

Einführung der Gesundheitskarte

Spezifikation für Musterkarten und Testkarten (eGK, HBA, SMC)

Version:	2.8.0
Revision:	\main\rel_main\21
Stand:	08.05.2009
Status:	freigegeben

Dokumentinformationen

Änderungen zur Vorversion

Einfügung des Anhangs B mit Kodierungsvorgaben für die ICCSN der Musterkarten.

Inhaltliche Änderungen gegenüber der letzten freigegebenen Version 2.7.0 sind gelb markiert. Sofern ganze Kapitel eingefügt wurden, wurde zur besseren Lesbarkeit lediglich die Überschrift durch gelbe Markierung hervorgehoben.

Referenzierung

Das Dokument wird von anderen gematik-Dokumenten referenziert als:

[gemSpec_MK]	gematik: Einführung der eGK - Spezifikation für Musterkarten und Testkarten (eGK, HBA, SMC)
--------------	--

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.6	14.03.06		Erstellung des Dokumentes „Spezifikation für Testlaborkarten, Musterkarten und Testkarten (eGK, HBA, SMC)“	gematik, AG3
0.8	28.03.06		Ergänzung um HBA- und SMC-Vorgaben	gematik, AG3
0.9	02.05.06		Umstellung auf Test-Root für CVC	gematik, AG3
0.995	17.05.06		Einarbeitung Spezifikation Testlaborkarten	gematik, AG3
1.0.0	18.05.06		Freigabe und Veröffentlichung	gematik
1.2.2	31.08.06		Überarbeitung und Aktualisierung gesamtes Dokument	gematik, AG3
1.3.0	03.09.06		freigegeben	gematik
1.3.1	06.09.06		Änderungen gemäß Hinweisen	gematik, AG3
1.4.1	29.04.07		Trennung von der Spezifikation für Testlaborkarten, Einarbeitung von Ergänzungen	gematik, AG3
2.0.0	04.05.07		freigegeben	gematik
*2.0.9	15.05.07		Ergänzung ZDA-Meldungen für HBA und SMC-B	gematik, AG7

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
2.1.0	15.05.07		freigegeben	gematik
2.1.6	25.09.07		Erweitert um Vorgaben für Musterkarten, die komplett beim Kostenträger erstellt werden, und zugehörige Ergänzungen	gematik, AG7
2.2.0	04.10.07		freigegeben	gematik
2.2.3	17.10.07		Einarbeitung der Kommentare zu 2.2.0	SPE/DK
2.3.0	18.10.07		freigegeben	gematik
2.3.5	02.11.07		Einarbeitung Kennzeichnung „Generation 1“ Grafiken überarbeitet	SPE/DK
2.5.0	18.12.07		freigegeben	gematik
2.5.3	21.01.08		Einarbeitung File-Struktur Abbildungen aus eGK, Anpassung an Modifikationen in den Spezifikationen	SPE/DK
2.5.4	31.01.08		Einfügen der OID-Vorgaben für X.509-Zertifikate	SPE/DK
2.5.5	03.02.08		Einfügen eines Kapitels für die SMC-K Anpassung der Vorgabe für die KVNR	SPE/DK
2.5.6	13.02.08		Einarbeitung interne Kommentare zu 2.5.5	SPE/DK
2.6.0	22.02.08		freigegeben	gematik
	02.06.08		Änderung des Speicherorts für die OID des Zertifikatstyps, Hinweis auf [gemSpecKrypt], Einfügen von Verweisen auf Dokumente zur Festlegung der diversen Zertifikate	SPE/DK
	15.07.08		Einfügen von Verweisen auf Dokumente zur Festlegung der diversen Zertifikate, Streichen von oid_tsl_ca	SPE/DK
2.7.0	17.07.08		freigegeben	gematik
2.7.1	22.08.08	5.6, Abb. 17 und 22	Anpassungen an Modifikationen in HBA-Spezifikationen	gematik
2.7.2	04.03.09		Anfügen eines Anhangs B mit Kodierungsvorgaben für die ICCSN der Musterkarten	gematik
2.8.0	08.05.09		freigegeben	gematik

Inhaltsverzeichnis

Dokumentinformationen	2
Inhaltsverzeichnis.....	4
1 Zusammenfassung	8
2 Einführung	9
2.1 Zielsetzung und Einordnung des Dokuments	9
2.2 Zielgruppe	10
2.3 Geltungsbereich	10
2.4 Arbeitsgrundlagen.....	10
2.5 Abgrenzung des Dokuments	11
3 Eingangsanforderungen.....	12
4 Vorgaben für Musterkarten eGK	13
4.1 PIN- und PUK-Werte	13
4.1.1 Feste PIN-Werte.....	13
4.1.2 Transport-PIN-Werte	13
4.2 Speicherplatz	13
4.3 MF	14
4.4 DF.HCA.....	14
4.5 DF.ESIGN	15
4.6 DF.QES.....	16
4.7 DF.CIA.ESIGN	16
4.8 Erstellung der Daten der Versicherten.....	17
4.8.1 Bereitstellung der Daten durch die gematik	17
4.8.2 Bereitstellung der Daten durch den Kostenträger	17
4.9 Erstellung der X.509-Zertifikate	17
4.9.1 Erzeugung beim Kartenhersteller	17
4.9.2 Erzeugung durch den Kartenherausgeber.....	18
4.10 CV-Zertifikate für eGK-Musterkarten.....	20
4.10.1 Test-Root-CVC-CA für Musterkarten	20
4.10.2 Test-CVC-CA für eGK-Musterkarten.....	20
4.10.3 Verfügbarkeit.....	21
4.11 Generierung der Secret Keys SK.CAMS, SK.VSDD und SK.VSDDCAMS	21

4.11.1	Beistellung durch die gematik.....	21
4.11.2	Erzeugung durch den Kartenherausgeber	21
4.12	Optische Gestaltung der eGK Musterkarten.....	21
4.13	Auszutauschende Daten zur Erstellung von eGK-Musterkarten.....	23
4.13.1	Beistellung der Daten durch die gematik	23
4.13.1.1	<i>Daten, die die gematik an den Kartenhersteller schickt.....</i>	<i>23</i>
4.13.1.2	<i>Daten, die der Kartenhersteller an die gematik liefert.....</i>	<i>23</i>
4.13.1.2.1	Vor Auslieferung der eGK-Musterkarten.....	23
4.13.1.2.2	Nach Auslieferung der eGK-Musterkarten.....	23
4.13.2	Datenerzeugung beim Kartenherausgeber	24
4.13.2.1	<i>Daten, die der Kartenherausgeber an die gematik liefert bzw. bereitstellen muss.....</i>	<i>24</i>
4.13.2.1.1	Vor Auslieferung der eGK-Musterkarten.....	24
4.13.2.1.2	Nach Auslieferung der eGK-Musterkarten.....	25
4.13.2.2	<i>Lieferung der eGK-Musterkarten.....</i>	<i>25</i>
5	Vorgaben für Musterkarten HBA.....	26
5.1	PIN- und PUK-Werte	26
5.1.1	Feste PIN-Werte.....	26
5.1.2	Transport-PIN-Werte	26
5.2	MF	27
5.3	DF.HPA.....	28
5.4	DF.ESIGN	29
5.5	DF.QES.....	30
5.6	DF.CIA.QES und DF.CIA.ESIGN.....	31
5.7	Erstellung der X.509-Zertifikate	31
5.7.1	Vorgaben für OIDs und ProfessionItem für HBA-Musterkarten	32
5.8	CV-Zertifikate für Musterkarten HBA.....	32
5.9	Optische Gestaltung der HBA-Musterkarten	32
5.10	An den Kartenhersteller zu liefernde Unterlagen zur Erstellung von HBA-Musterkarten.....	34
5.11	Vom ZDA vor Auslieferung der HBA-Musterkarten an die gematik zu liefernde Daten	34
6	Vorgaben für Musterkarten SMC Typ A.....	35
6.1	PIN- und PUK-Werte	35
6.2	MF	35
6.3	DF.SMA	36
6.4	DF.KT.....	36
6.5	Erstellung des X.509-Zertifikats	37
6.5.1	OID-Vorgaben für SMC-A-Musterkarten	37
6.6	CV-Zertifikate für Musterkarten SMC-Typ A.....	37

6.7	Optische Gestaltung der Musterkarten für SMC Typ A.....	37
6.8	An den Kartenhersteller zu liefernde Unterlagen zur Erstellung von SMC Typ A-Musterkarten	39
6.9	Vor Auslieferung der SMC-A-Musterkarten	39
7	Vorgaben für Musterkarten SMC Typ B.....	40
7.1	PIN- und PUK-Werte	40
7.1.1	Feste PIN-Werte.....	40
7.1.2	Transport-PIN-Werte	40
7.2	MF	40
7.3	DF.SMA	41
7.4	DF.KT.....	41
7.5	DF.ESIGN	43
7.6	Erstellung der X.509-Zertifikate	43
7.6.1	OID-Vorgaben für SMC-B-Musterkarten	44
7.7	CV-Zertifikate für Musterkarten SMC-Typ B.....	44
7.8	Optische Gestaltung der Musterkarten für SMC Typ B.....	45
7.9	An den Kartenhersteller zu liefernde Unterlagen zur Erstellung von SMC-Typ B-Musterkarten	46
7.10	Vom ZDA/von der CA an die gematik zu liefernde Daten	47
7.10.1	Vor Auslieferung der SMC-B-Musterkarten.....	47
7.10.1.1	X.509-Zertifikate AUT, ENC und OSIG	47
7.10.1.2	X.509-Zertifikate SMKT.AUT.....	47
7.11	Vom Kartenhersteller nach Erstellung der SMC-Typ B-Musterkarten an die gematik zu liefernde Daten.....	47
8	Vorgaben für Musterkarten SMC-K.....	49
8.1	MF	49
8.2	DF.AK	49
8.3	DF.NK	50
8.4	DF.SAK.....	50
8.5	DF.Sicherheitsanker.....	51
8.6	Erstellung der X.509-Zertifikate	51
8.6.1	OID-Vorgaben für SMC-K-Musterkarten	51
8.7	CV-Zertifikate für Musterkarten SMC-Typ K.....	52
8.8	Zulassungs-ID im Zertifikat.....	52
8.9	CV-Zertifikate für Musterkarten SMC- K.....	52
8.10	Optische Gestaltung der Musterkarten für SMC K.....	52
8.11	An den Kartenhersteller zu liefernde Unterlagen zur Erstellung von SMC-K-Musterkarten.....	54

8.12	Daten	54
8.12.1	Vor Auslieferung der SMC-K-Musterkarten	54
8.13	Vom Kartenhersteller nach Erstellung der SMC-K-Musterkarten an die gematik zu liefernde Daten	54
9	Layout Testkarten eGK	56
10	Layout Testkarten HBA	58
Anhang A Festlegungen für IK der Krankenkassen, IIN des Kartenherausgebers und KVNR für Musterkarten eGK		
		59
A.1	Festlegungen für die IK des Kostenträgers für Musterkarten eGK	59
A.2	Festlegungen zur IIN des Kartenherausgebers für Musterkarten eGK	60
A.3	Festlegungen zur KVNR für Musterkarten eGK	60
Anhang B	Festlegungen für die ICCSN für Musterkarten	62
B.1	Definition der ICCSN	62
B.2	Kodierung der ICCSN	63
B.3	Festlegungen im Detail	63
B.3.1	IIN	63
B.3.2	Herstellerkennung	64
B.3.3	Kodierung des ZDA/der CA	64
B.3.4	Kodierung der Fehlerkategorie	65
B.3.5	Kodierung der Kartenart	65
Anhang C		66
C.1 -	Abkürzungen	66
C.2 -	Glossar	67
C.3 -	Abbildungsverzeichnis	67
C.4 -	Tabellenverzeichnis	68
C.5 -	Referenzierte Dokumente	68

1 Zusammenfassung

In diesem Dokument werden zunächst die verschiedenen, in der Einführungsphase der elektronischen Gesundheitskarte verwendeten Kartentypen (eGK, HBA und SMC) definiert. Anschließend werden die Voraussetzungen und Abläufe beschrieben, die von einem Kartenhersteller bei der Erstellung von eGK-, HBA- und SMC-Musterkarten eingehalten werden müssen.

Vor dem Testen mit Daten und Strukturen, wie sie in den Teilen 1 und 2 der eGK-Spezifikation ([gemSpec_eGK_P1] und [gemSpec_eGK_P2]) und in den entsprechenden Spezifikationen von HBA und SMC [HBA-P1], [HBA-P2] und [HBA-P3] beschrieben werden, müssen Chipkarten auf ihre grundsätzliche Eignung als eGK, HBA bzw. SMC getestet werden. Grundvoraussetzung ist, dass sie die funktionale Freigabe der gematik erhalten haben.

Nach einer entsprechenden Freigabe müssen Musterkarten für eGK, HBA und SMC zum weiteren Testen gemäß dieser Spezifikation erstellt werden. In dieser Spezifikation werden die Daten beschrieben, die auf Musterkarten aufzubringen sind. Außerdem wird festgelegt, wie diese Daten analog der jeweiligen Spezifikation in die Datenstrukturen der Musterkarten zu schreiben sind.

Anschließend werden Funktionen und Abläufe in den Testregionen mit Testkarten getestet. Diese Testkarten enthalten Echtdaten. Hinweise zum Layout dieser Karten stehen in den Kapiteln 9 und 10.

2 Einführung

2.1 Zielsetzung und Einordnung des Dokuments

Mit der Einführung der elektronischen Gesundheitskarte und dem Aufbau der zugehörigen Telematikinfrastruktur sind hohe Anforderungen an die Verfügbarkeit, Zuverlässigkeit, Performance und die Sicherheit der eingesetzten Komponenten, Dienste und Funktionen sowie des gesamten Systems verbunden.

Speziell die eingesetzten Chipkarten (eGK, HBA und SMC) müssen vor dem Einsatz in definierten Umgebungen ausführlich auf Übereinstimmung mit den Spezifikationen und mit den Vorgaben für die Funktionalität geprüft werden. Abbildung 1 zeigt die Kartentypen am Beispiel der elektronischen Gesundheitskarte, die während der Einführungsphase und auch für Freigabe und Tests im weiteren Verlauf des Projektes genutzt werden.




		
Testlaborkarten	Musterkarten	Testkarten
Teststufe I	Teststufe II	Teststufe III
Testlabor	Musterumgebung	Feldtest
Stückzahl: < 10	Stückzahl ~100	Stückzahl~10.000
Schwerpunkt: Betriebssystem	Schwerpunkt: Funktionen und Abläufe	Schwerpunkt: Funktionen und Abläufe
CVC-CA Root gematik	Test-CVC-CA- Root D-Trust	CVC-CA Root D-Trust
X-509: Hersteller	X-509: Hersteller bzw. LE-Org.	X-509: wie im Wirkbetrieb
	TSP-Eintrag in Test-TSL	TSP-Eintrag in Produktiv-TSL
Test-Datenstruk- turen	Muster-Daten	Echtdaten

Abbildung 1: Definition der verschiedenen Kartentypen am Beispiel der eGK

Testlaborkarten:

Zunächst sollen Chipkarten herstellerbezogen mit speziell spezifizierten Strukturen und Inhalten im Labor auf die Einhaltung der eGK-Spezifikationen [gemSpec_eGK_P1] und [gemSpec_eGK_P2] zur Verwendung als eGK und der HBA/SMC-Spezifikationen [HBA-P1], [HBA-P2] und [HBA-P3] zur Verwendung als HBA bzw. SMC getestet werden. Die speziell dafür festgelegten Strukturen und Spezifikationen sind im Dokument [gemSpec_TLK] enthalten. Nach erfolgreichem Test werden die jeweiligen Karten für den nächsten Schritt freigegeben.

Musterkarten:

In den Testregionen sollen Verfahren und Abläufe, die in der gematik für die Nutzung der Telematikinfrastuktur definiert werden, im praktischen Betrieb erprobt werden. Diese Erprobung erfolgt zunächst in Musterumgebungen (erst in der gematik-Musterumgebung und anschließend in den Musterumgebungen der Testregionen) mit Musterkarten. Die Musterkarten müssen den jeweiligen Spezifikationen entsprechen, enthalten aber keine Echtdaten. Nach erfolgreichem Test werden die Karten für den nächsten Schritt freigegeben.

Testkarten:

In den Testregionen sollen Verfahren und Abläufe, die in der gematik für die Nutzung der Telematikinfrastuktur definiert werden, im praktischen Betrieb erprobt werden. Die Erprobung mit Testkarten erfolgt in echten Umgebungen mit Testkarten. Die Testkarten müssen den jeweiligen Spezifikationen (mit einer möglichen Ergänzung im Layout, siehe Kapitel 9 und 10) entsprechen und enthalten Echtdaten.

Dieses Dokument beschreibt, welche Daten zur Erstellung der Musterkarten bereitgestellt und wie die in den verschiedenen Teilen der Spezifikation festgelegten Daten für die Musterkarten aufbereitet und in die Musterkarten geladen bzw. aufgedruckt werden müssen. Außerdem wird die Layout-Ergänzung für Testkarten beschrieben.

2.2 Zielgruppe

Dieses Dokument ist für die Testgruppe der gematik, für die Vertreter der Leistungserbringer, für die Kostenträger und für die Hersteller der Karten (Chipkartenhersteller und -personalisierer, Zertifizierungsdiensteanbieter) bestimmt und ermöglicht ihnen die Herstellung und Nutzung spezifikationsgerechter Musterkarten.

2.3 Geltungsbereich

Dieses Dokument enthält verbindliche Festlegungen für die Abläufe, die Datenformate und die Verantwortung für die Erzeugung der verschiedenen zur Erstellung einer Musterkarte benötigten Daten.

2.4 Arbeitsgrundlagen

Die Ausarbeitung basiert auf den Anforderungen, die sich aus den aktuellen Planungen zur Einführung der eGK ergeben. Grundlage der Definitionen der Daten, der Zertifikate,

der verwendeten Schlüssel und der Datenstrukturen sind die eGK-Spezifikation [gemSpec_eGK_P1], [gemSpec_eGK_P2], [gemSpec_eGK_P3] und ergänzenden Dokumente sowie die HBA/SMC-Spezifikationen [HBA-P1], [HBA-P2] und [HBA-P3] sowie ergänzenden Dokumente. Soweit zur Erreichung des genannten Zieles notwendig, sind die Ausschnitte aus den jeweiligen Spezifikationen und Dokumenten als Anhänge in dieses Dokument integriert.

Weiterführende obligatorische Anforderungen an Muster- und Testkarten (mit der Kennung Arzt) werden durch das Projektbüro eArztausweis der Bundesärztekammer vorgegeben.

2.5 Abgrenzung des Dokuments

Dieses Dokument definiert Struktur, Inhalt und Umfang der Daten, die auf die Musterkarten geschrieben werden müssen. Die Festlegungen für diese Musterkarten sind [gemSpec_eGK_P1], [gemSpec_eGK_P2], [gemSpec_eGK_P3], [HBA-P1], [HBA-P2], [HBA-P3] und einigen ergänzenden Dokumenten in der jeweils aktuellen Version entnommen. Bei Abweichungen zwischen diesen Teilen und den auf der gematik-Webseite veröffentlichten Fassungen ist die Fassung auf der gematik-Webseite verbindlich, falls dies nicht ausdrücklich anders festgelegt ist.

3 Eingangsanforderungen

Dieser Abschnitt wird in einer nächsten Version dieses Dokumentes ergänzt.

4 Vorgaben für Musterkarten eGK

Die Musterkarten müssen alle Vorgaben der eGK-Spezifikation erfüllen. Dies betrifft sowohl die Bereitstellung der definierten Kommandos [gemSpec_eGK_P1] als auch die Einrichtung der definierten File-Struktur [gemSpec_eGK_P2]. Insbesondere müssen das DF.HCA, das DF.ESIGN, das DF.CIA.ESIGN jeweils mit der kompletten Unterstruktur und mit den definierten Security- und Access-Conditions angelegt werden (siehe Abbildungen 2 bis 6). DF.QES kann angelegt werden (Siehe Kapitel 4.6.)

4.1 PIN- und PUK-Werte

4.1.1 Feste PIN-Werte

Die PIN-Werte MÜSSEN einheitlich auf den Wert 123456 gesetzt werden (Ausnahme siehe 4.1.2).

Die zugehörigen PUK-Werte MÜSSEN einheitlich auf den Wert 12345678 gesetzt werden.

4.1.2 Transport-PIN-Werte

Es KÖNNEN Musterkarten mit den in der Spezifikation zugelassenen Transport-PIN-Verfahren geliefert werden. Die Anzahl der mit den zugelassenen Transport-PIN-Verfahren zu liefernden Musterkarten muss mit der gematik abgestimmt werden.

4.2 Speicherplatz

Basis für die Größe des EEPROMs ist der im Dokument [gemeGK_Fach] angegebene Speicherplatzbedarf der eGK.

Zu den dort aufgeführten Nettodaten muss der Hersteller den Bedarf für den von ihm benötigten Overhead hinzurechnen und eine ausreichende Speichergröße wählen.

