Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation für Testkarten gematik (eGK, HBA, (g)SMC) der Generation 2

Version:	3.6.0
Revision:	\main\rel_online\rel_ors1\44
Stand:	24.07.2015
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemSpec_TK]

Dokumentinformationen

Änderungen zur Vorversion

Folgende Änderungen gegenüber der Version 3.7.0 wurden durchgeführt:

1) gemErrata_R1.4.7

   a) C_5021 wirkt sich aus auf Card-G2-A_2724, Card-G2-A_2725, Card-G2-A_2734, Card-G2-A_2773 Card-G2-A_2790, Card-G2-A_2804, Card-G2-A_2805, Card-G2-A_3518, Card-G2-A_2823, Card-G2-A_2824, Card-G2-A_3519, Card-G2-A_2837, Card-G2-A_2838, Card-G2-A_3520

Dokumentenhistorie

Version	Stand	Grund der Änderung, besondere Hinweise	Bearbeitung
3.0.0	19.09.12	freigegeben	gematik
3.0.1	29.10.12	Einarbeitung Kommentare und Hinweise	gematik
3.1.0 RC	10.01.13	Überarbeitung der optionalen Eigenschaften	gematik
3.1.1	23.01.13	Referenz auf Schnittstelle aus AFOs entfernt	gematik
3.2.0	23.10.13	Einfügen Bemaßung und Position gematik, Rückseite ohne EHIC, Vorgaben zu EHIC	gematik
3.3.0 RC	19.12.13	Einfügen AFOs zur CAN	gematik
3.4.0	21.02.14	Einfügen der Vorgaben für zusätzliche PINs bei HBA, SMC-B und gSMC-K	gematik
3.5.0	06.06.14	Streichen der AFO Card-G2-A_2799 „Rolle des Karten-inhabers der SMC-B-Testkarten GE“, Einarbeitung Änderungen Iteration 3	gematik
3.5.1	24.07.15	Folgende Errata eingearbeitet: R1.4.7	gematik
3.6.0	24.07.15	freigegeben	gematik

© gematik – öffentlich

Inhaltsverzeichnis

Dokumentinformationen 2

Inhaltsverzeichnis 3

1 Einführung des Dokumentes 6

1.1 Zielsetzung 6

1.2 Zielgruppe 8

1.3 Geltungsbereich 8

1.4 Abgrenzung des Dokuments 9

1.5 Methodik 9

1.6 Produktionskennzeichnung 9

2 Strukturen zu Herstellung von Testkarten GE G2 10

3 Vorgaben zu CV-Zertifikaten, gültig für alle Karten 11

3.1 CV-Zertifikate für Testkarten GE der Generation 2 11

3.1.1 Test-Root-CVC-CAs (Testkarten GE) 11

3.1.2 Test-CVC-CA der Generation 2 für Testkarten 11

3.2 Generierung der Vertrauensanker für CV-Zertifikate 12

3.2.1 Öffentlicher Schlüssel PuK.RCA.CS.XXXX für Testkarten 12

3.2.2 Asymmetrische Schlüsselpaare mit dem öffentlichen Schlüssel PuK.CMS_YYY.AUT_CVC.XXXX für Testkarten GE 12

4 Vorgaben zu symmetrischen Schlüsseln 14

4.1 Generierung der Secret Keys SK.CMS.AESXXX, SK.VSD.AESXXX und SK.VSDCMS.AESXXX für Testkarten GE 14

5 Vorgaben für eGK-Testkarten GE der Generation 2 15

5.1 PIN- und PUK-Werte 15

5.1.1 PIN-Werte 15

5.1.2 PUK-Werte 15

5.1.3 CAN-Wert 15

5.1.4 Bereitstellung der Daten durch die gematik 16

5.2 Erstellung der X.509-Zertifikate für die eGK-Testkarten GE 17

5.2.1 Erstellung der X.509-Zertifikate für ENC, ENCV, AUT und AUTN bei der jeweiligen CA (Los 3 G2 und Los 4 G2) 17

5.2.2 Erstellung der X.509-Zertifikate für die Pseudo-QES bei der jeweiligen CA (Los 3 G2 und Los 4 G2) für die eGK-Testkarten GE 18

