“ belegt werden.

6 Anhang A – Verzeichnisse

6.1 Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

6.2 Tabellenverzeichnis

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion	7
Tabelle 2: Mitgeltende Dokumente.....	7
Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"	9
Tabelle 4: Anforderungen zur funktionalen Eignung "Herstellereklärung"	15
Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sich.techn. Eignung: Zertifizierung nach Technischer Richtlinie".....	17
Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Herstellereklärung"	23
Tabelle 7: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung	24
Tabelle 8: Offene Umsetzungsanforderungen an das Zulassungsobjekt.....	26

6.3 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
[(EU) 2016/650]	Durchführungsbeschluss (EU) 2016/650 der Kommission vom 25. April 2016 zur Festlegung

	<p>von Normen für die Sicherheitsbewertung qualifizierter Signatur- und Siegelerstellungseinheiten gemäß Artikel 30 Absatz 3 und Artikel 39 Absatz 2 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (Text von Bedeutung für den EWR) (siehe http://data.europa.eu/eli/dec_impl/2016/650/oj)</p>
[eIDAS-VO]	<p>Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (siehe http://data.europa.eu/eli/reg/2014/910/oj)</p>