4.3 MF

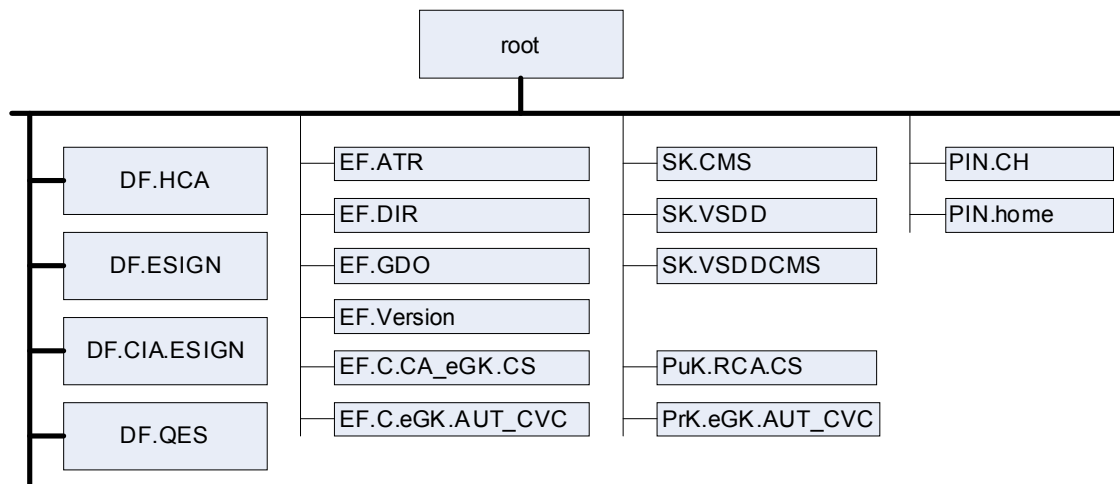


Abbildung 2: Objektstruktur einer eGK auf oberster Ebene

Die in [gemSpec_eGK_P2] festgelegten Parameter für Größe und Zugriffsregeln für das MF und die zugehörigen EFs sind umzusetzen. Die EFs und die Schlüsselfiles werden entsprechend der Spezifikation mit den angelieferten bzw. beim Kartenhersteller erzeugten Daten gefüllt.

4.4 DF.HCA

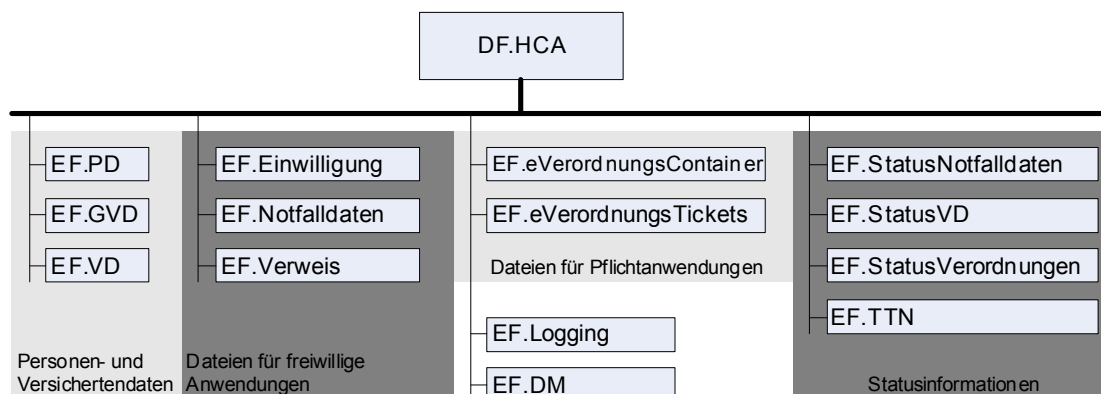


Abbildung 3: Objektstruktur der Gesundheitsanwendung DF.HCA

Die in [gemSpec_eGK_P2] festgelegten Parameter für Größe und Zugriffsregeln für das DF.HCA und seine EFs sind umzusetzen. Die EFs werden entsprechend der Spezifikation [gemeGK_Fach] mit den angelieferten bzw. beim Kartenhersteller erzeugten Daten gefüllt.

Die Vorgaben in [gemeGK_Fach] bezüglich der Füllung der EFs in DF.HCA sind umzusetzen. Falls keine Daten angeliefert bzw. vom Kartenhersteller erzeugt werden, sind die Initialwerte einzutragen. Dabei ist zu beachten, dass die Versionsnummer der VSD-Struktur der PD-, VD- und GVD-Daten dem Auftragsformular zu entnehmen ist und gemäß Spezifikation formatiert werden muss.

4.5 DF.ESIGN

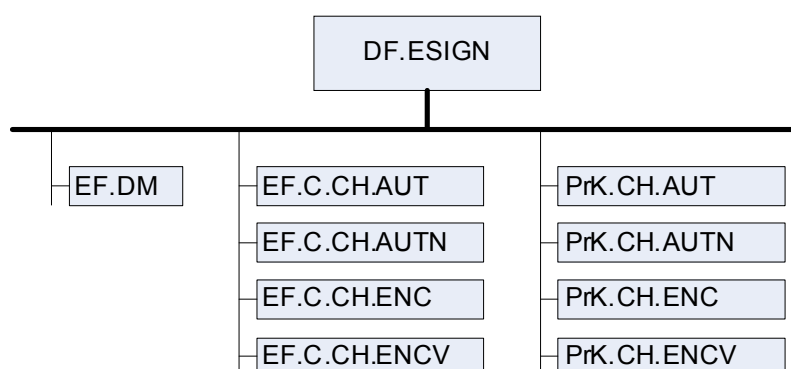


Abbildung 4: Objektstruktur der Anwendung ESIGN

Die in [gemSpec_eGK_P2] festgelegten Parameter für Größe und Zugriffsregeln für DF.ESIGN und die dazu gehörenden EFs sind umzusetzen. Die EFs und die Schlüsselfiles werden entsprechend der Spezifikation mit den angelieferten bzw. beim Kartenhersteller erzeugten Daten gefüllt.

4.6 DF.QES

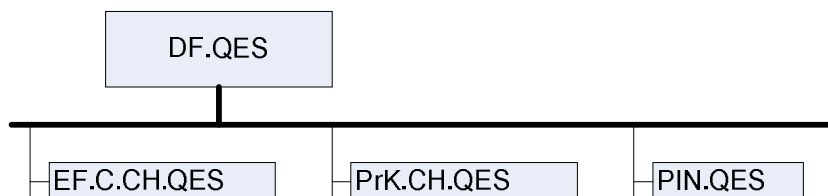


Abbildung 5: Objektstruktur der Anwendung QES

Das Anlegen von DF.QES ist nicht vorgeschrieben.

Falls DF.QES angelegt wird, muss die komplette Anwendung mit den oben angegebenen EFs, den in der eGK-Spezifikation Teil 2 [gemSpec_eGK_P2] definierten Security- und Access-Conditions und einem Zertifikat und einem Schlüsselpaar für eine fortgeschrittene Signatur angelegt werden.

Das Verfahren zum Nachladen von qualifizierten elektronischen Signaturen ist in der eGK-Spezifikation Teil 2 in den Kapiteln 7.2 bis 7.9 [gemSpec_eGK_P2#7.2-7.9] definiert. Es ist zulässig, testweise Sicherheitsanker in Form von X.509- oder CV-Zertifikaten aufzubringen. In diesen Fällen muss die komplette Struktur für das jeweils gewählte Verfahren (CV-Zertifikat oder Gütesiegel-Zertifikat als Sicherheitsanker), wie in [gemSpec_eGK_P2#7.2-7.9] in den Kapiteln 7.2 bis 7.9 definiert, auf der Karte realisiert werden. Diese Daten müssen technisch die Spezifikation abbilden, entsprechen aber nicht den Anforderungen der QES. Das Nachlade-Verfahren wird im Moment von der gematik nicht getestet.

4.7 DF.CIA.ESIGN

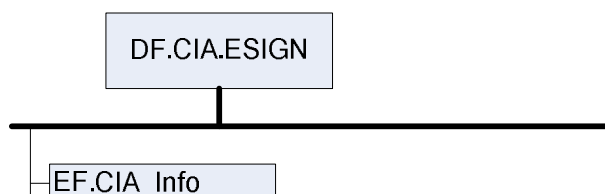


Abbildung 6: Objektstruktur der Anwendung DF.CIA.ESIGN

Die in [gemSpec_eGK_P2] festgelegten Parameter für Größe und Zugriffsregeln für DF.CIA.ESIGN und das dazu gehörende EF sind umzusetzen. Das EF wird entsprechend der Spezifikation [gemSpec_eGK_P2] gefüllt.

4.8 Erstellung der Daten der Versicherten

4.8.1 Bereitstellung der Daten durch die gematik

Die Musterkarten müssen Daten von fiktiven Versicherten enthalten. Die Datensätze werden in der im Dokument XML-Formatierung der Versichertendaten für die eGK [gemPers] spezifizierten Form im XML-Format angeliefert. Sie müssen vom Kartenhersteller in die entsprechenden EFs geschrieben werden. In diesen Datensätzen sind von der gematik vorgegebene ICCSN-Werte gemäß den Regeln in Anhang A enthalten.

Der Wert für den Issuer Identifier (gematik) ist dabei mit 00001 festgelegt.

4.8.2 Bereitstellung der Daten durch den Kostenträger

Die Musterkarten müssen Daten von fiktiven Versicherten enthalten. Sie müssen die Kostenträgerkennung (Issuer Identifier) in der ICCSN enthalten. Weitere Kodierungen in der ICCSN sind zulässig, solange sie die Eineindeutigkeit nicht beeinträchtigen. Die Kodierung der Kostenträgerkennung für Musterkarten ist in Anhang A festgelegt.

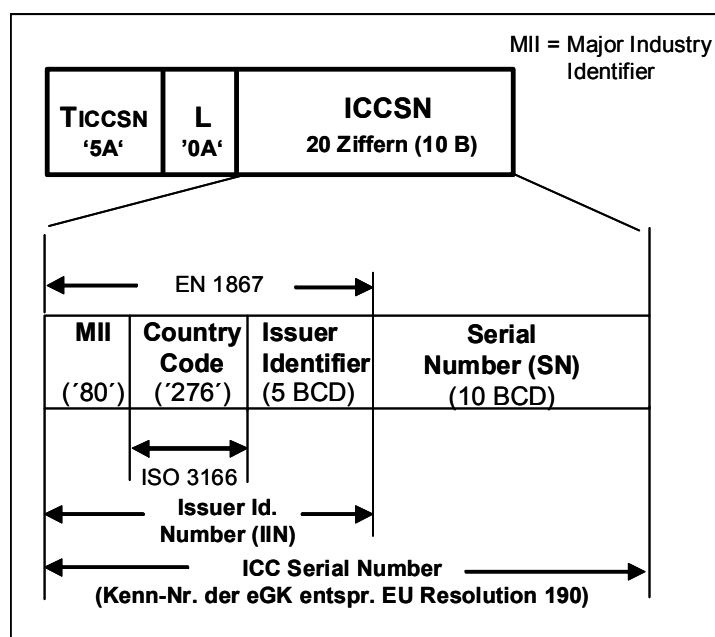


Abbildung 7: ICCSN für Gesundheitskarten

4.9 Erstellung der X.509-Zertifikate

4.9.1 Erzeugung beim Kartenhersteller

Die Schlüsselpaare für ENC, ENCV, AUT und AUTN werden vom Kartenhersteller erzeugt, dabei werden auch die zugehörigen Zertifikate in dem in [gemX.509_eGK] vorgegebenen Format berechnet. Als Schlüssellänge für das RSA-Verfahren werden die in [gemSpecKrypt] festgelegten Werte gefordert.

Als Gültigkeitszeitraum soll bei 10% der Karten eine Woche, bei den restlichen 90% 1 Jahr ab Herstellungsdatum eingetragen werden. Alle X.509-Zertifikate einer Karte (ENC, ENCV, AUT, AUTN, QES (falls vorhanden)) müssen dieselbe Gültigkeitsdauer haben.

Die zur Personalisierung der Zertifikate notwendigen Daten werden aus den mitgelieferten Personen-Datensätzen (siehe Kapitel 4.8) im spezifizierten Umfang extrahiert. .

Falls der OCSP-Responder der gematik genutzt werden soll, muss im CommonName des SubjectDN der Firmenname des Kartenherausgebers als Unterscheidungskriterium enthalten sein (siehe auch Kapitel 4.13.2.1.2).

Der Vorgabewert zur Füllung des Feldes "AuthorityInfoAccess" in den Zertifikaten muss in das entsprechende Datenfeld eingetragen werden.

Das DF.QES wird entweder nicht oder mit den in Abbildung 5 angegebenen EFs, den in [gemSpec_eGK_P2] definierten Security- und Access-Conditions und einem Zertifikat und einem Schlüsselpaar für eine fortgeschrittene Signatur angelegt.

Das Verfahren zum Nachladen von qualifizierten elektronischen Signaturen ist in der eGK-Spezifikation Teil 2 [gemSpec_eGK_P2#7.2-7.9] in den Kapiteln 7.2 bis 7.9 definiert. Es ist zulässig, testweise Sicherheitsanker in Form von X.509- oder CV-Zertifikaten aufzubringen. In diesen Fällen muss die komplette Struktur für das jeweils gewählte Verfahren (CV-Zertifikat oder Gütesiegel-Zertifikat als Sicherheitsanker), wie in [gemSpec_eGK_P2#7.2-7.9] in den Kapiteln 7.2 bis 7.9 definiert, auf der Karte realisiert werden. Diese Daten müssen technisch die Spezifikation abbilden, entsprechen aber nicht den Anforderungen der QES. Das Verfahren wird im Moment von der gematik nicht getestet

Bei den Tests mit Musterkarten wird auch die Online-Abfrage von Sperrinformationen getestet (OCSP-Abfrage). Damit dies für die vom Kartenhersteller erzeugten X.509-Zertifikate möglich ist, müssen die unter 4.13.2.1 definierten Daten nach Erstellung der Musterkarten an die gematik geliefert werden, falls der OCSP-Service der gematik genutzt werden soll. Andernfalls muss der Herausgeber dafür sorgen, dass ein funktionsfähiger OCSP-Service für die von ihm beschafften Musterkarten bereitsteht und die für diesen gültigen Daten in das Feld der eGK eingetragen werden.

4.9.2 Erzeugung durch den Kartenherausgeber

Die Schlüsselpaare für ENC, ENCV, AUT und AUTN werden vom Kartenherausgeber oder von einer vom Kartenherausgeber beauftragten CA erzeugt. Dabei werden auch die zugehörigen Zertifikate in dem in [gemX.509_eGK] vorgegebenen Format berechnet. Als Schlüssellänge für das RSA-Verfahren werden die in [gemSpecKrypt] festgelegten Werte gefordert

Der Gültigkeitszeitraum kann vom Kostenträger frei festgelegt werden. Alle X.509-Zertifikate einer Karte (ENC, ENCV, AUT, AUTN, SIG/QES (falls vorhanden)) müssen dieselbe Gültigkeitsdauer haben.

Die zur Personalisierung der Zertifikate notwendigen Daten werden aus den vom Kostenträger generierten Personen-Datensätzen im spezifizierten Umfang extrahiert.

Das Feld „AuthorityInfoAccess" in den Zertifikaten muss mit den Daten der genutzten CA gefüllt werden. Falls der OCSP-Service der gematik genutzt werden soll, müssen die Daten dieses Service eingetragen werden.

Das DF.QES wird entweder nicht oder mit den in Abbildung 5 angegebenen EFs, den in [gemSpec_eGK_P2] definierten Security- und Access-Conditions und einem Zertifikat und einem Schlüsselpaar für eine fortgeschrittene Signatur angelegt.

Das Verfahren zum Nachladen von qualifizierten elektronischen Signaturen ist in der eGK-Spezifikation Teil 2 [gemSpec_eGK_P2#7.2-7.9] in den Kapiteln 7.2 bis 7.9 definiert. Es ist zulässig, testweise Sicherheitsanker in Form von X.509- oder CV-Zertifikaten aufzubringen. In diesen Fällen muss die komplette Struktur für das jeweils gewählte Verfahren (CV-Zertifikat oder Gütesiegel-Zertifikat als Sicherheitsanker), wie in [gemSpec_eGK_P2#7.2-7.9] in den Kapiteln 7.2 bis 7.9 festgelegt, auf der Karte realisiert werden. Diese Daten müssen technisch die Spezifikation abbilden, entsprechen aber nicht den Anforderungen der QES. Das Verfahren wird im Moment von der gematik nicht getestet.

Bei den Tests mit Musterkarten wird auch die Online-Abfrage von Sperrinformationen getestet (OCSP-Abfrage). Daher muss die genutzte CA einen entsprechenden Online-Verzeichnisdienst bereitstellen. Falls der OCSP-Service der gematik genutzt werden soll, müssen die unter 4.13.2.1 definierten Daten nach Erstellung der Musterkarten an die gematik geliefert werden.

OID-Vorgaben für eGK-Musterkarten

In die X.509-Zertifikate der Musterkarten müssen gemäß [gemX.509_eGK] und [gemTSL_SP_CP_Test] OIDs und Texte eingetragen werden. In der folgenden Tabelle sind die Referenzbezeichnungen angegeben. Die zugehörigen OIDs/Texte finden sich im Dokument [gemSpec_OID].

Tabelle 1 OID-Referenzen für Musterkarten eGK (verpflichtend)

Speicherort	OID-Referenz
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.CH.ENC, C.CH.ENCV, C.CH.AUT, C.CH.AUTN, falls vorhanden: C.CH.QES oder C.CH.SIG)	oid_versicherter
CertificatePolicies, in allen Zertifikaten (C.CH.ENC, C.CH.ENCV, C.CH.AUT, C.CH.AUTN, falls vorhanden: C.CH.QES oder C.CH.SIG)	oid_policy_muster_cp
CertificatePolicies in C.CH.ENC	oid_egk_enc
CertificatePolicies in C.CH.ENCV	oid_egk_encv
CertificatePolicies in C.CH.AUT	(1) oid_egk_aut
CertificatePolicies in C.CH.AUTN	oid_egk_autn
CertificatePolicies in C.CH.SIG	oid_egk_sig

4.10 CV-Zertifikate für eGK-Musterkarten

4.10.1 Test-Root-CVC-CA für Musterkarten

Es gibt eine Test-Root-CVC-CA für Musterkarten. Von dieser müssen alle CV-Zertifikate für die Musterkarten abgeleitet werden. Dies gilt sowohl für eGK als auch für HBA und für SMC Musterkarten.

Die gematik ist verantwortlich für die Test-Root-CVC-CA. Betrieben wird diese durch den gleichen Dienstleister (D-Trust) wie die Produktiv-Root-CVC-CA.

Der öffentliche Schlüssel der Test-Root-CVC-CA wird durch den Betreiber im Internet veröffentlicht, siehe

<https://www.d-trust.net/internet/content/gematik-roots.html>

Der CA-Name der Test-Root-CVC-CA ist DEGXX.

Die Schlüssellänge wird durch [gemSpecKrypt] festgelegt.

Anmerkung: Die ab Release 2.3.2 verwendeten Karten (eGK, HBA, SMC) müssen CV-Zertifikate enthalten, die von einer komplett neuen Kette (Root-CVC-CA und CVC-CAs) stammen: die Schlüssellänge der RSA-Schlüssel muss 2048 bit betragen, es muss SHA2 als Hash-Algorithmus verwendet werden (siehe auch [gemSpec_eGK_P1]). Es wird keine Cross-Zertifizierung zwischen der bisherigen Root-CVC-CA und der neuen Root-CVC-CA geben.

4.10.2 Test-CVC-CA für eGK-Musterkarten

Kartenherausgeber müssen dafür sorgen, dass die Musterkarten mit Test-CV-Zertifikaten ausgestattet sind. Dies gilt sowohl für eGK- als auch HBA- und SMC-Musterkarten.

Test-CV-Zertifikate müssen durch eine Test-CVC-CA generiert werden. Eine Test-CVC-CA muss sich bei der gematik registrieren lassen. Erst danach kann das Test-CA-CV-Zertifikat für die Test-CVC-CA bei der Test-Root-CVC-CA beantragt werden.

Eine Test-CVC-CA muss einen registrierten CA-Namen besitzen. Siehe hierzu "http://www.sit.fraunhofer.de/cms/de/forschungsbereiche/sde/rid_sde/ZDA.php"

Die Schlüssellänge wird durch [gemSpecKrypt] festgelegt.

Das Vorgehen für die Registrierung bei der gematik sowie für das Beantragen des Test-CA-CV-Zertifikats bei D-Trust wird in [gemPKI_Reg] beschrieben.

Der Kartenproduzent muss neben dem Test-CV-Zertifikat der Musterkarte den öffentlichen Schlüssel der Test-Root-CVC-CA sowie das Test-CA-CV-Zertifikat der ausgebenden Test-CVC-CA in die eGK-Musterkarten einbringen.