5.2.3 OID-Vorgaben für eGK-Testkarten 19

5.3 CV-Zertifikate für die eGK -Testkarten GE der Generation 2 19

5.4 Secret Keys SK.CMS.AES128, SK.VSD.AES128 und SK.VSDCMS.AES128 für die eGK-Testkarten GE der Generation 2.....19

5.5 Optische Gestaltung der eGK Testkarten GE der Generation 2 20

5.6 Daten zur Erstellung von eGK-Testkarten GE der Generation 2 23

5.7 Lieferung der eGK-Testkarten GE der Generation 2 23

6 Vorgaben für die HBA-Testkarten GE der Generation 2.....24

6.1 PIN- und PUK-Werte 24
6.1.1 PIN-Werte.....24
6.1.2 PUK-Werte 24
6.1.3 CAN-Wert.....25

6.2 Erstellung der X.509-Zertifikate für ENC und AUT der HBA-Testkarten GE bei der jeweiligen CA (Los 3 G2 und Los 4 G2).....25
6.2.1 Erstellung der X.509-Zertifikate für die Pseudo-QES bei der jeweiligen CA (Los 3 G2 und Los 4 G2) für die HBA-Testkarten GE.....26
6.2.2 OID-Vorgaben für die HBA-Testkarten GE 27

6.3 CV-Zertifikate für die HBA-Testkarten GE der Generation 2.....28

6.4 Secret Keys SK.CMS.AES128 und SK.CMS.AES256 für die HBA-Testkarten GE der Generation 2.....28

6.5 Optische Gestaltung der HBA-Testkarten GE der Generation 2 28

6.6 Daten zur Erstellung von HBA-Testkarten GE der Generation 2.....31

6.7 Lieferung der HBA-Testkarten GE der Generation 2.....32

7 Vorgaben für die SMC-B-Testkarten GE der Generation 2.....33

7.1 PIN- und PUK-Werte 33
7.1.1 PIN-Werte.....33
7.1.2 PUK-Werte 33

7.2 Erstellung der X.509-Zertifikate für die SMC-B-Testkarten GE.....34
7.2.1 OID-Vorgaben für die SMC-B-Testkarten der Generation 2.....35