Anmerkung: Die ab Release 2.3.2 verwendeten Karten (eGK, HBA, SMC) müssen CV-Zertifikate enthalten, die von einer komplett neuen Kette (Root-CVC-CA und CVC-CAs) stammen: die Schlüssellänge der RSA-Schlüssel muss 2048 bit betragen, es muss SHA2 als Hash-Algorithmus verwendet werden (siehe auch [gemSpec_eGK_P1]). Es wird keine Cross-Zertifizierung zwischen der bisherigen Root-CVC-CA und der neuen Root-CVC-CA geben.

4.10.3 Verfügbarkeit

Die Test-Root-CVC-CA für eine Schlüssellänge von 2048 bit wird ab 15.6.2008 zur Verfügung stehen.

4.11 Generierung der Secret Keys SK.CAMS, SK.VSDD und SK.VSDDCAMS

4.11.1 Beistellung durch die gematik

Die zur gegenseitigen Authentifizierung mit symmetrischen Schlüsseln benötigten Secret Keys SK.CAMS, SK.VSDD und SK.VSDDCAMS (3DES-Schlüssel) werden von der gematik erzeugt und den Herstellern zur Verfügung gestellt. Für Musterkarten werden keine kartenindividuellen Schlüssel aus Masterkeys abgeleitet; die Schlüssel sind für alle eGK-Musterkarten gleich.

4.11.2 Erzeugung durch den Kartenherausgeber

Der Kartenherausgeber kann die symmetrischen 3DES-Schlüssel (auch kartenindividuell) mit seinem Prozess erzeugen und in die Karten einbringen. Zum Testen der damit abgesicherten Funktionen müssen die entsprechenden Services (CAMS und VSDD) zur Verfügung stehen. Damit die gematik die Funktionen testen kann, müssen die erzeugten (evtl. kartenindividuellen) Schlüssel an die gematik übermittelt werden.

4.12 Optische Gestaltung der eGK Musterkarten

Für die äußere Gestaltung der Musterkarten gilt bezüglich der Maße [gemSpec_eGK_P3]. Die optische Gestaltung der Vorderseite ist gemäß folgender Vorlagen auszuführen:

Gestaltung ohne Bild siehe Abbildung 8.

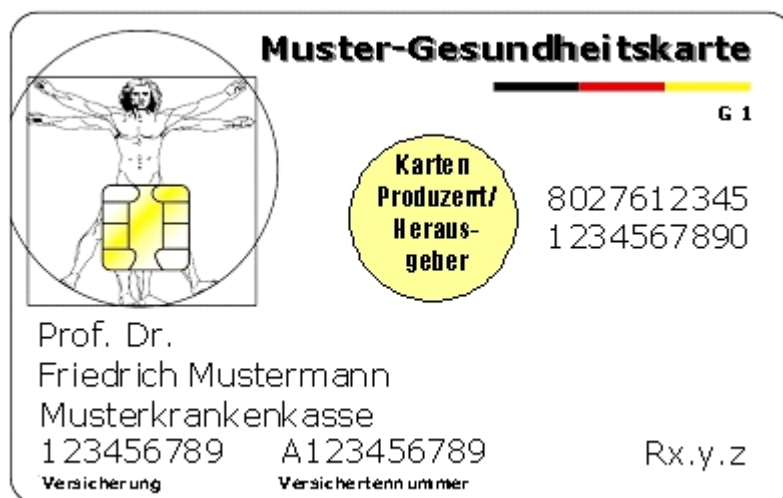


Abbildung 8: Kartenvorderseite mit Personalisierung, ohne Bild

Gestaltung mit Bild siehe Abbildung 9:

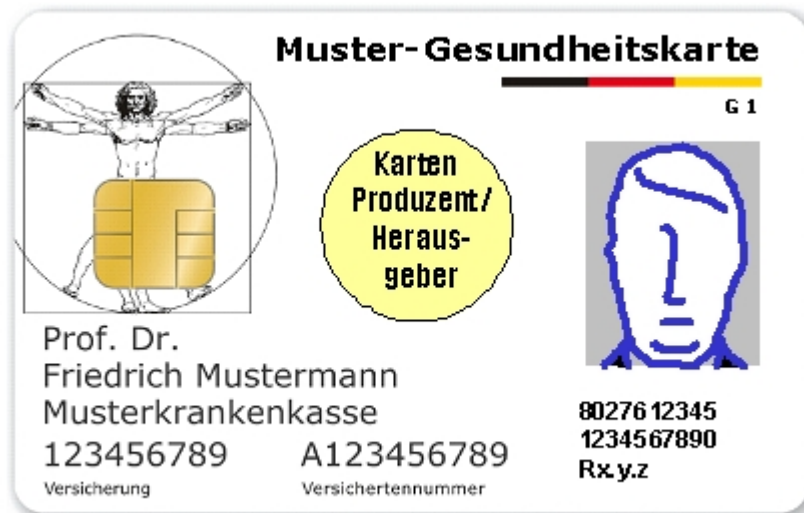


Abbildung 9: Kartenvorderseite mit Personalisierung, mit Bild

Anordnung ICCSN und Release-Bezeichnung beispielhaft

Dem Schriftzug „Gesundheitskarte“ gemäß [gemSpec_eGK_P3] ist in gleicher Schriftart das Wort „Muster-“ voranzustellen.

Der Schriftzug „G 1“ ist gemäß [gemSpec_eGK_P3] aufzubringen.

Die Daten zur Person, zur Versicherung und die Versichertennummer werden dem jeweils verwendeten Datensatz gemäß [gemSpec_eGK_P2] Anhang E entnommen.

Regeln für die Vergabe von IK der Krankenkasse, zur IIN des Kartenherausgebers und zur Versichertennummer sind im Anhang A festgelegt.

Für Muster-eGK ist eine Fotopersonalisierung nicht verpflichtend. Das BSI-Logo darf nicht aufgedruckt werden.

Die ICCSN MUSS auf die Karte aufgedruckt werden.

Wird kein Foto aufgebracht, kann die ICCSN stattdessen in zwei Zeilen mit je 10 Stellen je Zeile aufgedruckt werden. Ausrichtung rechtsbündig zum Schriftzug „Gesundheitskarte“. Schrift analog der sonstigen Personalisierung auf der Vorderseite. Die ICCSN kann auch auf die Rückseite (z. B. im dafür vorgesehenen EHIC-Feld, falls vorhanden) aufgedruckt werden.

Wird die Muster-eGK mit einem Foto gemäß [gemSpec_eGK_P3] versehen, MUSS die ICCSN entweder an anderer Stelle der Vorderseite (Beispiel siehe Abbildung 9) oder auf die Rückseite (z. B. im dafür vorgesehenen EHIC-Feld, falls vorhanden) aufgedruckt werden.

Zusätzlich muss das Release, für das die Musterkarten hergestellt worden sind, im Format x.y.z auf die Vorderseite (Beispiele siehe Abbildungen 8 und 9) oder auf die Rückseite (zusammen mit der ICCSN, falls kein EHIC-Feld vorhanden ist) gedruckt werden. Damit sind auch die jeweiligen Spezifikationsversionen festgelegt.

An der Stelle „Muster-Kartenproduzent/Muster-Kartenherausgeber“ kann der Hersteller/Herausgeber der Musterkarten sein Logo einfügen.

Die Kartenrückseite ist weiß. Alternativ kann auch eine entwertete EHIC-Rückseite zum Einsatz kommen.

4.13 Auszutauschende Daten zur Erstellung von eGK-Musterkarten

4.13.1 Beistellung der Daten durch die gematik

4.13.1.1 Daten, die die gematik an den Kartenhersteller schickt

Kartenhersteller, die eGK-Musterkarten gemäß dieser Vorgaben erstellen wollen, melden dies formlos (Brief, E-Mail, Fax) bei der gematik an. Daraufhin erhalten sie von der gematik folgende Datensätze:

- (1) Auftragsformular mit den für alle Karten geltenden Daten:
 - Stückzahl
 - Vorgaben zum Füllen des Feldes "AuthorityInfoAccess"
 - Lieferanschrift für die Musterkarten
- (2) Datensatz mit Muster-Versichertendaten für Musterkarten (Zahl der Datensätze entspricht der geforderten Stückzahl) im XML-Format gemäß aktueller Spezifikation; die Musterdatensätze enthalten die jeweilige ICCSN einschließlich der Kodierung für die Kategorisierung.
- (3) Datensatz mit den 3DES-Schlüsselpaaren SK.CAMS.ENC, SK.CAMS.MAC, SK.VSDD.ENC und SK.VSDD.MAC, falls nicht schon vorhanden.

4.13.1.2 Daten, die der Kartenhersteller an die gematik liefert

4.13.1.2.1 *Vor Auslieferung der eGK-Musterkarten*

CAs, die eGK-Musterkarten gemäß dieser Vorgaben erstellen wollen, müssen gemäß dem Dokument [gemX.509_TSP] „PKI für X.509-Zertifikate: Registrierung eines Trust Service Provider (TSP)“ bei der gematik als zugelassene CA registriert sein und die zu registrierenden Zertifikate gemäß [gemX.509_TSP#4.3.1] vor Auslieferung der Musterkarten an die gematik zum Eintrag in die Test-TSL liefern.

4.13.1.2.2 *Nach Auslieferung der eGK-Musterkarten*

Kartenhersteller, die eGK-Musterkarten gemäß dieser Vorgaben erstellt haben, müssen folgende Daten nach Auslieferung der eGK-Musterkarten an die gematik zurückliefern:

- (1) X.509-Zertifikate (ENC, ENCV, AUT, AUTN, SIG/QES (falls vorhanden)) aller erstellten Musterkarten im Format .cer. Bei größerer Anzahl erstellter Zertifikate (>25) sollen die Zertifikate in einer Datei gezippt werden

- (2) Zu den eigentlichen Zertifikaten ist eine Liste beizufügen, die zu jedem erzeugten Zertifikat Dateinamen, den CommonName und die Zertifikatsseriennummer enthält.
- (3) Das CA-Zertifikat der CA, mit der die Versichertenzertifikate erstellt wurden, mit dem dazugehörigen Schlüsselpaar (öffentlicher und privater Schlüssel) im Format PKCS#12. Der Aufbau der CA-Zertifikate MUSS ISIS-MTT-konform sein. Im Zertifikat der CA MUSS der Wert ca=true in den BasicConstraints eingetragen werden (siehe Tabelle 1). Als Verwendungszweck (Key Usage) MUSS neben „keyCertSign“ auch „crlSign“ eingetragen sein. Das Passwort für die PKCS#12-Datei soll einheitlich auf den Wert „Musterkarte“ gesetzt sein.

Tabelle 2 Auszug aus [ISIS-MTT Part 1], Table 18

#	ASN.1 DEFINITION	SEMANTICS	SUPPORT		REFERENCES		NOTES
			GEN CA/EE CERT	PROC	RFC3280	ISISMTT	
1	BasicConstraints ::= SEQUENCE {	Indicates a CA certificate and defines how deep a certificate may exist below that CA.	++/+-	++	4.2.1.10		[1]
2	ca BOOLEAN DEFAULT FALSE,	ca=TRUE indicates a CA certificate ca=FALSE indicates an end entity					
3	pathLenConstraint INTEGER (0..MAX) OPTIONAL }	only meaningful if ca=TRUE, indicates how many CA certificates may be included in the certification path below this CA. That is, pathLenConstraint=0 indicates that only end entity certificates may follow in the path. If this field does not appear, there is no limit to the path length.					
[1]	[RFC3280] This extension MUST appear as a critical extension in all CA certificates that contain public keys used to validate digital signatures on certificates. This extension MAY appear as a critical or non-critical extension in CA certificates that contain public keys used exclusively for purposes other than validating digital signatures on certificates. Such CA certificates include ones that contain public keys used exclusively for validating digital signatures on CRLs and ones that contain key management public keys used with certificate enrollment protocols. This extension MAY appear as a critical or non-critical extension in end entity certificates. ISIS-MTT PROFILE: This extension MAY appear in end entity certificates and MUST appear in CA certificates. It MUST be marked critical.						

4.13.2 Datenerzeugung beim Kartenherausgeber

In diesem Fall werden die entsprechenden Daten in der Verantwortung des Kostenträgers erzeugt und vom Kartenhersteller in die Karte geschrieben. Dies gilt für die Datensätze für die Versichertendaten, die X.509-Zertifikate einschließlich der Schlüsselpaare und für die symmetrischen Schlüssel. Es ist zu beachten, dass in der ICCSN die richtige Kennung für den Kartenherausgeber verwendet wird. Es ist möglich, in der ICCSN noch spezielle Kennungen des Kartenherausgebers unterzubringen; diese dürfen die Eineindeutigkeit der ICCSN nicht verhindern (siehe auch Anhang A).

4.13.2.1 Daten, die der Kartenherausgeber an die gematik liefert bzw. bereitstellen muss

4.13.2.1.1 Vor Auslieferung der eGK-Musterkarten

CAs, die eGK-Musterkarten gemäß dieser Vorgaben erstellen wollen, müssen gemäß dem Dokument [gemX.509_TSP] „PKI für X.509-Zertifikate: Registrierung eines Trust Service Provider (TSP)“ bei der gematik als zugelassene CA registriert sein und die zu registrierenden Zertifikate gemäß Kapitel 4.3.1 in [gemX.509_TSP#4.3.1] vor Auslieferung der Musterkarten an die gematik zum Eintrag in die Test-TSL liefern.

Um eine Online-Überprüfung der Zertifikate zu ermöglichen, muss das Feld "AuthorityInfoAccess" von der die Zertifikate ausstellenden CA gefüllt und der dazugehörige Verzeichnisdienst bereitgestellt werden.

4.13.2.1.2 *Nach Auslieferung der eGK-Musterkarten*

Kartenhersteller, die eGK-Musterkarten gemäß diesen Vorgaben erstellt haben, müssen folgende Daten nach Auslieferung der eGK-Musterkarten an die gematik zurückliefern:

Damit die gematik die mit den symmetrischen Schlüsseln abgesicherten Prozesse überprüfen kann, müssen die (evtl. kartenindividuellen) symmetrischen 3DES-Schlüssel (zusammen mit den jeweiligen X.509-Zertifikaten) an die gematik geliefert werden.

Falls der OCSP-Service der gematik genutzt werden soll, müssen folgende Daten an die gematik geliefert werden:

- (1) X.509-Zertifikate (ENC, ENCV, AUT, AUTN, SIG/QES (falls vorhanden)) aller erstellten Musterkarten im Format .cer. Bei größerer Anzahl erstellter Zertifikate (>25) sollen die Zertifikate in einer Datei gezippt werden. Im CommonName des SubjectDN soll der Kostenträgername als Unterscheidungskriterium enthalten sein.
- (2) Zu den eigentlichen Zertifikaten ist eine Liste beizufügen, die zu jedem erzeugten Zertifikat Dateinamen, den CommonName und die Zertifikatsseriennummer enthält.
- (3) Das CA-Zertifikat der CA, mit der die Versichertenkarten erstellt wurden, mit dem dazugehörige Schlüsselpaar (öffentlicher und privater Schlüssel) im Format PKCS#12. Der Aufbau der CA-Zertifikate MUSS ISIS-MTT-konform sein. Im Zertifikat der CA MUSS der Wert ca=true in den BasicConstraints eingetragen werden (siehe Tabelle 1). Als Verwendungszweck (Key Usage) MUSS neben „keyCertSign“ auch „crlSign“ eingetragen sein. Das Passwort für die PKCS#12-Datei soll einheitlich auf den Wert „Musterkarte“ gesetzt sein.

4.13.2.2 **Lieferung der eGK-Musterkarten**

Die eGK-Musterkarten müssen an die gematik geschickt werden. Wenn nicht anders abgesprochen, sollte eine Lieferung aus mindestens 100 eGKs bestehen.

5 Vorgaben für Musterkarten HBA

Die Musterkarten müssen alle Vorgaben der HBA-Spezifikation erfüllen. Dies betrifft sowohl die Bereitstellung der definierten Kommandos [HBA-P1] als auch die Einrichtung der definierten File-Struktur [HBA-P2]. Insbesondere müssen DF.HPA, DF.ESIGN, DF.QES und DF.CIA.ESIGN jeweils mit der kompletten Unterstruktur und mit den definierten Security- und Access-Conditions angelegt werden (siehe Abbildungen 12 bis 16).

5.1 PIN- und PUK-Werte

5.1.1 Feste PIN-Werte

Die PIN-Werte MÜSSEN einheitlich auf den Wert 123456 gesetzt werden Ausnahme siehe 5.1.2).

Die zugehörigen PUK-Werte MÜSSEN einheitlich auf den Wert 12345678 gesetzt werden.

5.1.2 Transport-PIN-Werte

Es KÖNNEN Musterkarten mit den in der Spezifikation zugelassenen Transport-PIN-Verfahren geliefert werden. Die Anzahl der mit den zugelassenen Transport-PIN-Verfahren zu liefernden Musterkarten muss mit der gematik abgestimmt werden.

5.2 MF

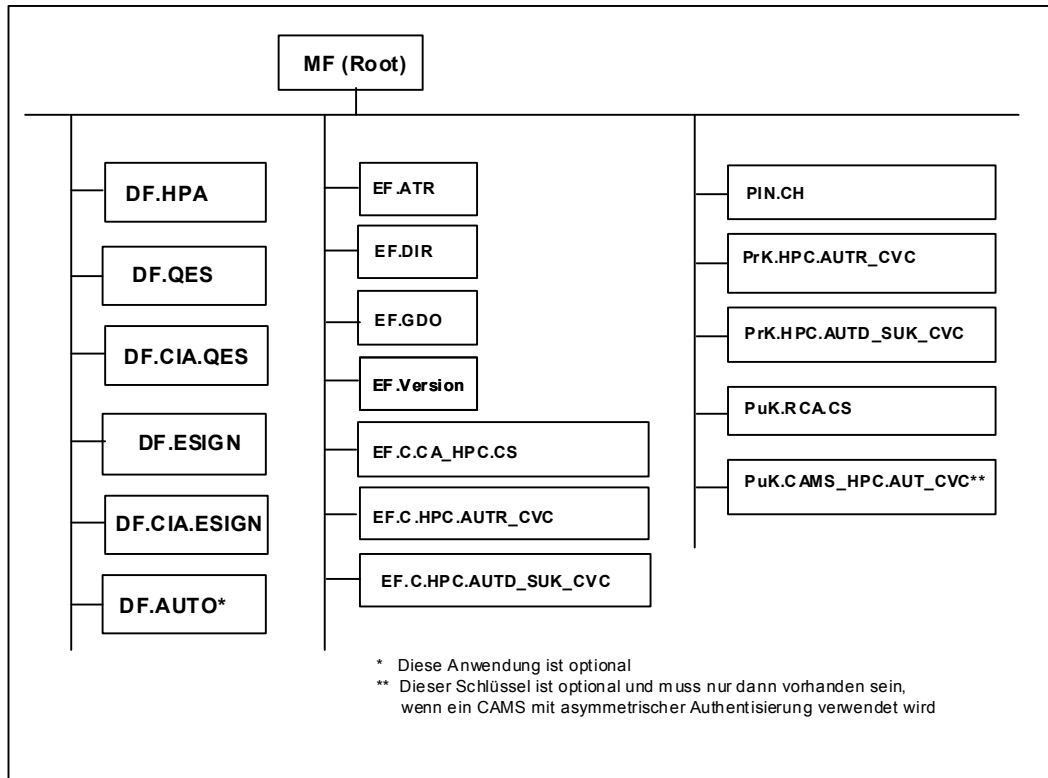


Abbildung 10: Allgemeine Dateistruktur des HBA

Die in [HBA-P2] festgelegten Parameter für Größe und Zugriffsregeln für das MF und die zugehörigen EFs sind umzusetzen. Die EFs und die zusätzlichen Schlüsselfiles werden entsprechend der Spezifikation mit den angelieferten bzw. beim ZDA/Kartenhersteller erzeugten Daten gefüllt.

5.3 DF.HPA

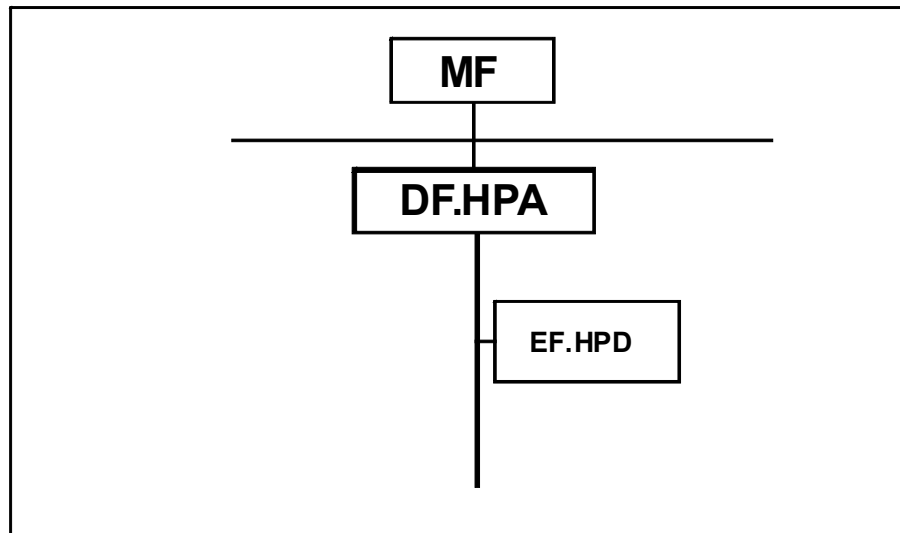


Abbildung 11: Dateistruktur von DF.HPA

Die in [HBA-P2] festgelegten Parameter für Größe und Zugriffsregeln für das DF.HPA und seine EFs sind umzusetzen. Die EFs werden entsprechend der Spezifikation mit den angelieferten bzw. beim ZDA/Kartenhersteller erzeugten Daten gefüllt.