7.3 CV-Zertifikate für die SMC-B-Testkarten GE der Generation 2.....36

7.4 Secret Keys SK.CMS.AES128 für die SMC-B-Testkarten GE der Generation 2 36

7.5 Optische Gestaltung der SMC-B-Testkarten GE der Generation 2.....36

7.6 Daten zur Erstellung von SMC-B-Testkarten GE der Generation 2.....40

7.7 Lieferung der SMC-B-Testkarten GE der Generation 2.....40

8 Vorgaben für die gSMC-K-Testkarten GE der Generation 2.....41

8.1 PIN- Werte 41
8.1.1 PIN-Werte.....41

8.2 Erstellung der X.509-Zertifikate der gSMC-K-Testkarten GE.....42

8.2.1 OID-Vorgaben für die gSMC-K-Testkarten GE der Generation 2 43
8.3 CV-Zertifikate für die gSMC-K-Testkarten GE der Generation 2 43
8.4 Secret Key SK.CMS.AES128 für die gSMC-K-Testkarten GE der Generation 2 43
8.5 Optische Gestaltung der gSMC-K-Testkarten GE der Generation 2 44
8.6 Daten zur Erstellung von gSMC-K-Testkarten GE der Generation 2 45
8.7 Lieferung der gSMC-K-Testkarten GE der Generation 2 46
9 Vorgaben für die gSMC-KT-Testkarten GE der Generation 2 47
9.1 Erstellung der X.509-Zertifikate der gSMC-KT-Testkarten GE 47
9.1.1 OID-Vorgaben für die gSMC-KT-Testkarten GE der Generation 2 48
9.2 CV-Zertifikate für die gSMC-KT-Testkarten GE der Generation 2 48
9.3 Secret Keys SK.CMS.AES128 für die gSMC-KT-Testkarten GE der Generation 2 49
9.4 Optische Gestaltung der gSMC-KT-Testkarten GE der Generation 2 49
9.5 Daten zur Erstellung von gSMC-KT-Testkarten GE der Generation 2 51
9.6 Lieferung der gSMC-KT-Testkarten GE der Generation 2 51
Anhang A - Verzeichnisse 52
A1 - Abkürzungen 52
A2 - Glossar 53
A3 - Abbildungsverzeichnis 53
A.4 – Tabellenverzeichnis 54
A5 - Referenzierte Dokumente 54
A5.1 – Dokumente der gematik 54
A5.2 - Weitere Dokumente 55
Anhang B - Festlegungen 56
B1 - Festlegungen für die IK des Kostenträgers für die eGK-Testkarten GE 56
B2 - Festlegungen zur IIN des Kartenherausgebers für die eGK-Testkarten GE 57
B3 - Festlegungen zur KVNR für die eGK-Testkarten GE 57
B4 - Definition der ICCSN 59
B5 - Kodierung der ICCSN für Testkarten GE 59

1 Einführung des Dokumentes

1.1 Zielsetzung

In diesem Dokument werden die im Rahmen einer Personalisierung von eGK-, HBA- und (g)SMC-Testkarten aufzubringenden elektronischen und optischen Daten sowie die zugehörigen Voraussetzungen und Prozesse beschrieben. Es wird festgelegt, wie diese Daten analog der jeweiligen Spezifikation in die Datenstrukturen der Testkarten zu schreiben sind.

Mit der Nutzung der elektronischen Gesundheitskarte und 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 (g)SMC) müssen vor dem Einsatz in definierten Umgebungen ausführlich auf Übereinstimmung mit den Spezifikationen und mit den Vorgaben für die Funktionalität geprüft werden. Die Abbildung Abb_TK_001 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.

Testlaborkarte	**Testkarte**	**Echtkarte**	**Dummy-Karte**
Zulassung	**Test**	**Wirkbetrieb**	**Promotion**
Testlabor	**Test- und Referenzumgebung**	**Produktiv-Umgebung**	**keine Funktion**
Schwerpunkt: Betriebssystem (COS) und Objektsystem	**Schwerpunkt: Funktionen und Abläufe**	**Schwerpunkt: Produktivbetrieb**	**Schwerpunkt: Look & Feel**
CVC: gematik-CVC-Root gematik-CVC-CA	**CVC: Test-CVC-Root Test-CVC-CA**	**CVC: CVC-Root CVC-CA**	**CVC keine Zertifikate**
X-509: gematik-CA	**X-509: Test-CA**	**X-509: Echt-CA**	**X.509 keine Zertifikate**
Test-Datenstrukturen	**Test-Daten**	**Echt-Daten**	**Keine Vorgabe**

Abbildung 1: Abb_TK_001 Definition der verschiedenen Kartentypen am Beispiel der eGK

Testlaborkarten:

Es handelt sich um Chipkarten, die herstellerbezogen mit speziell spezifizierten Strukturen und Inhalten im Labor auf die Einhaltung der Betriebssystemspezifikation [gemSpec_COS], der eGK-Spezifikation [gemSpec_eGK_ObjSys] zur Verwendung als eGK, der HBA-Spezifikation [gemSpec_HBA_ObjSys] zur Verwendung als HBA, der SMC-B Spezifikation [gemSpec_SMC-B_ObjSys] zur Verwendung als SMC-B, der gSMC-K-Spezifikation [gemSpec_SMC-B_ObjSys] zur Verwendung als SMC-K und der gSMC-KT-Spezifikation [gemSpec_SMC-B_ObjSys] zur Verwendung als SMC-KT getestet werden. Die speziell dafür festgelegten Strukturen und Spezifikationen sind im Dokument [gemSpec_TLK_COS_G2] enthalten.

Testkarten:

Testkarten dienen der Erprobung in Testumgebungen mit Testdaten.