5.4 DF.ESIGN

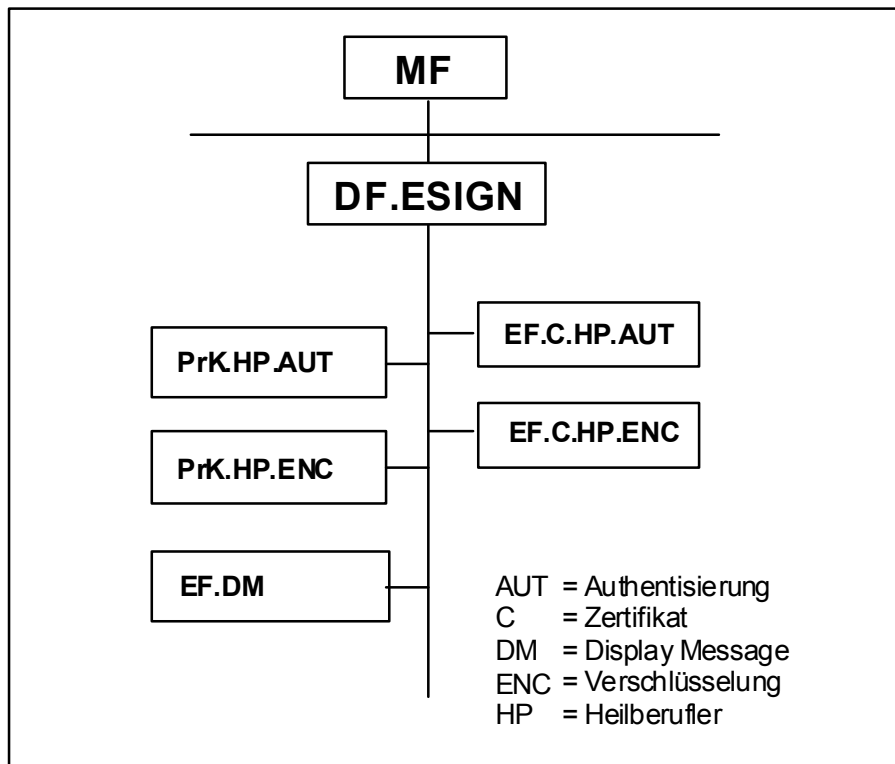


Abbildung 12: Prinzipielle Struktur von DF.ESIGN

Die in [HBA-P2] festgelegten Parameter für Größe und Zugriffsregeln für das DF.ESIGN und seine EFs sind umzusetzen. Die EFs und die zusätzlichen Schlüsselfiles werden entsprechend der Spezifikation mit den angelieferten bzw. beim ZDA erzeugten Daten gefüllt.

5.5 DF.QES

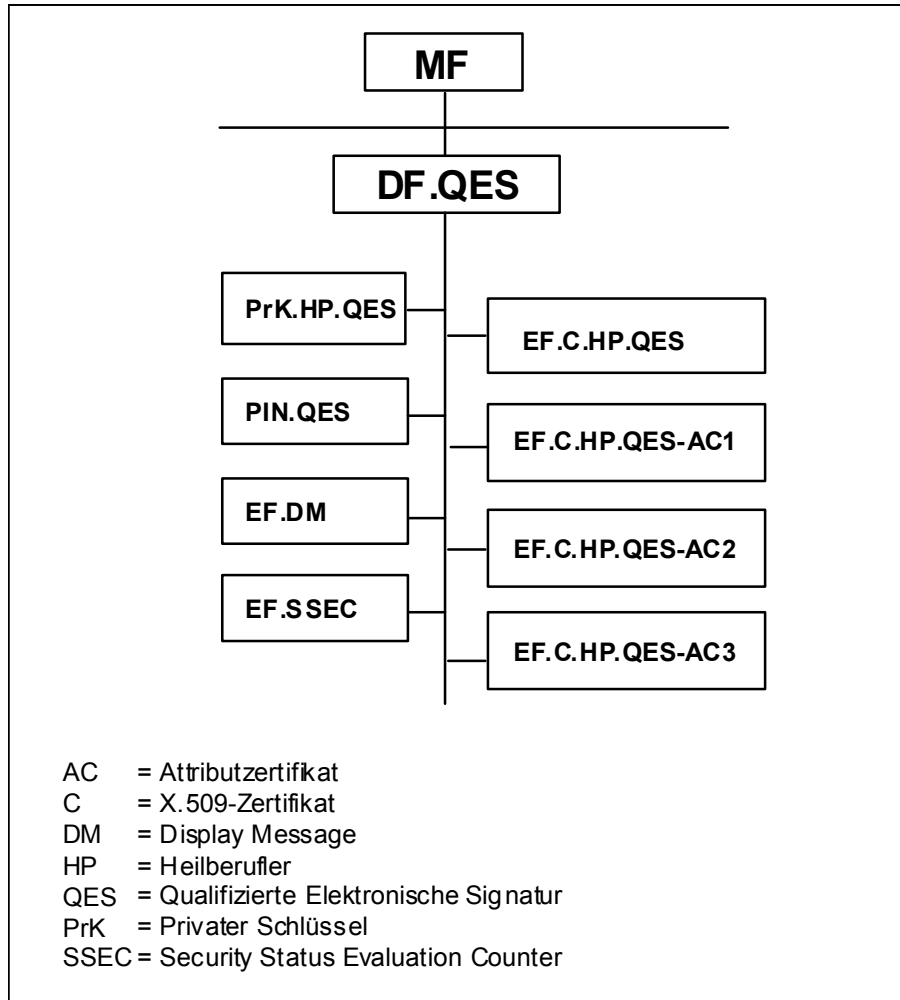


Abbildung 13: Struktur der QES-Anwendung

Das DF.QES wird mit allen in [HBA-P2] festgelegten EFs und mit den definierten Security- und Access-Conditions angelegt. Vom ZDA wird die Anwendung mit Schlüsseln und einem Zertifikat für eine fortgeschrittene Signatur gefüllt.

5.6 DF.CIA.QES und DF.CIA.ESIGN

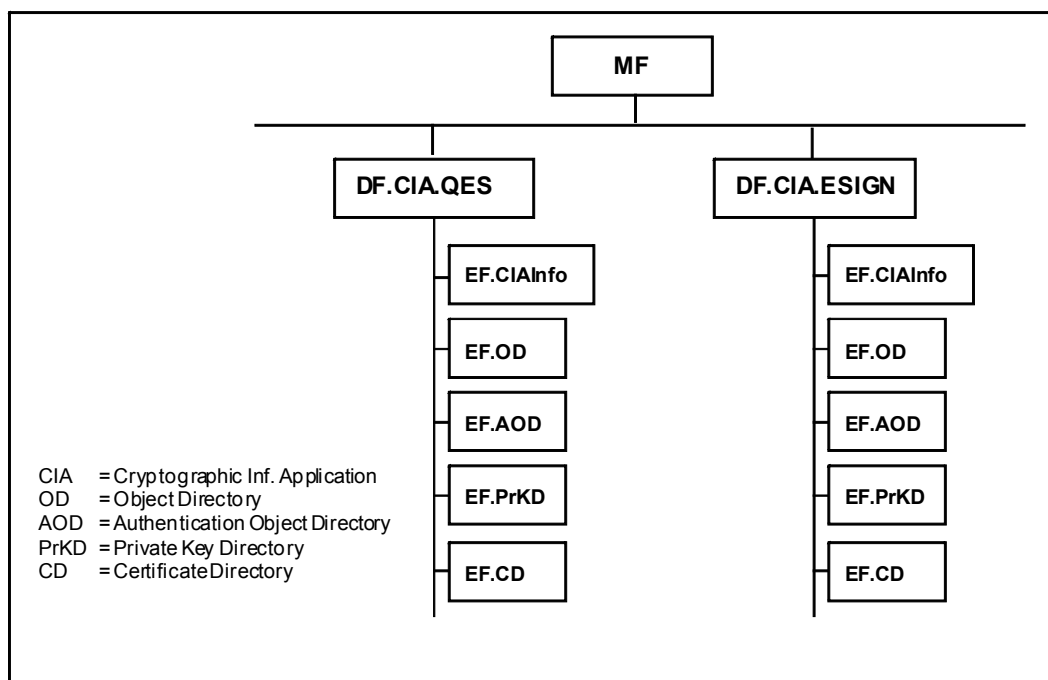


Abbildung 14: Dateistruktur von DF.CIA.QES und DF.CIA.ESIGN

Die in [HBA-P2] festgelegten Parameter für Größe und Zugriffsregeln für DF.CIA.QES und DF.CIA.ESIGN und ihre EFs sind umzusetzen. Die EFs werden entsprechend der Spezifikation gefüllt.

5.7 Erstellung der X.509-Zertifikate

Die Schlüsselpaare für ENC und AUT werden von einem ZDA erzeugt, der auch die zugehörigen Zertifikate in dem in [HBA-P2] und vom jeweiligen Sektor vorgegebenen Format berechnet. Als Schlüssellänge für das RSA-Verfahren werden die in [gemSpecKrypt] festgelegten Werte gefordert

Der Gültigkeitszeitraum kann auf Anforderung des Requestors bei ausgewählten Karten auf eine Woche begrenzt sein. Standardmäßig sollen die Zertifikate 3 Jahre ab Herstellungsdatum gültig sein.

Die zur Personalisierung der Zertifikate notwendigen Daten werden den mitgelieferten Personen-Datensätzen entnommen.

Der Vorgabewert zur Füllung des Feldes "AuthorityInfoAccess" in den Zertifikaten muss in die entsprechenden Datenfelder eingetragen werden und den realen Gegebenheiten bei dem ausstellenden Zertifizierungsdiensteanbieter entsprechen.

Das DF.QES wird mit Schlüsseln und einem Zertifikat (Zertifikatsinhalt gemäß [HBA-P2]) für eine fortgeschrittene Signatur (Gültigkeitsdauer wie bei ENC und AUT) angelegt. Alle X.509-Zertifikate einer Karte (ENC, AUT, SIG und Attributzertifikat) müssen dieselbe Gültigkeitsdauer haben.

5.7.1 Vorgaben für OIDs und ProfessionItem für HBA-Musterkarten

In die X.509-Zertifikate der Musterkarten müssen gemäß den Festlegungen durch die Leistungserbringer-Organisationen und [gemTSL_SP_CP_Test] OIDs und Texte eingetragen werden. In der folgenden Tabelle sind die Referenzbezeichnungen angegeben. Die zugehörigen OIDs/Texte finden sich im Dokument [gemSpec_OID].

Tabelle 3 OID-Referenzen für Musterkarten HBA (verpflichtend)

Speicherort	OID-Referenz
Admission: ProfessionItem und ProfessionOID in den Attributs-Zertifikaten (C.HP.QES/C.HP.SIG, C.HP.AUT, C.HP.ENC) für Ärzte	oid_arzt
Admission: ProfessionItem und ProfessionOID in allen Basis-Zertifikaten (C.HP.QES/C.HP.SIG, C.HP.AUT, C.HP.ENC) für Zahnärzte	oid_zahnarzt
Admission: ProfessionItem und ProfessionOID in allen Basis-Zertifikaten (C.HP.QES/C.HP.SIG, C.HP.AUT, C.HP.ENC) für Apotheker	oid_apotheker
Admission: ProfessionItem und ProfessionOID in allen Basis-Zertifikaten (C.HP.QES/C.HP.SIG, C.HP.AUT, C.HP.ENC) für Psychotherapeuten	oid_psychotherapeut
CertificatePolicies, alle Zertifikate	oid_policy_muster_cp
CertificatePolicies in C.HP.ENC	oid_hba_enc
CertificatePolicies in C.HP.QES-AC1	oid_hba_qes_ac1
CertificatePolicies in C.HP.AUT	oid_hba_aut
CertificatePolicies in C.HP.SIG	oid_hba_sig

5.8 CV-Zertifikate für Musterkarten HBA

Es gelten die Vorgaben aus Abschnitt 4.10.

5.9 Optische Gestaltung der HBA-Musterkarten

Für die äußere Gestaltung der Musterkarten gilt bezüglich der Maße [gemSpec_eGK_P3]. Die optische Gestaltung der Vorderseite ist gemäß folgender Vorlage auszuführen:

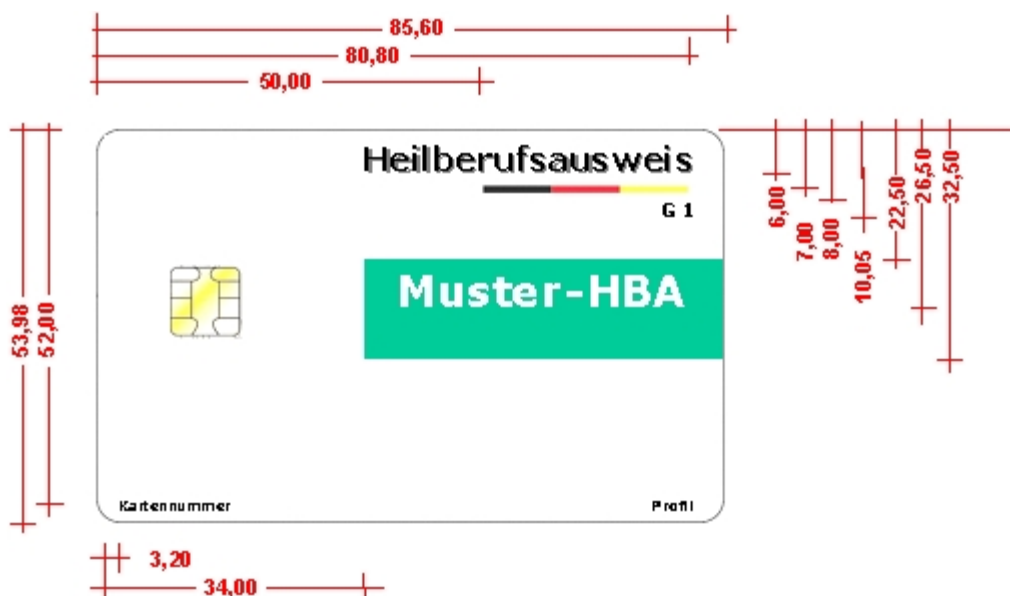


Abbildung 15: Kartenvorderseite, konstante Elemente

Der Muster-HBA ist durch einen auffälligen Farbblock in Türkis (HKS 53) gekennzeichnet. Die Beschriftung „Muster-HBA“ ist in diesem Farbbalken in Verdana True Type fett 22 pt auszuführen, vorzugsweise als Negativdruck. Auch eine Ausführung in Schwarz ist zulässig, wenn die Anfertigung des Negativdrucks unverhältnismäßigen Aufwand verursacht.

In dem Farbblock wird bei der Personalisierung die Rolle des Karteninhabers im Klartext dargestellt in Verdana True Type fett 22 pt, Farbe Schwarz, rechtsbündig zu „Heilberufsausweis“ und „Muster-HBA“.

Der Schriftzug „G 1“ ist in Verdana True Type 6 pt fett, Farbe Schwarz, rechtsbündig zu „Heilberufsausweis“ und dem Block in den nationalen Farben aufzubringen.



Abbildung 16: Kartenvorderseite, Personalisierung

Die Daten zum Heilberufler und zum zugehörigen Profil (Arzt und Zahnarzt = Profil 2, Apotheker = Profil 3, Psychotherapeut = Profil 4) werden dem jeweils verwendeten Datensatz entnommen bzw. implizit nach der jeweils bestellenden Organisation gesetzt.

Für Muster-HBAs ist keine Fotopersonalisierung vorgesehen.

An der Stelle „Muster-Karten-Produzent“ kann der Hersteller der Musterkarten sein Logo einfügen.

Zusätzlich muss das Release im Format x.y.z angegeben werden, für das die Musterkarten hergestellt worden sind. Damit sind auch die jeweiligen Spezifikationsversionen festgelegt. Schrift analog der sonstigen Personalisierung auf der Vorderseite.

Die Kartenrückseite ist weiß.

5.10 An den Kartenhersteller zu liefernde Unterlagen zur Erstellung von HBA-Musterkarten

Die Musterkarten müssen die Herausgeberkennung (Issuer Identifier) in der ICCSN enthalten. Weitere Kodierungen in der ICCSN sind zulässig, solange sie die Eineindeutigkeit nicht beeinträchtigen. Die Kodierung der Herausgeberkennung für Musterkarten ist in Anhang A festgelegt.

Zertifizierungsdiensteanbieter, die HBA-Musterkarten gemäß diesen Vorgaben erstellen wollen, melden dies bei der jeweiligen Leistungserbringer-Organisation an. Daraufhin erhalten diese Kartenhersteller von der jeweiligen Leistungserbringer-Organisation folgende Datensätze:

(1) Auftragsformular mit den für alle Karten geltenden Daten:

- Stückzahl
- spezifische Nummernkreise für die verschiedenen ZDA
- Lieferadresse für die Musterkarten

(2) generierte Datensätze (> der o. g. Stückzahl) mit Muster-Heilberuflerdaten für HBA-Musterkarten einschließlich der impliziten Berufsgruppeninformation im XML-Format.

5.11 Vom ZDA vor Auslieferung der HBA-Musterkarten an die gematik zu liefernde Daten

ZDAs, die HBA-Musterkarten gemäß dieser Vorgaben erstellen wollen, müssen gemäß dem Dokument „PKI für X.509-Zertifikate: Registrierung eines Trust Service Provider (TSP)“ [gemX.509_TSP] bei der gematik als zugelassene CA registriert sein und die zu registrierenden Zertifikate an die gematik zum Eintrag in die Test-TSL liefern [gemX.509_TSP#4.3.1].

Die Abfrage der Gültigkeit der X.509-Zertifikate HBA-Musterkarten muss über einen vom ausgebenden ZDA betriebenen Verzeichnisdienst möglich sein.

6 Vorgaben für Musterkarten SMC Typ A

Die Musterkarten müssen alle Vorgaben der SMC-Spezifikation erfüllen. Dies betrifft sowohl die Bereitstellung der definierten Kommandos [HBA-P1] als auch die Einrichtung der definierten File-Struktur [HBA-P3].

6.1 PIN- und PUK-Werte

Für die SMC-A ist ab Release 2.3.2 keine PIN-Freischaltung zugelassen.

6.2 MF

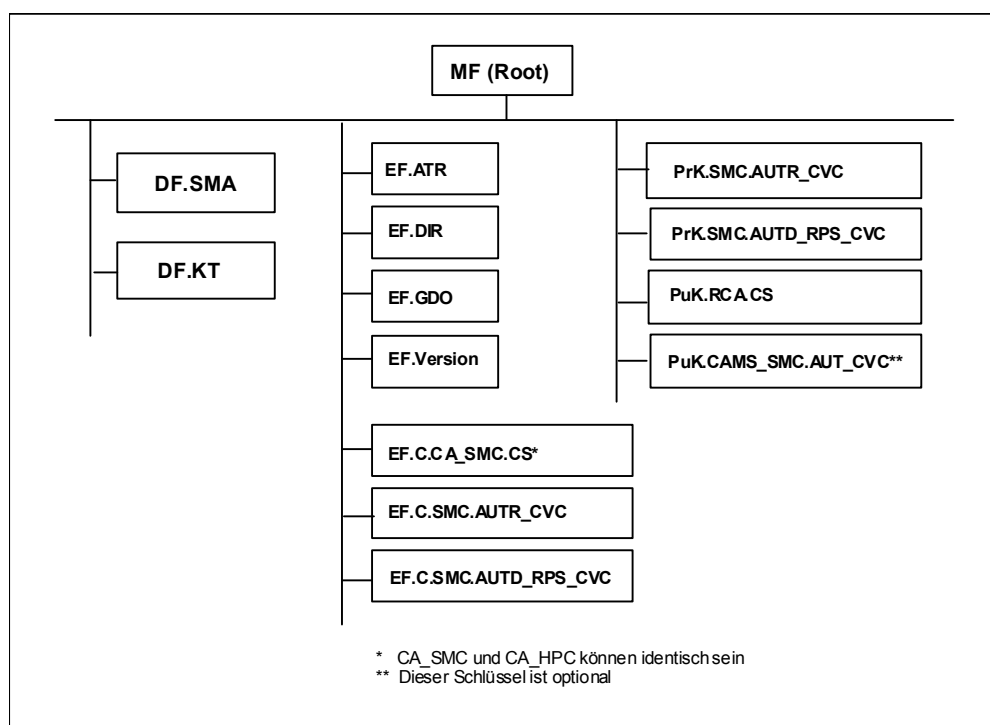


Abbildung 17: Prinzipielle Dateistruktur der SMC-A

Die in [HBA-P3] festgelegten Parameter für Größe und Zugriffsregeln für das MF und die zugehörigen EFs sind umzusetzen. Die EFs und die zusätzlichen Schlüsselfiles werden entsprechend der Spezifikation mit den angelieferten bzw. beim Kartenhersteller erzeugten Daten gefüllt.

6.3 DF.SMA

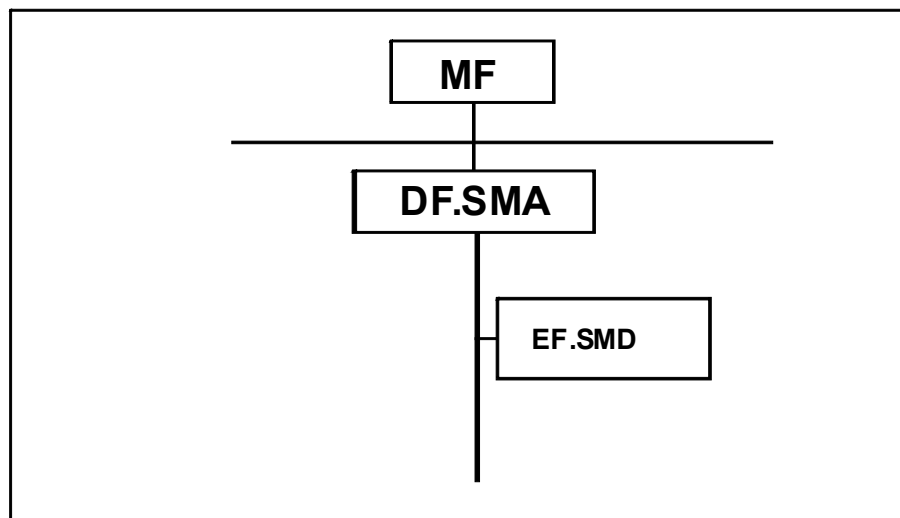


Abbildung 18: Dateistruktur von DF.SMA einer SMC-A

Die in [HBA-P3] festgelegten Parameter für Größe und Zugriffsregeln für das DF.SMA und seine EFs sind umzusetzen. Die EFs werden entsprechend der Spezifikation mit den angelieferten bzw. beim Kartenhersteller erzeugten Daten gefüllt.

6.4 DF.KT

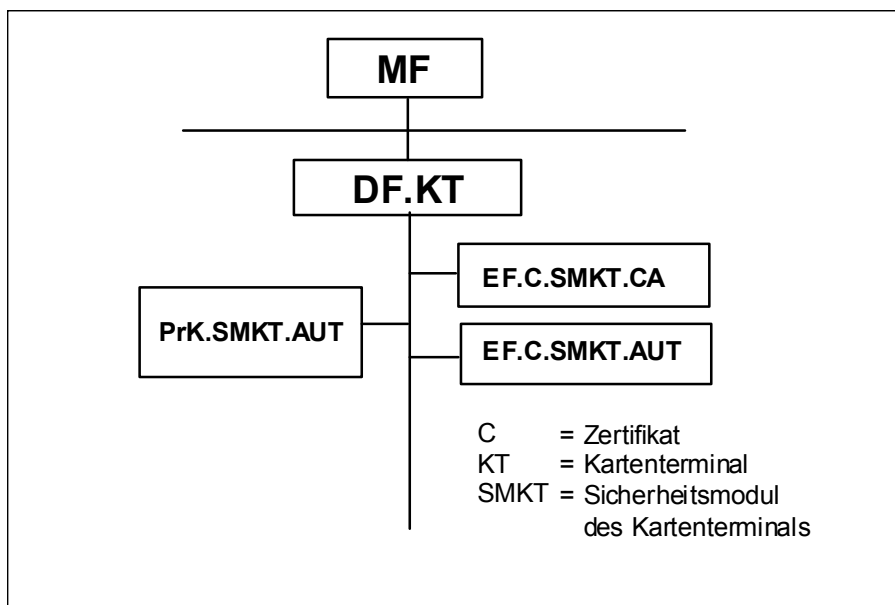


Abbildung 19: Dateistruktur von DF.KT

Die in [HBA-P3] festgelegten Parameter für Größe und Zugriffsregeln für das DF.KT und seine EFs sind umzusetzen. Die EFs werden entsprechend der Spezifikation mit den angelieferten bzw. beim Kartenhersteller erzeugten Daten gefüllt.

6.5 Erstellung des X.509-Zertifikats

Das Schlüsselpaar für SMKT-AUT wird vom Kartenhersteller oder von einer vom Kartenherausgeber beauftragten CA erzeugt, dabei wird auch das zugehörnde Zertifikat in dem in [gemPKI_KT] vorgegebenen Format berechnet. Als Schlüssellängen für das RSA-Verfahren werden die in [gemSpecKrypt] festgelegten Werte gefordert

Als Gültigkeitszeitraum soll bei 10% der Karten eine Woche, bei den restlichen 90% 1 Jahr ab Herstellungsdatum eingetragen werden.

6.5.1 OID-Vorgaben für SMC-A-Musterkarten

In das X.509-Zertifikat der Musterkarten müssen OIDs eingetragen werden. In der folgenden Tabelle sind die Referenzbezeichnungen angegeben. Die zugehörigen OIDs/Texte finden sich im Dokument [gemSpec_OID].

Tabelle 4 OID-Referenzen für Musterkarten SMC-B (verpflichtend)

Speicherort	OID-Referenz
Admission: ProfessionItem und ProfessionOID im Zertifikat C.SMKT.AUT	oid_kt
CertificatePolicies, im Zertifikat C.SMKT.AUT	oid_policy_muster_cp
CertificatePolicies in C.SMKT.AUT	oid_smkt_aut

6.6 CV-Zertifikate für Musterkarten SMC-Typ A

Es gelten die Vorgaben aus Kapitel 4.10.

6.7 Optische Gestaltung der Musterkarten für SMC Typ A

Für die äußere Gestaltung der Musterkarten gilt bezüglich der Maße [gemSpec_eGK_P3]. Die optische Gestaltung der Vorderseite ist gemäß folgender Vorlage auszuführen:

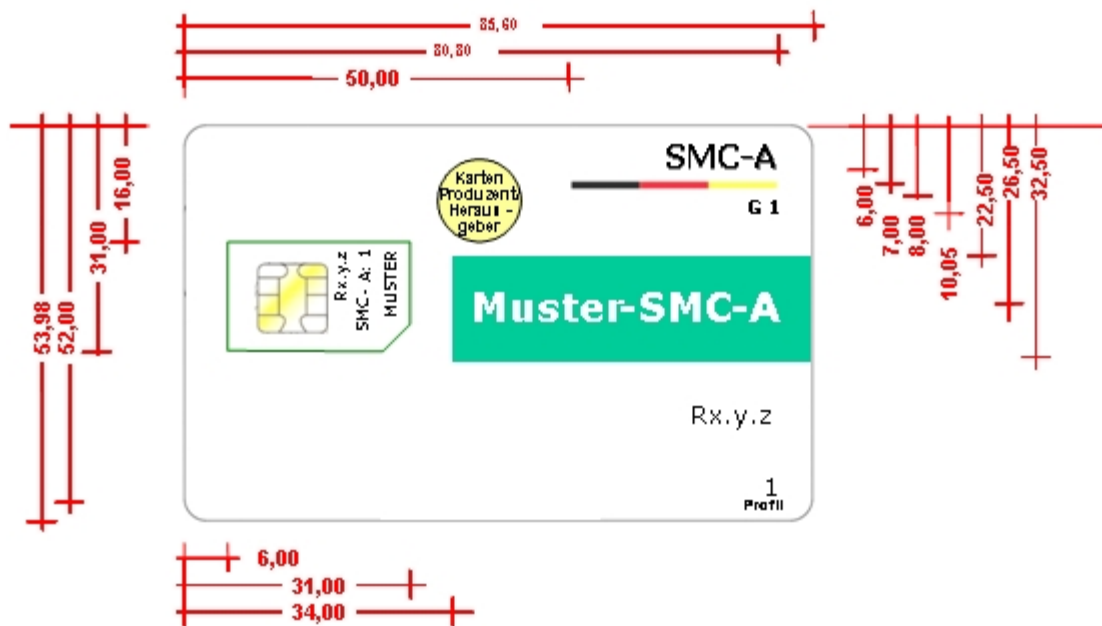


Abbildung 20: Kartenvorderseite SMC Typ A

Die Muster-SMC ist durch einen auffälligen Farbblock in Türkis (HKS 53) gekennzeichnet. Die Beschriftung „Muster-SMC-A“ ist in diesem Farbbalken in Verdana True Type fett 22 pt auszuführen, vorzugsweise als Negativdruck. Auch eine Ausführung in Schwarz ist zulässig, wenn die Anfertigung des Negativdrucks unverhältnismäßigen Aufwand verursacht.

Der Schriftzug „G 1“ ist in Verdana True Type 6 pt fett, Farbe Schwarz, rechtsbündig zu „SMC-A“ und dem Block in den nationalen Farben aufzubringen.

An der Stelle „Muster-Karten-Produzent“ kann der Hersteller der Musterkarten sein Logo einfügen.

Zusätzlich muss das Release im Format x.y.z angegeben werden, für das die Musterkarten hergestellt worden sind. Damit sind auch die jeweiligen Spezifikationsversionen festgelegt. Schrift analog der sonstigen Personalisierung auf der Vorderseite.

Auf der Vorderseite ist in dem als ID-00-Format verbleibenden Ausschnitt in Verdana True Type 8 pt „Muster-SMC-A“ analog Abbildung 20 (Information über Zugehörigkeit zu Generation 1 (G 1), Release, Typ, Profil und Zusatz: Muster) aufzubringen.

Auf der Rückseite ist in dem als ID-00-Format verbleibenden Ausschnitt in Verdana True Type 8 pt „A“ und das Profil und die Zugehörigkeit zur Generation 1 (G 1) sowie in einer zweiten Zeile eine Kodierung für Hersteller, Version und laufende Nummer analog Abbildung 21 aufzubringen. Die Art der Kodierung bleibt dem Hersteller überlassen.

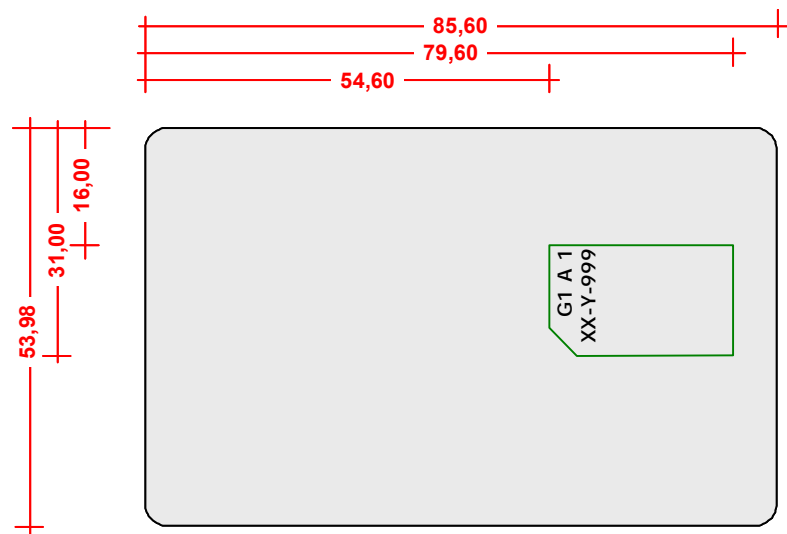


Abbildung 21: Kartenrückseite SMC Typ A mit Kodierung

6.8 An den Kartenhersteller zu liefernde Unterlagen zur Erstellung von SMC Typ A-Musterkarten

Die Musterkarten müssen die Herausgeberkennung (Issuer Identifier) in der ICCSN enthalten. Weitere Kodierungen in der ICCSN sind zulässig, solange sie die Eineindeutigkeit nicht beeinträchtigen. Die Kodierung der Herausgeberkennung für Musterkarten ist in Anhang A festgelegt.

Kartenhersteller, die SMC Typ A-Musterkarten gemäß diesen Vorgaben erstellen wollen, melden dies bei der jeweiligen Leistungserbringer-Organisation an. Daraufhin erhalten diese Kartenhersteller von der jeweiligen Leistungserbringer-Organisation folgende Datensätze:

(1) Auftragsformular mit den für alle Karten geltenden Daten:

- Gesamt-Stückzahl
- Vorgaben für die Festlegung der ICCSN
- Lieferadresse für die Musterkarten

(2) Vorgabe für das für die Lieferung geltende Profil.

6.9 Vor Auslieferung der SMC-A-Musterkarten

CAs, die SMC-A-Musterkarten mit einem Zertifikat C.SMKT.AUT gemäß dieser Vorgaben erstellen wollen, müssen gemäß dem Dokument [gemPKI_KT] „PKI für die X.509-Zertifikate der Identitäten der eHealth-Kartenterminals – Lastenheft“ bei der gematik als zugelassene Test-CA registriert sein und dabei die zu registrierenden Test-CA-Zertifikate vor Auslieferung der Musterkarten an die gematik zum Eintrag in die Test-TCL liefern.

Ein OCSP-Dienst wird für diese Zertifikate nicht benötigt.

7 Vorgaben für Musterkarten SMC Typ B

Die Musterkarten müssen alle Vorgaben der SMC-Spezifikation erfüllen. Dies betrifft sowohl die Bereitstellung der definierten Kommandos [HBA-P1] als auch die Einrichtung der definierten File-Struktur [HBA-P3]. Insbesondere müssen DF.ESIGN und DF.SMA mit der kompletten Unterstruktur und mit den definierten Security- und Access-Conditions angelegt werden (siehe Abbildungen 21 bis 23).

7.1 PIN- und PUK-Werte

7.1.1 Feste PIN-Werte

Die PIN-Werte MÜSSEN einheitlich auf den Wert 123456 gesetzt werden (Ausnahme siehe 7.1.2).

Die zugehörigen PUK-Werte MÜSSEN einheitlich auf den Wert 12345678 gesetzt werden.

7.1.2 Transport-PIN-Werte

Es KÖNNEN Musterkarten mit den in der Spezifikation zugelassenen Transport-PIN-Verfahren geliefert werden. Die Anzahl der mit den zugelassenen Transport-PIN-Verfahren zu liefernden Musterkarten muss mit der gematik abgestimmt werden.

7.2 MF

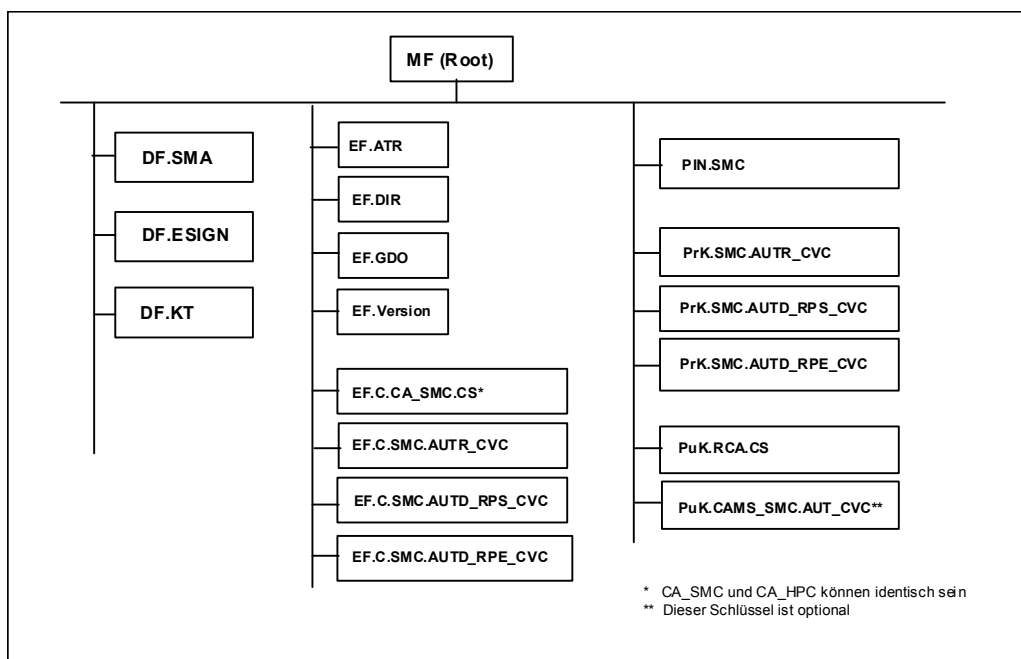


Abbildung 22: Prinzipielle Struktur der SMC-B

Die in [HBA-P3] festgelegten Parameter für Größe und Zugriffsregeln für das MF und die zugehörigen EFs sind umzusetzen. Die EFs und die zusätzlichen Schlüsselfiles werden entsprechend der Spezifikation mit den angelieferten bzw. beim Kartenhersteller erzeugten Daten gefüllt.

7.3 DF.SMA

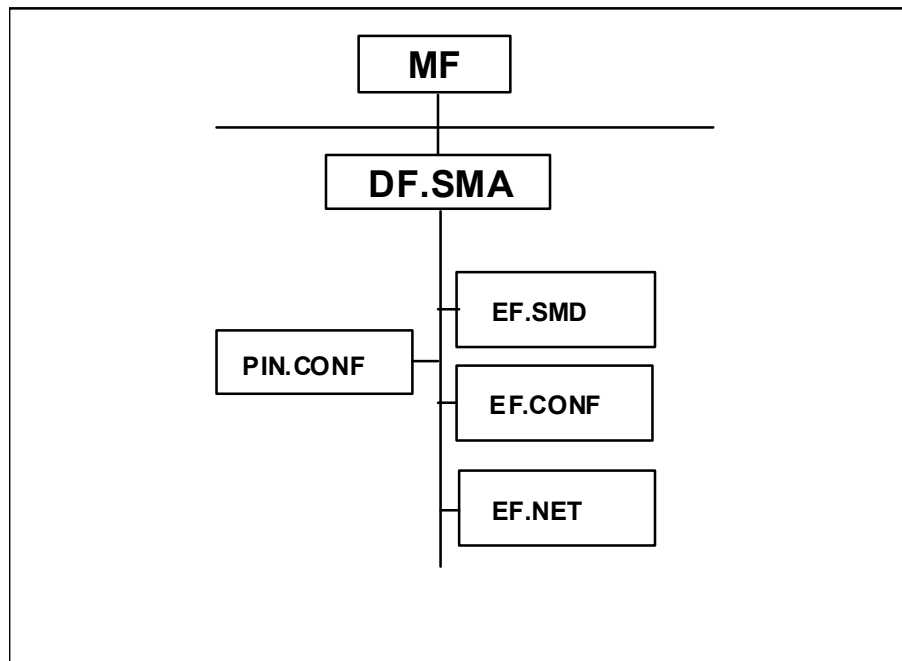


Abbildung 23: Prinzipielle Struktur von DF.SMA einer SMC-B

Die in [HBA-P3] festgelegten Parameter für Größe und Zugriffsregeln für das DF.SMA und seine EFs sind umzusetzen. Die EFs werden entsprechend der Spezifikation mit Daten gefüllt.

7.4 DF.KT

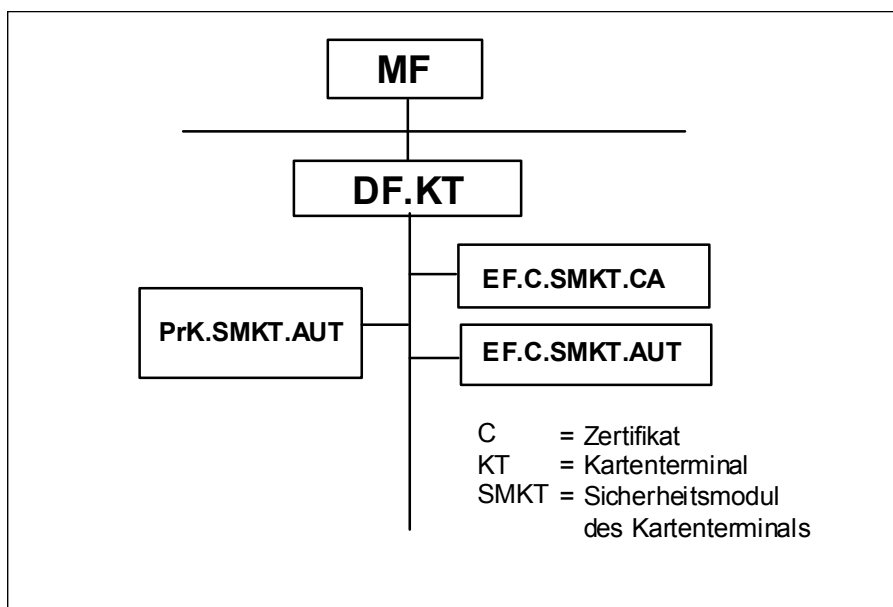


Abbildung 24: Dateistruktur von DF.KT

Die in [HBA-P3] festgelegten Parameter für Größe und Zugriffsregeln für das DF.KT und seine EFs sind umzusetzen. Die EFs werden entsprechend der Spezifikation mit den angelieferten bzw. beim Kartenhersteller erzeugten Daten gefüllt.