Testkarten müssen den technischen Spezifikationen entsprechen, wie sie in den Spezifikationen für die eGK ([gemSpec_COS] und [gemSpec_eGK_ObjSys]) und in den entsprechenden Spezifikationen für den HBA [gemSpec_HBA_ObjSys], die SMC-B [gemSpec_SMC-B_ObjSys], die SMC-K [gemSpec_gSMC-K_ObjSys] und die SMC-KT [gemSpec_gSMC-KT_ObjSys] beschrieben sind.

Die Testkarten enthalten keine Echtdaten.

Echtkarten:

Echtkarten werden im Wirkbetrieb genutzt.

Karten für Öffentlichkeitsarbeit

Karten für Öffentlichkeitsarbeit werden genutzt, um das Aussehen der jeweiligen Karte präsentieren zu können. Diese Karten sollten keine funktionalen Eigenschaften haben, auf jeden Fall dürfen sie keine CVC-Zertifikate und keine X.509-Zertifikate enthalten.

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

1.2 Zielgruppe

Dieses Dokument ist für Hersteller von Karten (Chipkartenhersteller und -personalisierer, Trusted Service Provider (TSP) mit den Einheiten Certification Authority (CA) und OCSP-Responder) bestimmt und ermöglicht ihnen die Herstellung spezifikationsgerechter Testkarten. Informativ dient es Herstellern von Produkten bei der Testung und Entwicklung ihrer Produkte mit Testkarten.

1.3 Geltungsbereich

Das vorliegende Dokument enthält normative Anforderungen und Festlegungen, die von Herstellern und Betreibern von Komponenten und Diensten der Telematikinfrastruktur zu beachten sind. Die Zuordnung der vorliegenden Version zu einem Release erfolgt über die jeweilige Dokumentenlandkarte. Diese wird zusammen mit den Dokumenten auf der Internetseite der gematik bereitgestellt.

Dieses Dokument enthält verbindliche Festlegungen zur Beauftragung der Personalisierung von Testkarten durch die gematik und legt die Abläufe, die Datenformate und die Verantwortung für die Erzeugung der zur Erstellung einer Testkarte benötigten Daten fest.

Außerhalb der Beauftragungen durch die gematik ist dieses Dokument informativ.

Schutzrechts-/Patentrechtshinweis

Dieses Dokument ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Inhalte in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der beschriebenen Inhalte angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

© gematik – öffentlich

1.4 Abgrenzung des Dokuments

Die Spezifikation definiert Struktur, Inhalt und Umfang der Daten, die auf die Testkarten geschrieben werden müssen.

Die Festlegungen für diese Testkarten sind den folgenden Dokumenten zu entnehmen:

- [gemSpec_SMC-B_ObjSys]
- [gemSpec_gSMC-K_ObjSys]
- [gemSpec_gSMC-KT_ObjSys]

Die Inhalte der x.509-Zertifikate werden in [gemSpec_PKI] festgelegt.

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

⌦ **Card-G2-A_0000 <Titel der Afo>**
Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

Da es neben dieser Spezifikation für Testkarten der gematik noch eine Spezifikation für Testkarten zum Test von Fachdiensten gibt, werden in diesem Dokument in den Überschriften und in den Anforderungstiteln aller Anforderungen die Karten als Testkarten GE bezeichnet.

1.6 Produktionskennzeichnung

Zur Unterscheidung des Entwicklungs- und Produktionsstands der Testkarten das fünfstellige Herstellerkürzel und die Versionsnummer des auf der Karte vorhandenen Objektsystems, im Rahmen der Personalisierung auf die Karten aufgedruckt werden. Zusätzlich wird eine Datumsangabe aufgedruckt mit welcher einzelne Produktionschargen der Personalisierung identifiziert werden können und die durch einen Bindestrich von der Versionsnummer getrennt wird.

© gematik – öffentlich

2 Strukturen zu Herstellung von Testkarten GE G2

Testkarten werden im Rahmen der Ausschreibung für die Karten der Generation 2 durch den Testkartenhersteller im Auftrag des Testkartenherausgebers gematik hergestellt. Die beteiligten Entitäten sind in Abb_TK_002 dargestellt.