7.5 DF.ESIGN

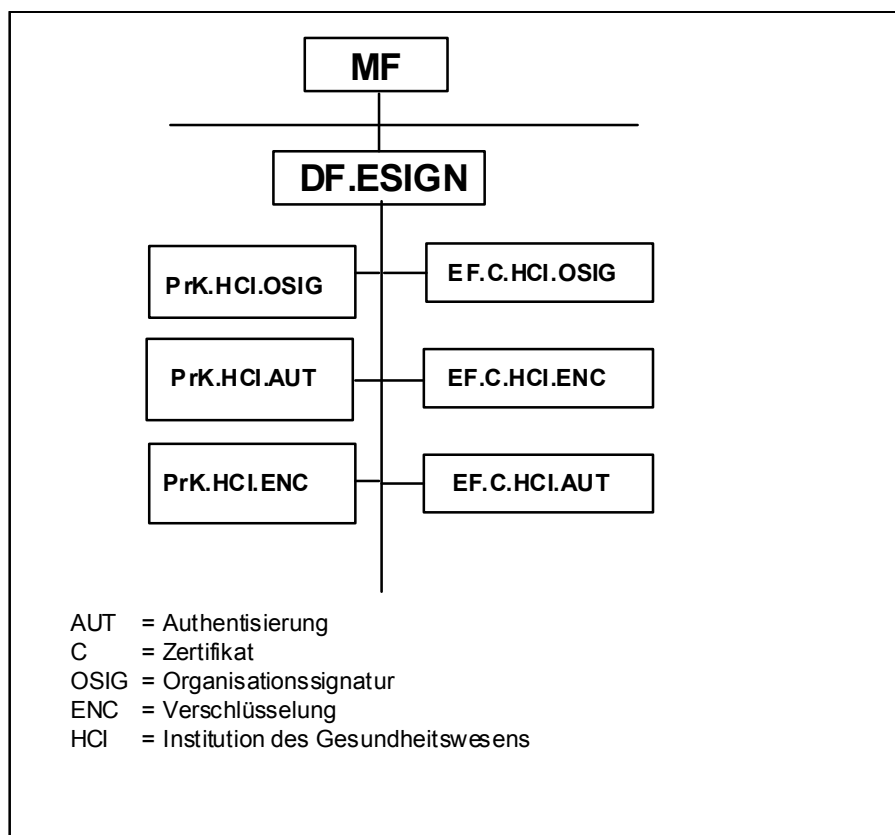


Abbildung 25: Struktur von DF.ESIGN

Die in [HBA-P3] festgelegten Parameter für Größe und Zugriffsregeln für das DF.ESIGN und seine EFs sind umzusetzen. Die EFs und die zusätzlichen Schlüsselfiles werden entsprechend der Spezifikation mit den angelieferten bzw. beim Kartenhersteller erzeugten Daten gefüllt.

7.6 Erstellung der X.509-Zertifikate

Die Schlüsselpaare für ENC, AUT, OSIG und SMKT-AUT werden vom Kartenhersteller oder von einer vom Kartenherausgeber beauftragten CA erzeugt, dabei werden auch die zugehörigen Zertifikate in dem in [gemX.509_SMCB] bzw. [gemPKI_KT] vorgegebenen Format berechnet. Als Schlüssellängen für das RSA-Verfahren werden die in [gemSpecKrypt] festgelegten Werte gefordert

Als Gültigkeitszeitraum soll bei 10% der Karten eine Woche, bei den restlichen 90% 1 Jahr ab Herstellungsdatum eingetragen werden.

Die zur Individualisierung der Zertifikate notwendigen Daten werden den mitgelieferten Datensätzen entnommen.

Der Vorgabewert zur Füllung des Feldes "AuthorityInfoAccess" in den Zertifikaten muss in das entsprechende Datenfeld eingetragen werden und den realen Gegebenheiten bei der

ausstellenden CA entsprechen. Falls der OCSP-Dienst der gematik für OCSP-Abfragen genutzt werden soll, müssen Daten gemäß Kapitel 7.11 für die SMC-B an die gematik geliefert werden.

7.6.1 OID-Vorgaben für SMC-B-Musterkarten

In die X.509-Zertifikate der Musterkarten müssen gemäß [gemX.509_SMCB], [gemTSL_SP_CP_Test] und [gemPKI_KT] OIDs eingetragen werden. In der folgenden Tabelle sind die Referenzbezeichnungen angegeben. Die zugehörigen OIDs/Texte finden sich im Dokument [gemSpec_OID].

Tabelle 5 OID-Referenzen für Musterkarten SMC-B (verpflichtend)

Speicherort	OID-Referenz
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.HCI.OSIG, C.HCI.AUT, C.HCI.ENC) für Praxen Ärzte	oid_praxis_arzt
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.HCI.OSIG, C.HCI.AUT, C.HCI.ENC) für Praxen Zahnärzte	oid_zahnarztpraxis
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.HCI.OSIG, C.HCI.AUT, C.HCI.ENC) für Praxen Psychotherapeuten	oid_praxis_psychotherapeut
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.HCI.OSIG, C.HCI.AUT, C.HCI.ENC) für Apotheken	oid_öffentliche_apotheke
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.HCI.OSIG, C.HCI.AUT, C.HCI.ENC) für Krankenhäuser	oid_krankenhaus
Admission: ProfessionOID im Zertifikat C.SMKT.AUT	oid_kt
CertificatePolicies, in allen Zertifikaten (C.HCI.OSIG, C.HCI.AUT, C.HCI.ENC, C.SMKT.AUT)	oid_policy_muster_cp
CertificatePolicies in C.HCI.ENC	oid_smc_b_enc
CertificatePolicies in C.HCI.AUT	oid_smc_b_aut
CertificatePolicies in C.HCI.OSIG	oid_smc_b_osig
CertificatePolicies in C.SMKT.AUT	oid_smkt_aut

7.7 CV-Zertifikate für Musterkarten SMC-Typ B

Es gelten die Vorgaben aus Abschnitt 4.10.

7.8 Optische Gestaltung der Musterkarten für SMC Typ B

Für die äußere Gestaltung der Musterkarten gilt bezüglich der Maße [gemSpec_eGK_P3]. Die optische Gestaltung der Vorderseite ist gemäß folgender Vorlage auszuführen:

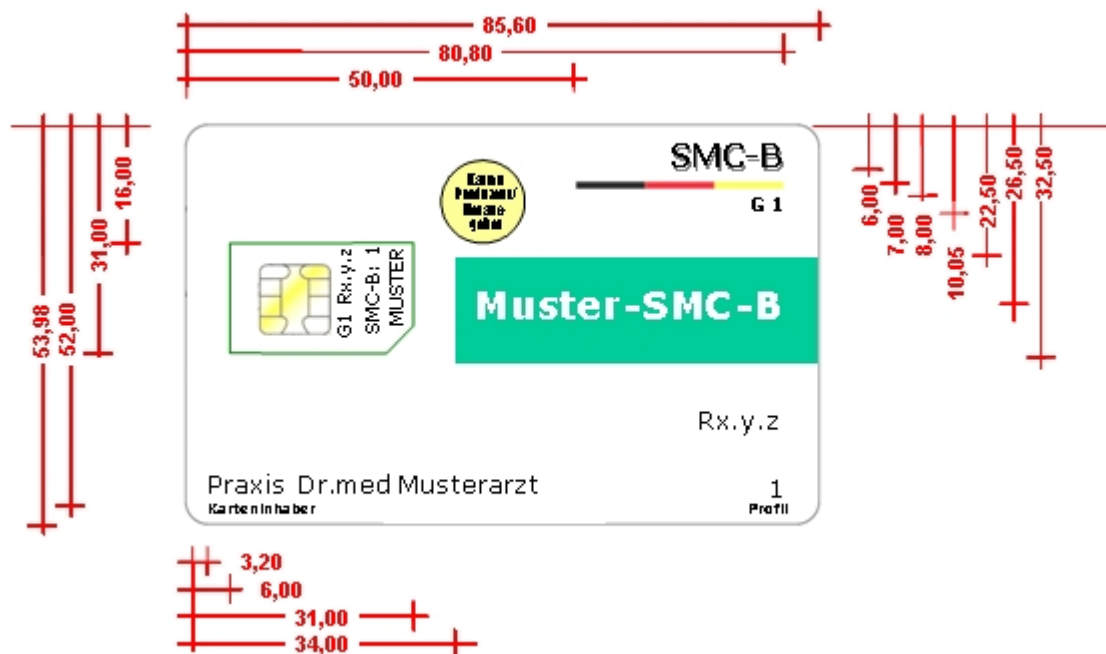


Abbildung 26: Kartenvorderseite SMC Typ B mit Institutionsbezeichnung

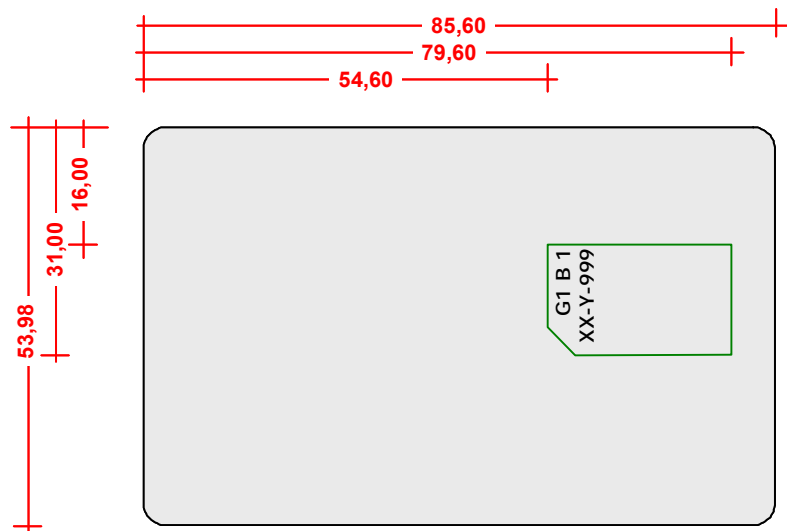


Abbildung 27: Kartenrückseite SMC Typ B mit Kodierung

Die Daten zur Institution und zum dazugehörigen Profil werden dem jeweils verwendeten Datensatz entnommen.

An der Stelle „Muster-Karten-Produzent“ kann der Hersteller der Musterkarten sein Logo einfügen.

Zusätzlich muss das Release im Format x.y.z angegeben werden, für das die Musterkarten hergestellt worden sind. Damit sind auch die jeweiligen Spezifikationsversionen festgelegt. Schrift analog der sonstigen Personalisierung auf der Vorderseite.

Die Muster-SMC ist durch einen auffälligen Farbblock in Türkis (HKS 53) gekennzeichnet. Die Beschriftung „Muster-SMC-B“ ist in diesem Farbbalken in Verdana True Type fett 22 pt auszuführen, vorzugsweise als Negativdruck. Auch eine Ausführung in Schwarz ist zulässig, wenn die Anfertigung des Negativdrucks unverhältnismäßigen Aufwand verursacht.

Der Schriftzug „G 1“ ist in Verdana True Type 6 pt fett, Farbe Schwarz, rechtsbündig zu „SMC-B“ und dem Block in den nationalen Farben aufzubringen.

Auf der Vorderseite ist in dem als ID-00-Format verbleibenden Ausschnitt in Verdana True Type 8 pt „Muster-SMC-A“ analog Abbildung 26 (Information über Zugehörigkeit zu Generation 1 (G 1), Release, Typ, Profil und Zusatz: Muster) aufzubringen.

Auf der Rückseite ist in dem als ID-00-Format verbleibenden Ausschnitt in Verdana True Type 8 pt „A“ und das Profil und die Zugehörigkeit zur Generation 1 (G 1) sowie in einer zweiten Zeile eine Kodierung für Hersteller, Version und laufende Nummer analog Abbildung 27 aufzubringen. Die Art der Kodierung bleibt dem Hersteller überlassen.

7.9 An den Kartenhersteller zu liefernde Unterlagen zur Erstellung von SMC-Typ B-Musterkarten

Die Musterkarten müssen die Herausgeberkennung (Issuer Identifier) in der ICCSN enthalten. Weitere Kodierungen in der ICCSN sind zulässig, solange sie die Eineindeutigkeit nicht beeinträchtigen. Die Kodierung der Herausgeberkennung für Musterkarten ist in Anhang A festgelegt.

Kartenhersteller, die SMC-Typ B-Musterkarten gemäß dieser Vorgaben erstellen wollen, melden dies bei der jeweiligen Leistungserbringer-Organisation an. Daraufhin erhalten diese Kartenhersteller von der jeweiligen Leistungserbringer-Organisation folgende Datensätze:

(1) Auftragsformular mit den für alle Karten geltenden Daten:

- Stückzahl
- Vorgaben zur Füllung des Feldes "AuthorityInfoAccess". Diese müssen eingesetzt werden, falls der OCSP-Dienst der gematik genutzt werden soll. Sonst sind die entsprechenden Daten des OCSP-Dienstes des herausgebenden ZDA/der herausgebenden CA zu verwenden.
- Vorgaben für die Festlegung der ICCSN
- Lieferadresse für die Musterkarten

(2) Datensätze mit Muster-Institutionsdaten zur Erzeugung der X.509-Zertifikate (Zahl der Datensätze entspricht der geforderten Stückzahl) im XML-Format. In diesen Datensätzen ist auch das jeweilige Profil für die CV-Zertifikate enthalten.

7.10 Vom ZDA/von der CA an die gematik zu liefernde Daten

7.10.1 Vor Auslieferung der SMC-B-Musterkarten

7.10.1.1 X.509-Zertifikate AUT, ENC und OSIG

CAs, die SMC-B-Musterkarten gemäß dieser Vorgaben erstellen wollen, müssen für die Zertifikate AUT, ENC und OSIG gemäß dem Dokument [gemX.509_TSP] „PKI für X.509-Zertifikate: Registrierung eines Trust Service Provider (TSP)“ bei der gematik als zugelassene CA registriert sein und die zu registrierenden Zertifikate gemäß Kapitel 4.3.1 in [gemX.509_TSP] vor Auslieferung der Musterkarten an die gematik zum Eintrag in die Test-TSL liefern.

Die Abfrage der Gültigkeit der X.509-Zertifikate der SMC-B-Musterkarten muss über einen von der ausgebenden CA betriebenen Verzeichnisdienst möglich sein, falls der OCSP-Dienst der gematik nicht genutzt wird.

7.10.1.2 X.509-Zertifikate SMKT.AUT

CAs, die SMC-A-Musterkarten mit einem Zertifikat C.SMKT.AUT gemäß dieser Vorgaben erstellen wollen, müssen gemäß dem Dokument [gemPKI_KT] „PKI für die X.509-Zertifikate der Identitäten der eHealth-Kartenterminals – Lastenheft“ bei der gematik als zugelassene Test-CA registriert sein und dabei die zu registrierenden Test-CA-Zertifikate vor Auslieferung der Musterkarten an die gematik zum Eintrag in die Test-TCL liefern.

Ein OCSP-Dienst wird für diese Zertifikate nicht benötigt.

7.11 Vom Kartenhersteller nach Erstellung der SMC-Typ B-Musterkarten an die gematik zu liefernde Daten

Dieser Abschnitt gilt nur, falls der OCSP-Dienst der gematik genutzt werden soll.

Kartenhersteller, die SMC-Typ B-Musterkarten gemäß dieser Vorgaben erstellt haben und den OCSP-Dienst der gematik nutzen wollen, müssen folgende Daten an die gematik zurückliefern:

- (1) X.509-Zertifikate (ENC, AUT, OSIG) aller erstellten Musterkarten im Format .cer. Bei größerer Anzahl erstellter Zertifikate (>25) sollen die Zertifikate in einer Datei gezippt werden. Im CommonName des SubjectDN soll der Firmenname des Herstellers als Unterscheidungskriterium enthalten sein.
- (2) Zu den eigentlichen Zertifikaten ist eine Liste beizufügen, die zu jedem erzeugten Zertifikat Dateinamen, den CommonName und die Zertifikatsseriennummer enthält.
- (3) Das CA-Zertifikat der CA, mit der die Versichertenzertifikate erstellt wurden, mit dem dazugehörige Schlüsselpaar (öffentlicher und privater Schlüssel) im Format PKCS#12. Der Aufbau der CA-Zertifikate MUSS ISIS-MTT-konform sein. Im Zertifikat der CA MUSS der Wert ca=true in den BasicConstraints eingetragen werden (siehe Tabelle 2). Als Verwendungszweck (Key Usage) MUSS neben „keyCert-Sign“ auch „crlSign“ eingetragen sein. Das Passwort für die PKCS#12-Datei soll einheitlich auf den Wert „Musterkarte“ gesetzt sein.

Tabelle 6 Auszug aus [ISIS-MTT Part 1], Table 18

#	ASN.1 DEFINITION	SEMANTICS	SUPPORT		REFERENCES		NOTES
			GEN CA/EE CERT	PROC	RFC3280	ISISMTT	
1	BasicConstraints ::= SEQUENCE {	Indicates a CA certificate and defines how deep a certificate may exist below that CA.	++/+-	++	4.2.1.10		[1]
2	ca BOOLEAN DEFAULT FALSE,	ca=TRUE indicates a CA certificate ca=FALSE indicates an end entity					
3	pathLenConstraint INTEGER (0..MAX) OPTIONAL }	only meaningful if ca=TRUE, indicates how many CA certificates may be included in the certification path below this CA. That is, pathLenConstraint=0 indicates that only end entity certificates may follow in the path. If this field does not appear, there is no limit to the path length.					
[1]	[RFC3280] This extension MUST appear as a critical extension in all CA certificates that contain public keys used to validate digital signatures on certificates. This extension MAY appear as a critical or non-critical extension in CA certificates that contain public keys used exclusively for purposes other than validating digital signatures on certificates. Such CA certificates include ones that contain public keys used exclusively for validating digital signatures on CRLs and ones that contain key management public keys used with certificate enrollment protocols. This extension MAY appear as a critical or non-critical extension in end entity certificates. ISIS-MTT PROFILE: This extension MAY appear in end entity certificates and MUST appear in CA certificates. It MUST be marked critical.						

8 Vorgaben für Musterkarten SMC-K

Die Musterkarten müssen alle Vorgaben der SMC-K-Spezifikation [gemSpec_SMC-K] erfüllen. Dies betrifft sowohl die Bereitstellung der definierten Kommandos als auch die Einrichtung der definierten File-Struktur. Insbesondere müssen DF.NK, DF.AK und DF.SAK mit der kompletten Unterstruktur und mit den definierten Security- und Access-Conditions angelegt werden (siehe Abbildungen 23 bis 25).

8.1 MF

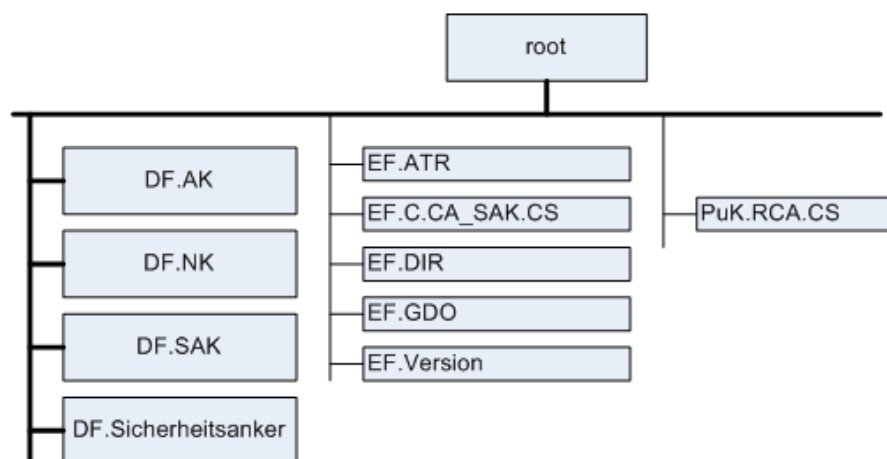


Abbildung 28: Dateistruktur einer SMC-K auf oberster Ebene

Die in [gemSpec_SMC-K] festgelegten Parameter für Größe und Zugriffsregeln für das MF und die zugehörigen EFs sind umzusetzen. Die EFs und die zusätzlichen Schlüsselfiles werden entsprechend der Spezifikation mit den angelieferten bzw. beim Kartenhersteller erzeugten Daten gefüllt.

8.2 DF.AK

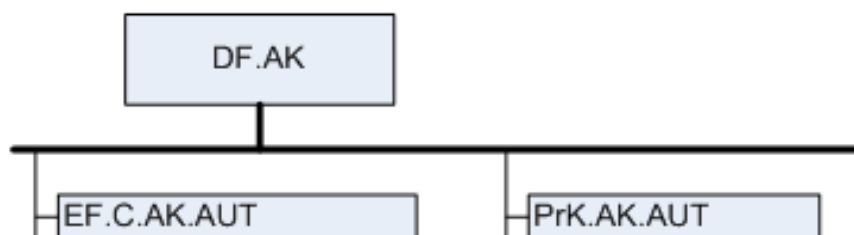


Abbildung 29 Dateistruktur der Anwendung DF.AK

Die in [gemSpec_SMC-K] festgelegten Parameter für Größe und Zugriffsregeln für das DF.AK und seine EFs sind umzusetzen. Die EFs werden entsprechend der Spezifikation mit Daten gefüllt.

8.3 DF.NK

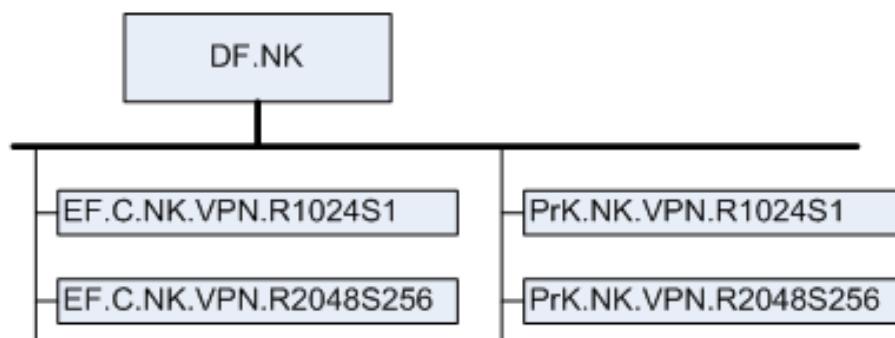


Abbildung 30 Dateistruktur der Anwendung DF.NK

Die in [gemSpec_SMC-K] festgelegten Parameter für Größe und Zugriffsregeln für das DF.NK und seine EFs sind umzusetzen. Die EFs und die zusätzlichen Schlüsselfiles werden entsprechend der Spezifikation mit den angelieferten bzw. beim Kartenhersteller erzeugten Daten gefüllt.

8.4 DF.SAK

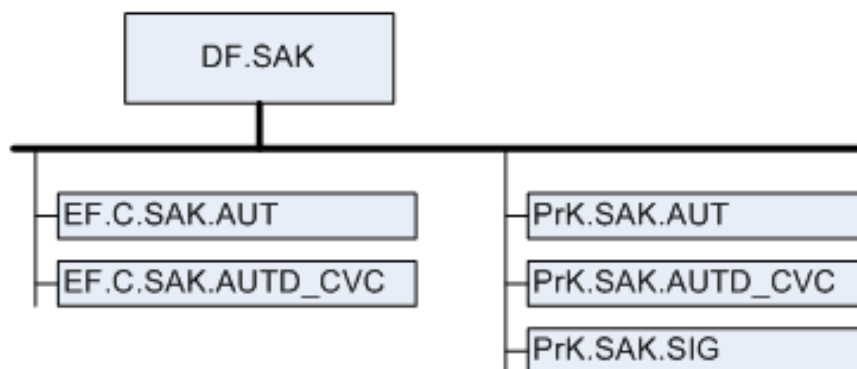


Abbildung 31: Dateistruktur der Anwendung DF.SAK

Die in [gemSpec_SMC-K] festgelegten Parameter für Größe und Zugriffsregeln für das DF.SAK und seine EFs sind umzusetzen. Das EF und das zusätzliche Schlüsselfile werden entsprechend der Spezifikation mit den angelieferten bzw. beim Kartenhersteller erzeugten Daten gefüllt.

8.5 DF.Sicherheitsanker

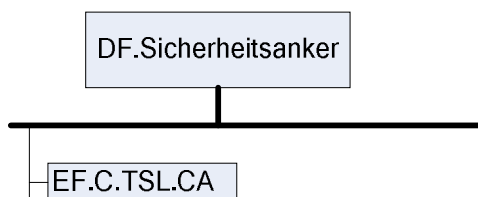


Abbildung 32: Dateistruktur der Anwendung DF.Sicherheitsanker

Die in [gemSpec_SMC-K] festgelegten Parameter für Größe und Zugriffsregeln für das DF.Sicherheitsanker und sein EF sind umzusetzen. Das EF wird entsprechend der Spezifikation mit den angelieferten bzw. beim Kartenhersteller erzeugten Daten gefüllt.

8.6 Erstellung der X.509-Zertifikate

Die X.509-Schlüsselpaare mit den in [gemSpecKrypt] festgelegten Schlüssellängen und die Zertifikate der jeweiligen CA werden vom Kartenhersteller oder von einer vom Kartenherausgeber beauftragten CA erzeugt, dabei werden auch die zugehörigen Zertifikate in dem in [gemX.509_Kon] vorgegebenen Format berechnet.

Als Gültigkeitszeitraum soll bei 10% der Karten eine Woche, bei den restlichen 90% 1 Jahr ab Herstellungsdatum eingetragen werden.

Der Vorgabewert zur Füllung des Feldes "AuthorityInfoAccess" in dem Zertifikat C.NK.AUT muss in das entsprechende Datenfeld eingetragen werden und den realen Gegebenheiten bei der ausstellenden CA entsprechen. Falls der OCSP-Dienst der gematik für OCSP-Abfragen genutzt werden soll, müssen Daten gemäß Kapitel 8.13 für die SMC-K an die gematik geliefert werden.

Für die X.509-Zertifikate in DF.AK und DF.SAK muss kein OCSP-Dienst installiert werden.

8.6.1 OID-Vorgaben für SMC-K-Musterkarten

In die X.509-Zertifikate der Musterkarten müssen gemäß [gemX.509_Kon] und [gemTSL_SP_CP_Test] OIDs eingetragen werden. In der folgenden Tabelle sind die Referenzbezeichnungen angegeben. Die zugehörigen OIDs/Texte finden sich im Dokument [gemSpec_OID].

Tabelle 7 OID-Referenzen für Musterkarten SMC-K (verpflichtend)

Speicherort	OID-Referenz
Admission: ProfessionItem und ProfessionOID in den Zertifikaten des DF.NK	oid_nk

Speicherort	OID-Referenz
Admission: ProfessionItem und ProfessionOID in den Zertifikaten des DF.AK	oid_ak
CertificatePolicies für alle Zertifikate	oid_policy_muster_cp
CertificatePolicies in C.AK.AUT	oid_ak_aut
CertificatePolicies in C.NK.VPN	oid_nk_vpn
CertificatePolicies in C.SAK.AUT	oid_sak_aut
CertificatePolicies in C.TSL.CA	oid_tsl_ca

8.7 CV-Zertifikate für Musterkarten SMC-Typ K

Es gelten die Vorgaben aus Abschnitt 4.10.

8.8 Zulassungs-ID im Zertifikat

In allen X.509-Zertifikaten der SMC-K-Musterkarten MUSS für die in [gemX.509_Kon#5.2.2] in Kapitel 5.2.2 unter commonName definierte Zulassungsnummer der folgende Wert eingetragen werden:

gemTest_Konn_20001231_0001

8.9 CV-Zertifikate für Musterkarten SMC- K

Es gelten die Vorgaben aus Abschnitt 4.10.

8.10 Optische Gestaltung der Musterkarten für SMC K

Für die äußere Gestaltung der Musterkarten gilt bezüglich der Maße [gemSpec_eGK_P3]. Die optische Gestaltung ist gemäß folgender Vorlagen auszuführen:

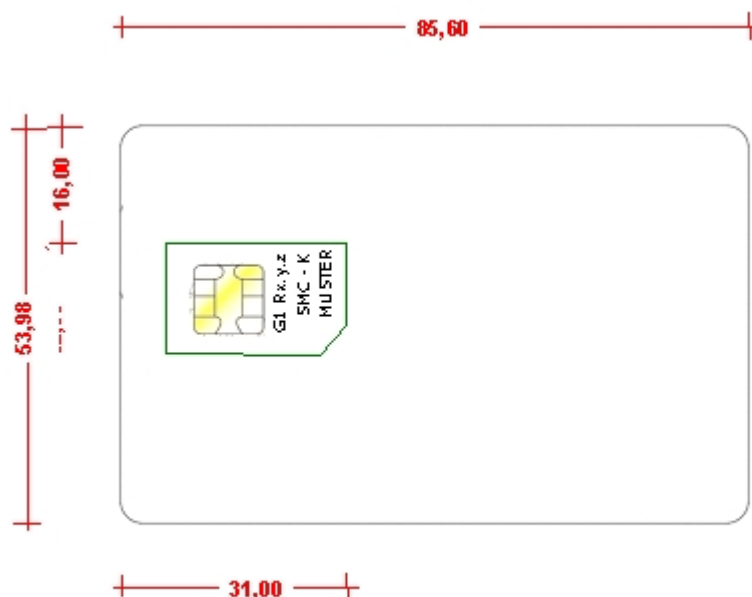


Abbildung 33: Kartenvorderseite SMC-K

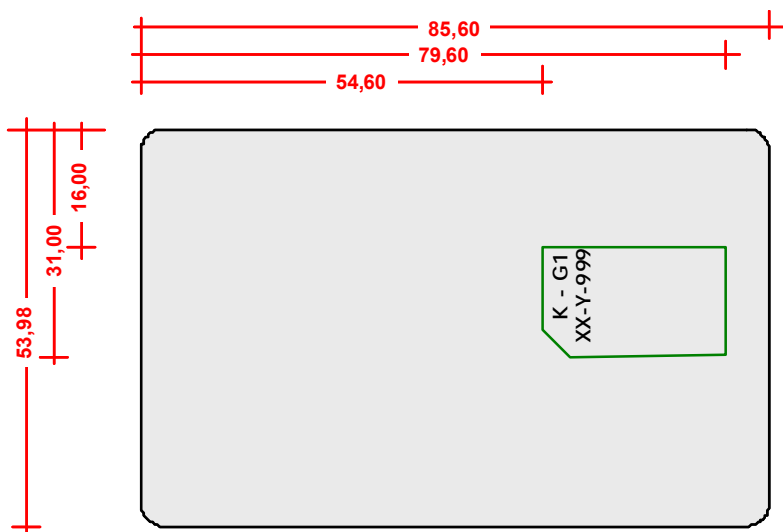


Abbildung 34: Kartenrückseite SMC-K mit Kodierung

Zusätzlich zur Kennzeichnung als SMC-K muss das Release im Format x.y.z angegeben werden, für das die Musterkarten hergestellt worden sind. Damit sind auch die jeweiligen Spezifikationsversionen festgelegt.

Auf der Vorderseite ist in dem als ID-00-Format verbleibenden Ausschnitt in Verdana True Type 8 pt „Muster-SMC-K“ analog Abbildung 26 (Information über Zugehörigkeit zu Generation 1 (G 1), Release, Typ, und Zusatz: Muster) aufzubringen.

Auf der Rückseite ist in dem als ID-00-Format verbleibenden Ausschnitt in Verdana True Type 8 pt „K“ und die Zugehörigkeit zur Generation 1 (G 1) sowie in einer zweiten Zeile

eine Kodierung für Hersteller, Version und laufende Nummer analog Abbildung 27 aufzubringen. Die Art der Kodierung bleibt dem Hersteller überlassen.

8.11 An den Kartenhersteller zu liefernde Unterlagen zur Erstellung von SMC-K-Musterkarten

Die Musterkarten müssen die Herausgeberkennung (Issuer Identifier) in der ICCSN enthalten. Die Herausgeberkennung für SMC-K-Musterkarten muss mit der gematik abgestimmt werden, falls der Kartenherausgeber noch keine gültige, von der GS1 Germany GmbH, Köln (www.gs1-germany.de) vergebene IIN besitzt. Weitere Kodierungen in der ICCSN sind zulässig, solange sie die Eineindeutigkeit nicht beeinträchtigen. Die Kodierung der Herausgeberkennung für Musterkarten ist in Anhang A festgelegt.

8.12 Daten

8.12.1 Vor Auslieferung der SMC-K-Musterkarten

CAs, die SMC-K-Musterkarten gemäß dieser Vorgaben erstellen wollen, müssen gemäß dem Dokument [gemX.509_TSP] „PKI für X.509-Zertifikate: Registrierung eines Trust Service Provider (TSP)“ bei der gematik als zugelassene CA registriert sein und die zu registrierenden Zertifikate gemäß Kapitel 4.3.1 in [gemX.509_TSP#4.3.1] vor Auslieferung der Musterkarten an die gematik zum Eintrag in die Test-TSL liefern.

Die Abfrage der Gültigkeit der X.509-Zertifikate C.NK.VPN der SMC-K-Musterkarten muss über einen von der ausgebenden CA betriebenen Verzeichnisdienst möglich sein, falls der OCSP-Dienst der gematik nicht genutzt wird.

Für die anderen X.509-Zertifikate (C.AK.AUT und C.SAK.AUT) muss kein OCSP-Dienst verfügbar sein.

8.13 Vom Kartenhersteller nach Erstellung der SMC-K-Musterkarten an die gematik zu liefernde Daten

Dieser Abschnitt gilt nur, falls der OCSP-Dienst der gematik genutzt werden soll.

Kartenhersteller, die SMC-K-Musterkarten gemäß dieser Vorgaben erstellt haben und den OCSP-Dienst der gematik nutzen wollen, müssen folgende Daten an die gematik zurückliefern:

- (1) X.509-Zertifikate aller erstellten Musterkarten im Format .cer. Bei größerer Anzahl erstellter Zertifikate (>25) sollen die Zertifikate in einer Datei gezippt werden. Im CommonName des SubjectDN soll der Firmenname des Herstellers als Unterscheidungskriterium enthalten sein.
- (2) Zu den eigentlichen Zertifikaten ist eine Liste beizufügen, die zu jedem erzeugten Zertifikat Dateinamen, den CommonName und die Zertifikatsseriennummer enthält.
- (3) Das CA-Zertifikat der CA, mit der die Versichertenzertifikate erstellt wurden, mit dem dazugehörige Schlüsselpaar (öffentlicher und privater Schlüssel) im Format

PKCS#12. Der Aufbau der CA-Zertifikate MUSS ISIS-MTT-konform sein. Im Zertifikat der CA MUSS der Wert ca=true in den BasicConstraints eingetragen werden (siehe Tabelle 2). Als Verwendungszweck (Key Usage) MUSS neben „keyCert-Sign“ auch „crlSign“ eingetragen sein. Das Passwort für die PKCS#12-Datei soll einheitlich auf den Wert „Musterkarte“ gesetzt sein.

Tabelle 8 Auszug aus [ISIS-MTT Part 1], Table 18

#	ASN.1 DEFINITION	SEMANTICS	SUPPORT		REFERENCES		NOTES
			GEN CA/EE CERT	PROC	RFC3280	ISISMTT	
1	BasicConstraints ::= SEQUENCE {	Indicates a CA certificate and defines how deep a certificate may exist below that CA.	++/+-	++	4.2.1.10		[1]
2	ca BOOLEAN DEFAULT FALSE,	ca=TRUE indicates a CA certificate ca=FALSE indicates an end entity					
3	pathLenConstraint INTEGER (0..MAX) OPTIONAL }	only meaningful if ca=TRUE, indicates how many CA certificates may be included in the certification path below this CA. That is, pathLenConstraint=0 indicates that only end entity certificates may follow in the path. If this field does not appear, there is no limit to the path length.					
[1]	[RFC3280] This extension MUST appear as a critical extension in all CA certificates that contain public keys used to validate digital signatures on certificates. This extension MAY appear as a critical or non-critical extension in CA certificates that contain public keys used exclusively for purposes other than validating digital signatures on certificates. Such CA certificates include ones that contain public keys used exclusively for validating digital signatures on CRLs and ones that contain key management public keys used with certificate enrollment protocols. This extension MAY appear as a critical or non-critical extension in end entity certificates. ISIS-MTT PROFILE: This extension MAY appear in end entity certificates and MUST appear in CA certificates. It MUST be marked critical.						

9 Layout Testkarten eGK

In den Testregionen werden in den Feldtests (10.000er-Tests) Karten eingesetzt, die Echtdaten enthalten

Das Layout der Testkarten eGK muss vollständig den Vorgaben von [gemSpec_eGK_P3] entsprechen.

Da heute noch nicht klar ist, ob Testkarten mit Echtdaten in den weiterführenden Erprobungen verwendet werden, können sie als Karten dieses Testabschnittes durch Einfügen des Buchstaben „T“ in der Schriftart Verdana True Type, 10pt, linksbündig unter dem Bild in gleicher Höhe wie die Zeile des Textfeldes für den Kostenträger kenntlich gemacht werden.

Eine weitere zusätzliche Art der Kennzeichnung (z. B. Schriftzug "Gesundheitskarte" in anderer Farbe, zusätzliches optisches Merkmal, ggf. auch kürzer befristetes Gültigkeitsdatum, etc...) ist den Herausgebern (Kassen) freigestellt.

Das BSI-Logo, wie es in [gemSpec_eGK_P3] vorgegeben ist, darf nur auf Karten aufgebracht werden, die gemäß dem BSI-PP evaluiert worden sind.

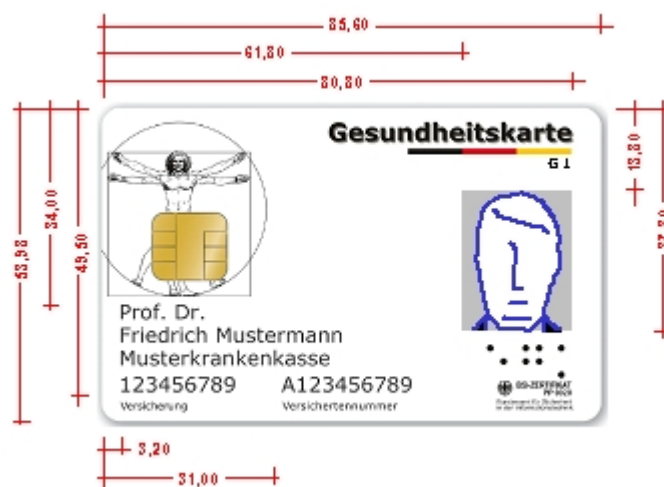


Abbildung 35: Layout Test-Gesundheitskarte ohne Kennzeichnung „T“ für Testkarte

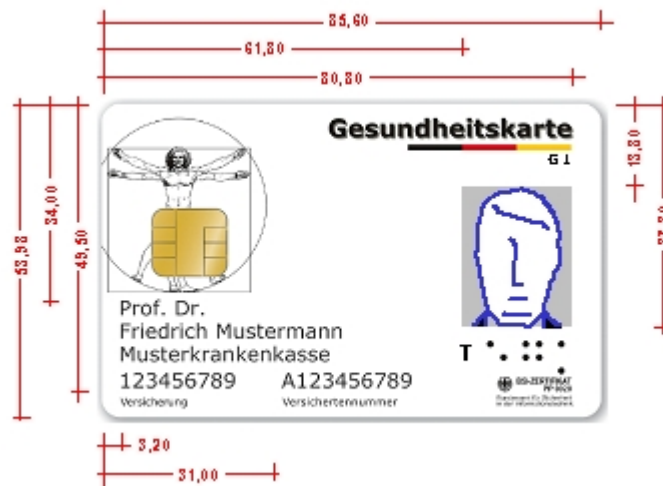


Abbildung 36: Layout Test-Gesundheitskarte mit Kennzeichnung „T“ für Testkarte

10 Layout Testkarten HBA

Das Layout der Testkarten mit der Rollenkennung ARZT, die während der ersten Tests (10.000er-Tests) eingesetzt werden, entspricht vollständig dem Layout des endgültigen Arztausweises. Weitere Details sind in [BÄK_HBA] "Handbuch zur optischen Gestaltung des eArztausweises" beschrieben.