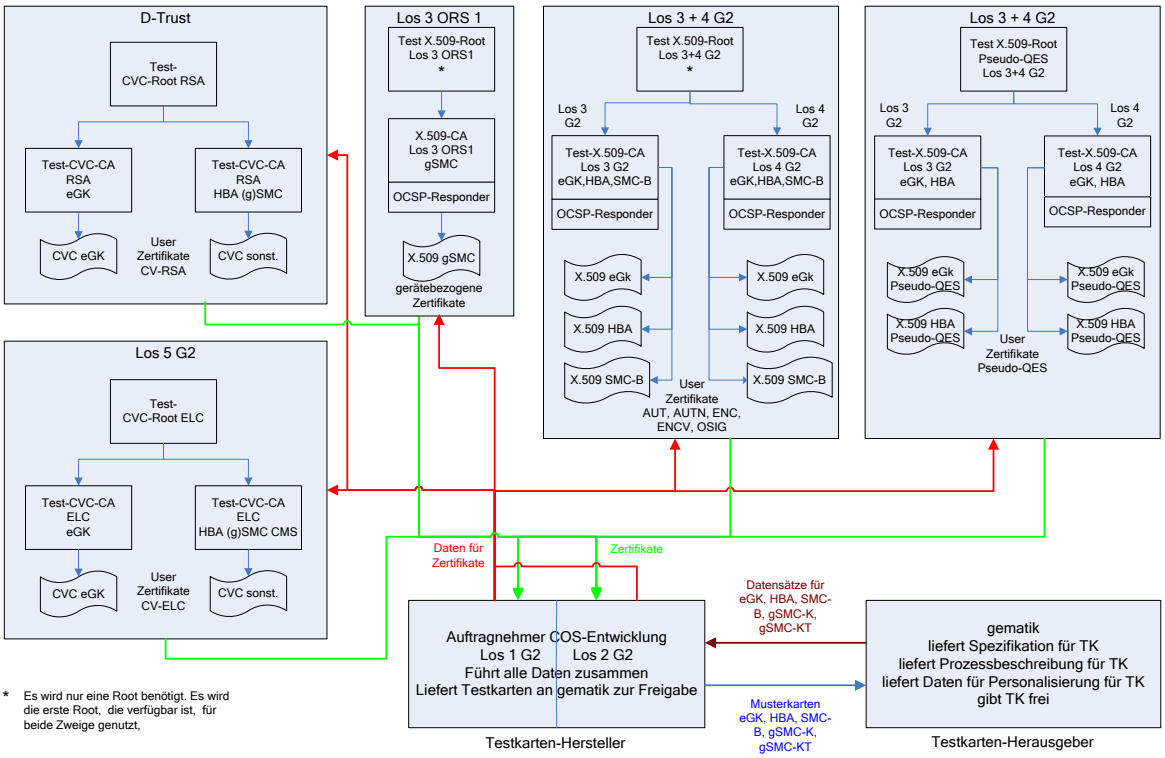


Abbildung 2: Abb_TK_002 Darstellung der Abläufe für die Erstellung von Testkarten G2 (mit Test-PKI)

In den folgenden Kapiteln werden die Aufgaben der in Abb_TK_002 aufgeführten Entitäten bei der Erstellung von Testkarten G2 beschrieben. Damit ist die gematik für die Testkarten dieser Spezifikation der Kartenherausgeber. Dies ist in den Anforderungen berücksichtigt, die Aufgaben für den Kartenherausgeber enthalten.

3 Vorgaben zu CV-Zertifikaten, gültig für alle Karten

3.1 CV-Zertifikate für Testkarten GE der Generation 2

3.1.1 Test-Root-CVC-CAs (Testkarten GE)

⌦ **Card-G2-A_2684 Bereitstellung von Test-Root-CVC-CAs (Testkarten GE)**

Die gematik MUSS sicherstellen, dass sowohl eine Test-Root-CVC-CA für Testkarten für das RSA-Verfahren (identisch zur Test-Root-CVC-CA der Generation 1) als auch eine Test-Root-CVC-CA für Testkarten für das Verfahren mit elliptischen Kurven (gemäß Los 5 G2: Test-Root-CVC-CA der Generation 2) für die Schlüssellänge 256 bit existiert. ⌫

⌦ **Card-G2-A_2685 CVC-CAs (Testkarten GE)**

Alle CV-Zertifikate für die Testkarten der Generation 2 MÜSSEN von CVC-CAs erstellt werden, die von der jeweiligen Test-Root-CVC abgeleitet ist. ⌫

⌦ **Card-G2-A_2686 Veröffentlichung der öffentlichen Schlüssel der Test-CVC-CA (Testkarten GE)**

Die öffentlichen Schlüssel der Test-Root-CVC-CA der Generation 1 und der Generation 2 MÜSSEN durch die Betreiber der jeweiligen Test-Root-CVC-CA auf ihren Homepages im Internet veröffentlicht werden. ⌫

⌦ **Card-G2-A_2687 Name der CVC-CA Generation 1 (Testkarten GE)**

Der CA-Name der aktuellen Test-Root-CVC-CA der Generation 1 MUSS DEGXX sein. ⌫

⌦ **Card-G2-A_2688 Name der CVC-CA Generation 2 (Testkarten GE)**

Der CA-Name der aktuellen Test-Root-CVC-CA der Generation 2 MUSS DEGXX sein. ⌫

⌦ **Card-G2-A_2689 Festlegung Schlüssellänge für CVC (Testkarten GE)**

Die Schlüssellänge für CV-Zertifikate für ELC-Kryptographie MUSS gemäß [gemSpec_COS] auf 256 bit festgelegt werden. ⌫

3.1.2 Test-CVC-CA der Generation 2 für Testkarten

⌦ **Card-G2-A_2690 Bereitstellung von CV-Zertifikaten für HBA- und SMC-B-Testkarten GE**

Der Testkartenhersteller MUSS dafür sorgen, dass die Testkarten HBA und SMC-B der Generation 2 mit Test-CV-Zertifikaten für das RSA-Verfahren (Schlüssellänge 2048 bit) und für das Verfahren mit elliptischen Kurven (Schlüssellänge 256 bit) gemäß [gemSpec_PKI] ausgestattet sind. ⌫

⌦ **Card-G2-A_2958 Bereitstellung von CV-Zertifikaten für eGK-, gSMC-K- und gSMC-KT-Testkarten GE**

Der Testkartenhersteller MUSS dafür sorgen, dass die Testkarten eGK, gSMC-K und gSMC-KT der Generation 2 mit Test-CV-Zertifikaten für das Verfahren mit elliptischen Kurven (Schlüssellänge 256 bit) gemäß [gemSpec_PKI] ausgestattet sind. ⌫

⌦ **Card-G2-A_2691 Datenbereitstellung für CV-Zertifikate für Testkarten GE**

Der Testkartenhersteller MUSS die notwendigen Daten zur Erstellung der CV-Zertifikate für HBA und SMC-B an die Test-CVC-CA der Generation 1 (RSA) und für alle Karten an die Test-CVC-CA der Generation 2 (ELC) senden. ⌫

⌦ **Card-G2-A_2692 Erzeugung der CV-Zertifikate für Testkarten GE**

Die Test-CV-Zertifikate für die jeweiligen Testkarten MÜSSEN durch die jeweilige Test-CVC-CA der jeweiligen Generation generiert werden. ⌫

⌦ **Card-G2-A_2693 Name der Test-CVC-CA G1 (Testkarten GE)**

Eine Test-CVC-CA der Generation 1 MUSS einen unter http://sit.sit.fraunhofer.de/_karten_ident/SIT/rid_sde/ZDA.php registrierten CA-Namen besitzen. ⌫

⌦ **Card-G2-A_2694 Name der Test-CVC-CA G2 (Testkarten GE)**

Eine Test-CVC-CA der Generation 2 MUSS einen unter http://sit.sit.fraunhofer.de/_karten_ident/SIT/rid_sde/ZDA.php registrierten CA-Namen besitzen. ⌫