Abbildung 37: Layout Test-Arztausweis

Anhang A

Festlegungen für IK der Krankenkassen, IIN des Kartenherausgebers und KVNR für Musterkarten eGK

A.1 Festlegungen für die IK des Kostenträgers für Musterkarten eGK

Die IK des Kostenträgers hat neun Stellen, von denen acht eine semantische Bedeutung haben und die 9.Ziffer eine Prüfziffer ist:

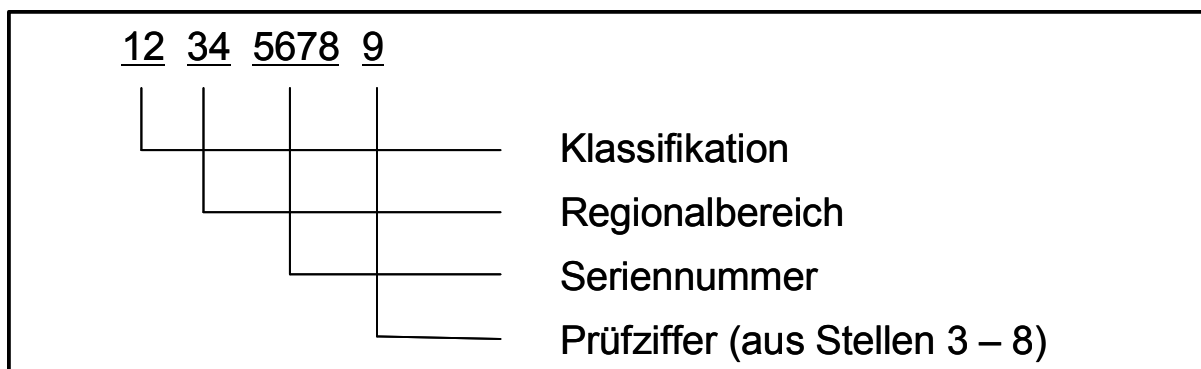


Abbildung 38: Bedeutung der Zifferngruppen der IK des Kostenträgers

Tabelle 9 Festlegungen für die IK des Kostenträgers

Klassifikation	Die Stellen 1 und 2 bezeichnen die Art der Institution oder die Personengruppe
Regionalbereich	Die Stellen 3 und 4 bezeichnen den Regionalbereich
Seriennummer	Die Stellen 5 bis 8 enthalten die Seriennummer. Die Seriennummern sind grundsätzlich frei verwendbar, sofern nicht Seriennummern-Kontingente festgelegt sind
Prüfziffer	Die Stelle 9 enthält die aus den Stellen 3 – 8 errechnete Prüfziffer (also ohne Einbeziehung der Klassifikation). Die Berechnung erfolgt nach dem Modulo-10-Verfahren von rechts beginnend mit der Gewichtung 1.2.1.2.1.2.

Festlegung:

Für die Musterkarten MUSS die dem Kostenträger zugewiesene IK verwendet werden.

A.2 Festlegungen zur IIN des Kartenherausgebers für Musterkarten eGK

Gemäß eGK-Spezifikation Teil 2 wird die Issuer Identification Nummer wie in Tabelle 9 angegeben gebildet:

Tabelle 10 Issuer Identification Number

MII für Gesundheitswesen	Country Code Germany	Issuer Identifier , für eine bestimmte Krankenversicherung
'80'	'276'	... (5 BCD)

Festlegung

Der 5-stellige Issuer Identifier fängt dabei bei allen vergebenen Nummern mit 00 an. Für die Musterkarten MUSS der 5-stellige Issuer Identifier mit 88 anfangen, danach folgen die letzten drei Stellen der 5-stelligen Ziffernfolge aus dem Issuer Identifier, der dem Kostenträger von GS1 Germany GmbH, Köln zugewiesen worden ist. Falls ein Kartenherausgeber noch keinen gültigen Issuer Identifier zugewiesen bekommen hat und kein Kostenträger ist, MUSS er sich wegen der Zuweisung einer nutzbaren IIN mit der gematik abstimmen.

A.3 Festlegungen zur KVNR für Musterkarten eGK

Vorgabe für die den unveränderlichen Teil der KVNR:

1 Buchstaben (A-Z),

8 Ziffern (0-9) und

1 Prüfziffer (0-9).

Der Buchstabe und die 8 Ziffern sind für jede Person „zufällig“, aber eindeutig, vergeben. Werte mit mehr als drei aufeinander folgenden gleichen Ziffern werden ausgeschlossen. „Zufällig“ meint hier, dass keine weitere Semantik enthalten ist. In Abweichung davon kann für spezielle Tests auch eine Semantik vereinbart werden.

Die Prüfziffer wird mit dem Modulo-10-Verfahren und den Gewichtungen 1-2-1-2-1-2-1-2 berechnet. Der Buchstabe wird dabei durch eine zweistellige Zahl ersetzt, das A mit 01, das B mit 02, ..., und das Z mit 26.

Festlegung

Da die Auswertung der Prüfziffer durch Systeme der Leistungserbringer (auch bei Musterkarten) möglich ist, müssen die KVNR für Musterkarten gemäß obiger Angabe korrekt gebildet werden.

Eine Prüfung des Verbots der Nutzung von mehr als drei aufeinander folgenden gleichen Ziffern erfolgt bei der Erstellung der KVNR beim Kostenträger. KVNR für Musterkarten dürfen deshalb ebenfalls nicht mehr als drei gleiche aufeinander folgende Ziffern enthalten.

Andererseits soll verhindert werden, dass identische KVNR für Musterkarten verschiedener Kartenherausgeber generiert werden. Deshalb müssen den Kartenherausgebern unterschiedliche Nummernräume zugewiesen werden.

Die Vergabe dieser Nummernkreise erfolgt auf formlosen Antrag durch die gematik.

Beispiele:

A11xxxxxP bis Z11xxxxxP

A22xxxxxP bis Z22xxxxxP

Anhang B

Festlegungen für die ICCSN für Musterkarten

B.1 Definition der ICCSN

Die ICCSN einer eGK muss weltweit eindeutig sein. Der Aufbau der ICCSN ist in Abbildung 39 noch einmal erläutert (siehe auch Abbildung 1):

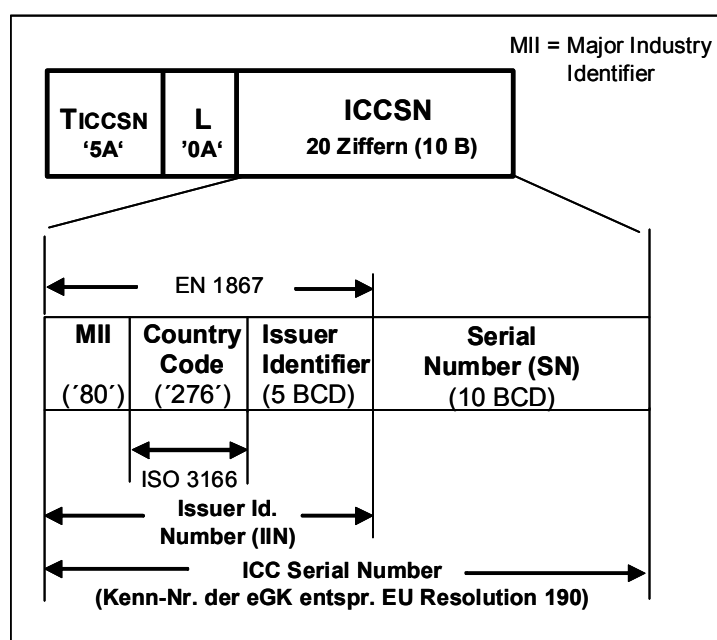


Abbildung 39: Aufbau der ICCSN

B.2 Kodierung der ICCSN

Um eine leichtere Zuordnung von Musterkarten zu Hersteller, ZDA, Kategorie und Kartenart zu erlauben, müssen bestimmte Stellen der ICCSN entsprechend kodiert werden. Die Kodierung der Stellen 1 – 10 ist bereits in den vorhandenen Spezifikationen festgelegt. Die Kodierung für die Stellen 11 – 20 der ICCSN der Musterkarten wird gemäß Tabelle 3 vorgegeben:

Tabelle 3: Kodierung der ICCSN

Stelle der ICCSN	Inhalt
1	8
2	0
3	2
4	7
5	6
6	8
7	8
8	Letzte 3 Stellen der Issuer Identification Nummer, die dem Herausgeber der Musterkarten von GS1 Germany GmbH, Köln zugewiesen worden ist
9	
10	
11	Herstellerkennung
12	
13	Kodierung des ZDA
14	Kodierung der Kategorie
15	Kodierung der Kartenart
16	Individuelle und eindeutige Nummerierung der Musterkarten im Nummernbereich, der durch die Stellen 1 – 15 definiert ist
17	
18	
19	
20	

B.3 Festlegungen im Detail

B.3.1 IIN

Jeder Karten-Herausgeber MUSS einen gültigen Issuer Identifier (IIN) besitzen, der dem Herausgeber von GS1 Germany GmbH, Köln zugewiesen worden ist. Der 5-stellige Issuer Identifier fängt dabei bei allen vergebenen Nummern mit 00 an. Für die Musterkarten MUSS der 5-stellige Issuer Identifier mit 88 anfangen, danach folgen die letzten drei Stellen der 5-stelligen Ziffernfolge aus dem Issuer Identifier, Falls ein Kartenherausgeber noch keinen gültigen Issuer Identifier zugewiesen bekommen hat, MUSS er einen gültigen Issuer Identifier (IIN) bei der GS1 Germany GmbH, Köln beantragen.

B.3.2 Herstellerkennung

Diese wird von der gematik auf Antrag vergeben. Bisher sind die Herstellerkennungen gemäß Tabelle 4 vergeben worden:

Tabelle 4: Herstellerkennung

Hersteller	Herstellerkennung
Gematik Testlabor	02
ComCard GmbH	04
Datacolor GmbH	05
Gemalto	06
Giesecke & Devrient GmbH	07
Novacard Informationssysteme GmbH	08
Oberthurcs	09
PAV Card GmbH	10
PPC Card Systems	11
Sagem-Orga GmbH	12
Systemform MediaCard GmbH	13
Winter AG	14
Siemens AG	15
Zeitcontrol Cardsystems GmbH	16
Collis	17
Intercomponentware AG	18
DAK	19
Camp for Management & Consultant	20
Akm software GmbH	21
T-Systems	22
MCS	23
PDE	24

B.3.3 Kodierung des ZDA/der CA

Die Kodierungen werden von der gematik auf Antrag vergeben. Bisher sind die ZDA/CA-Kennungen gemäß Tabelle 5 vergeben worden:

Tabelle 5: Kodierung des ZDA/der CA

ZDA/CA	Kodierung
D-Trust	1
DGN	2
SignTrust	3
TC-Trust-Center	4
Telesec	5
gematik	6

B.3.4 Kodierung der Fehlerkategorie

Falls definierte Fehlermuster für Musterkarten erzeugt werden sollen, müssen die jeweiligen Fehlerkategorien gemäß Tabelle 6 kodiert werden. Die Zuordnung einer konkreten Fehlerkategorie (die dann entsprechend benannt wird) zu einem Wert für die Kodierung erfolgt auf Antrag durch die gematik.

Tabelle 6: Kodierung der Fehlerkategorie

Fehlerkategorie	Kodierung
Standardkarte	1
Fehlerkategorie 1 (tbd)	2
Fehlerkategorie 2 (tbd)	3
Fehlerkategorie 3 (tbd)	4
Fehlerkategorie 4 (tbd)	5
Fehlerkategorie 5 (tbd)	6
Fehlerkategorie 6 (tbd)	7
Fehlerkategorie 7 (tbd)	8
Fehlerkategorie 8 (tbd)	9
Fehlerkategorie 9 (tbd)	0

B.3.5 Kodierung der Kartenart

Die verschiedenen Kartenarten werden durch eine entsprechende Kodierung unterschieden. Die Werte für die Kodierung werden von der gematik vergeben. Bisher sind die Kodierungen für die Kartenart gemäß Tabelle 7 vergeben worden:

Tabelle 7: Kodierung der Kartenart

Kartenart	Kodierung
SMC-A	1
SMC-B	2
HBA	3
eGK	4
SMC-B light	5
SMC-K	6
SMC-KomSiT	7

Anhang C

C.1 - Abkürzungen

Kürzel	Erläuterung
AUT	Authentifizierung
BSI	Bundesamt für die Sicherheit in der Informationstechnik
BÄK	Bundesärztekammer
BCD	Binär kodierte Dezimalzahl
CVC	Card Verifiable Certificate
DF	Dedicated File
EF	Elementary File
eGK	elektronische Gesundheitskarte
EHIC	Europäische Krankenversichertenkarte
ENV	Verschlüsselung (Encryption)
HBA	Heilberufsausweis (auch HPC)
HPC	Health Professional Card (auch HBA)
IIN	Issuer Identifier Number, Kennung des Kartenanbieters
IK	Institutionskennzeichen: Ordnungsbegriff für Teilnehmer am Telematikprozess
KomSiT	Komfortsignatur-Token
KVNR	Krankenversichertennummer
MF	Master File
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PIN	Persönliche Identifikationsnummer
PuK	Public Key (öffentlicher Schlüssel)
PUK	Pin Unblocking Key
PrK	Private Key (privater Schlüssel)
SMC	Security Module Card
SMC-K	Security Module Card des Konnektors
TLV	Tag Length Value

Kürzel	Erläuterung
XML	Universelle Datenbeschreibungssprache (Extensible Markup Language)
ZDA	Zertifizierungsdiensteanbieter

C.2 - Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

C.3 - Abbildungsverzeichnis

Abbildung 1: Definition der verschiedenen Kartentypen am Beispiel der eGK.....	9
Abbildung 2: Objektstruktur einer eGK auf oberster Ebene.....	14
Abbildung 3: Objektstruktur der Gesundheitsanwendung DF.HCA	14
Abbildung 4: Objektstruktur der Anwendung ESIGN.....	15
Abbildung 5: Objektstruktur der Anwendung QES	16
Abbildung 6: Objektstruktur der Anwendung DF.CIA.ESIGN	16
Abbildung 7: ICCSN für Gesundheitskarten.....	17
Abbildung 8: Kartenvorderseite mit Personalisierung, ohne Bild	21
Abbildung 9: Kartenvorderseite mit Personalisierung, mit Bild	22
Abbildung 10: Allgemeine Dateistruktur des HBA	27
Abbildung 11: Dateistruktur von DF.HPA.....	28
Abbildung 12: Prinzipielle Struktur von DF.ESIGN	29
Abbildung 13: Struktur der QES-Anwendung.....	30
Abbildung 14: Dateistruktur von DF.CIA.QES und DF.CIA.ESIGN.....	31
Abbildung 15: Kartenvorderseite, konstante Elemente.....	33
Abbildung 16: Kartenvorderseite, Personalisierung	33
Abbildung 17: Prinzipielle Dateistruktur der SMC-A	35
Abbildung 18: Dateistruktur von DF.SMA einer SMC-A	36
Abbildung 19: Dateistruktur von DF.KT.....	36
Abbildung 20: Kartenvorderseite SMC Typ A.....	38
Abbildung 21: Kartenrückseite SMC Typ A mit Kodierung	39
Abbildung 22: Prinzipielle Struktur der SMC-B.....	40
Abbildung 23: Prinzipielle Struktur von DF.SMA einer SMC-B	41
Abbildung 24: Dateistruktur von DF.KT.....	42
Abbildung 25: Struktur von DF.ESIGN.....	43
Abbildung 26: Kartenvorderseite SMC Typ B mit Institutionsbezeichnung	45
Abbildung 27: Kartenrückseite SMC Typ B mit Kodierung	45
Abbildung 28: Dateistruktur einer SMC-K auf oberster Ebene.....	49
Abbildung 29 Dateistruktur der Anwendung DF.AK.....	49
Abbildung 30 Dateistruktur der Anwendung DF.NK	50
Abbildung 31: Dateistruktur der Anwendung DF.SAK	50
Abbildung 32: Dateistruktur der Anwendung DF.Sicherheitsanker	51
Abbildung 33: Kartenvorderseite SMC-K	53
Abbildung 34: Kartenrückseite SMC-K mit Kodierung	53
Abbildung 35: Layout Test-Gesundheitskarte ohne Kennzeichnung „T“ für Testkarte	56
Abbildung 36: Layout Test-Gesundheitskarte mit Kennzeichnung „T“ für Testkarte	57
Abbildung 37: Layout Test-Arzttausweis.....	58
Abbildung 38: Bedeutung der Zifferngruppen der IK des Kostenträgers.....	59

Abbildung 39: Aufbau der ICCSN62

C.4 – Tabellenverzeichnis

Tabelle 1 OID-Referenzen für Musterkarten eGK (verpflichtend).....	19
Tabelle 2 Auszug aus [ISIS-MTT Part 1], Table 18	24
Tabelle 3 OID-Referenzen für Musterkarten HBA (verpflichtend).....	32
Tabelle 4 OID-Referenzen für Musterkarten SMC-B (verpflichtend).....	37
Tabelle 5 OID-Referenzen für Musterkarten SMC-B (verpflichtend).....	44
Tabelle 6 Auszug aus [ISIS-MTT Part 1], Table 18	48
Tabelle 7 OID-Referenzen für Musterkarten SMC-K (verpflichtend).....	51
Tabelle 8 Auszug aus [ISIS-MTT Part 1], Table 18	55
Tabelle 9 Festlegungen für die IK des Kostenträgers.....	59
Tabelle 10 Issuer Identification Number.....	60

C.5 - Referenzierte Dokumente

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik. Der mit dem vorliegenden Dokument korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen, die im Rahmen des Vorhabens zur Einführung der Gesundheitskarte veröffentlicht werden, wird pro Release in einer Dokumentenlandkarte definiert. Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Die jeweils gültige Version und das Freigabedatum der aufgeführten gematik-Dokumente entnehmen Sie bitte der von der gematik veröffentlichten Dokumentenlandkarte (aktuell [gemDokLK_2.3.4]), wobei jeweils der aktuellste Releasestand maßgeblich ist, in dem die vorliegende Version aufgeführt wird. Zur Unterstützung der Zuordnung wird in der Dokumentenlandkarte im Kapitel 4 eine Übersicht über die Dokumentenversionen und deren Zuordnung zu den verschiedenen Releases bereitgestellt.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemDokLK_2.3.4]	gematik: Einführung der Gesundheitskarte – Dokumentenlandkarte Releasestand 2.3.4 – Online Feldtest 10.000 Festlegung der Versionsstände
[gemeGK_Fach]	gematik: Einführung der eGK - Speicherstrukturen der eGK für Gesundheitsanwendungen (gemäß der ausgewählten Dokumentenlandkarte, siehe oben)
[gemPKI_Reg]	gematik: Einführung der eGK - PKI für CV-Zertifikate: Registrierung einer CVC-CA der zweiten Ebene, (gemäß der ausgewählten Dokumentenlandkarte, siehe oben)
[gemPers]	gematik: Einführung der Gesundheitskarte – Übergabeschnittstelle für die Produktion der eGK, (gemäß der ausgewählten Dokumentenlandkarte, siehe oben)

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_eGK_P1]	gematik: Einführung der Gesundheitskarte – Die Spezifikation elektronische Gesundheitskarte; Teil 1 – Kommandos, Algorithmen und Funktionen des Kartenbetriebssystems (gemäß der ausgewählten Dokumentenlandkarte, siehe oben)
[gemSpec_eGK_P2]	gematik: Einführung der Gesundheitskarte – Die Spezifikation elektronische Gesundheitskarte ;Teil 2 – Anwendungen und anwendungsspezifische Strukturen (gemäß der ausgewählten Dokumentenlandkarte, siehe oben)
[gemSpec_eGK_P3]	gematik: Einführung der Gesundheitskarte – Die Spezifikation elektronische Gesundheitskarte; Teil 3 – Äußere Gestaltung
[gemSpec_Krypt]	gematik: Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematik- infrastruktur
[gemSpec_OID]	gematik: Einführung der Gesundheitskarte - Spezifikation: Festlegung von OIDs
[gemSpec_SMC-K]	gematik: Einführung der Gesundheitskarte - Spezifikation der SMC-K
[gemSpec_TLK]	gematik: Einführung der Gesundheitskarte – Spezifikation für Testlaborkarten (eGK, HBA, SMC)
[gemX.509_eGK]	gematik: Einführung der Gesundheitskarte – Festlegungen zu den X.509-Zertifikaten der Versicherten
[gemX.509_Kon]	gematik: Einführung der Gesundheitskarte - Festlegungen zu den X.509-Komponentenzertifikaten des Konnektors
[gemX.509_SMCB]	gematik: Einführung der Gesundheitskarte – Festlegungen zu den X.509-Zertifikaten der SMC-Typ-B
[gemX.509_TSP]	gematik: Einführung der Gesundheitskarte - PKI für X.509-Zertifikate: Registrierung eines Trust Service Provider

Weitere Referenzen

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[DIN66291-1]	DIN V66291-1 (2000): Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG/SigV Teil 1: Anwendungsschnittstelle
[HBA-P1]	BÄK et. al: Spezifikation des elektronischen Heilberufsausweises Teil I: Kommandos, Algorithmen und Funktionen der Betriebssystemplattform (gemäß der ausgewählten Dokumentenlandkarte, siehe oben), www.gematik.de , www.baek.de/30/eArzttausweis/index.html

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[HBA-P2]	BÄK et al.: Spezifikation des elektronischen Heilberufsausweises Teil II: HBA – Anwendungen und Funktionen (gemäß der ausgewählten Dokumentenlandkarte, siehe oben), www.gematik.de , www.baek.de/30/eArzttausweis/index.html
[HBA-P3]	BÄK et al.: Spezifikation des elektronischen Heilberufsausweises Teil III: SMC – Anwendungen und Funktionen (gemäß der ausgewählten Dokumentenlandkarte, siehe oben), www.gematik.de , www.baek.de/30/eArzttausweis/index.html
[ISIS-MTT Part 1]	ISIS-MTT Specification Part 1: Certificate And CRL Profiles Version 1.1 – 16 March 2004
[BÄK_HBA]	Bundesärztekammer: Handbuch zur optischen Gestaltung des eArzttausweises; Richtlinien für die optische Gestaltung (Gestaltung, Produktion und Dateivorlagen); zum Release gehörende Fassungen