⌦ **Card-G2-A_2695 Bereitstellung des öffentlichen Root-Schlüssels für CV-Zertifikate für Testkarten GE**

Die jeweilige Test-CVC-Root (für RSA und für ELC) MUSS den von ihr verwendeten öffentlichen Root-Schlüssel PuK.RCA.CS.XXXX (XXXX aus der Menge {R2048, E256) an die Testkarten-Hersteller übermitteln. ⌫

⌦ **Card-G2-A_2696 Lieferung der CV-Zertifikate für Testkarten GE**

Die jeweilige Test-CVC-CA MUSS die CV-Zertifikate und das Test-CV-CA-Herausgeberzertifikat an den Testkartenhersteller liefern. ⌫

3.2 Generierung der Vertrauensanker für CV-Zertifikate

3.2.1 Öffentlicher Schlüssel PuK.RCA.CS.XXXX für Testkarten

Siehe Kapitel 3.1.2, [Card-G2-A_2695]

3.2.2 Asymmetrische Schlüsselpaare mit dem öffentlichen Schlüssel PuK.CMS_YYY.AUT_CVC.XXXX für Testkarten GE

⌦ **Card-G2-A_2697 Vertrauensanker PuK.CMS_YYY.AUT_CVC.XXXX für Testkarten GE**

Die zur gegenseitigen Authentifizierung mit asymmetrischen Verfahren zwischen der jeweiligen Karte und dem zugehörenden CMS benötigten öffentlichen Schlüssel

PuK.CMS_YYY.AUT_CVC.E256 (YYY aus der Menge {eGK, HBA, gSMC-KT, KONN, SMC-B} MÜSSEN von der gematik zur Verfügung gestellt werden. Für Testkarten werden keine kartenindividuellen Schlüssel erstellt; die Schlüssel sind für alle Testkarten gleich. ⌫

4 Vorgaben zu symmetrischen Schlüsseln

4.1 Generierung der Secret Keys SK.CMS.AESXXX, SK.VSD.AESXXX und SK.VSDCMS.AESXXX für Testkarten GE

⌦ **Card-G2-A_2698 Bereitstellung symmetrischer Schlüssel für die Testkarten GE**

Die zur gegenseitigen Authentifizierung mit symmetrischen Schlüsseln benötigten Secret Keys SK.CMS.AES128, SK.CMS.AES256, SK.CUP.AES128 (nicht für eGK-Testkarten), SK.CUP.AES256 (nicht für eGK-Testkarten), SK.VSD.AES128 (nur für eGK-Testkarten FD) und SK.VSD.AES256 (nur für eGK-Testkarten FD), werden von der gematik zur Verfügung gestellt. Für Testkarten werden keine kartenindividuellen Schlüssel aus Master Keys abgeleitet; die Schlüssel sind für alle Testkarten gleich. ⌫

5 Vorgaben für eGK-Testkarten GE der Generation 2

⌦ **Card-G2-A_2699 Einhalten der eGK-Spezifikationen für eGK-Testkarten GE**

Die eGK-Testkarten der Generation 2 MÜSSEN alle Vorgaben der eGK-Spezifikation mit Ausnahme der Optionen

- Option kontaktlose Schnittstelle
- Option USB-Schnittstelle
- Option logische Kanäle
- Option Kryptobox

erfüllen. Dies betrifft sowohl die Bereitstellung der definierten Kommandos aus [gemSpec_COS], als auch die Einrichtung der definierten File-Struktur aus [gemSpec_eGK_ObjSys]. ⌫

⌦ **Card-G2-A_2959 Authentifizierung zur Kartenadministration der eGK-Testkarten GE**

Schlüsselobjekte für mindestens eines der oder beide Authentisierungsverfahren für

- symmetrische_Authentifizierung_für_CMS
- asymmetrische_Authentifizierung_für_CMS

MÜSSEN mit Schlüsseln befüllt werden.⌫

5.1 PIN- und PUK-Werte

5.1.1 PIN-Werte

⌦ **Card-G2-A_3203 Werte für eGK-Testkarten GE>**

Die PIN.CH der eGK-Testkarten GE MUSS einheitlich auf den Wert 123456 gesetzt werden.⌫

5.1.2 PUK-Werte

⌦ **Card-G2-A_2701 Werte für PUK für eGK-Testkarten GE**

Die zu den PINs (PIN.CH und PIN.QES) gehörenden PUK-Werte MÜSSEN bei den eGK-Testkarten einheitlich auf den Wert 12345678 gesetzt werden. ⌫

5.1.3 CAN-Wert

⌦ **Card-G2-A_3474 Wert für CAN für eGK-Testkarten GE**

Die für das PACE-Protokoll gefordert 6-stellige Ziffernfolge CAN MUSS bei den eGK-Testkarten GE einheitlich auf den Wert 123123 gesetzt werden. ⌫

5.1.4 Bereitstellung der Daten durch die gematik

⌦ **Card-G2-A_2702 Nutzung von fiktiven Versichertendaten für die eGK-Testkarten GE**

Die Testkarten MÜSSEN Daten von fiktiven Versicherten enthalten. ⌫

⌦ **Card-G2-A_2703 Lieferung der Datensätze für die eGK-Testkarten GE**

Die Datensätze für die eGK-Testkarten MÜSSEN von der gematik in dem vereinbarten Format an den Testkartenhersteller geliefert werden. ⌫

⌦ **Card-G2-A_2704 Übertragung der Datensätze in die eGK-Testkarten GE**

Die von der gematik gelieferten Daten MÜSSEN vom Testkartenkartenhersteller in die entsprechenden EFs geschrieben werden. In diesen Datensätzen sind die IC-CSN-Werte gemäß den in Tab_TK_008 zusammengefassten Vorgaben enthalten. ⌫

⌦ **Card-G2-A_2705 Wert für den Issuer Identifier für die eGK-Testkarten GE**

Als Wert für den Issuer Identifier MUSS der für die gematik als Herausgeber der Testkarten in Tab_TK_008 angegebene Wert verwendet werden.⌫

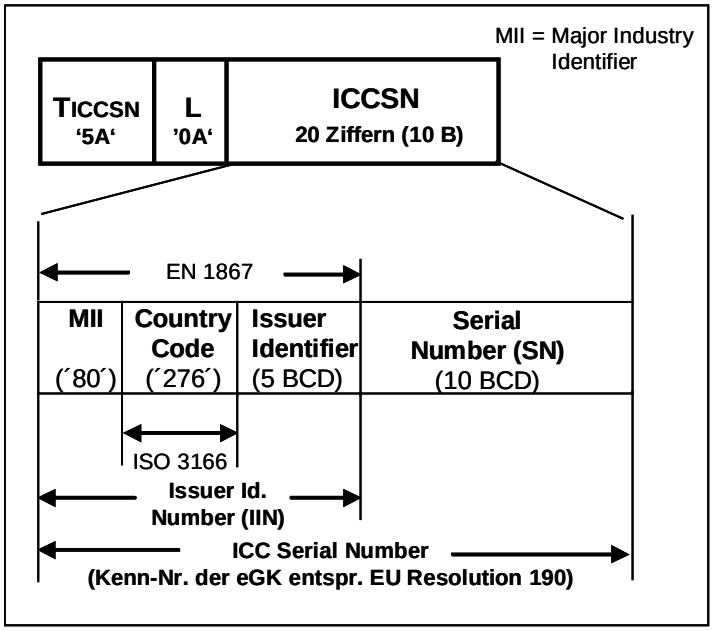


Abbildung 3: Abb_TK_003 ICCSN für Gesundheitskarten

5.2 Erstellung der X.509-Zertifikate für die eGK-Testkarten GE

5.2.1 Erstellung der X.509-Zertifikate für ENC, ENCV, AUT und AUTN bei der jeweiligen CA (Los 3 G2 und Los 4 G2)

⌦ **Card-G2-A_2706 Daten für die X.509-Zertifikate der eGK-Testkarten GE**

Die zur Personalisierung der X.509-Zertifikate in DF.ESIGN notwendigen Daten MÜSSEN vom Kartenhersteller aus den von der gematik gelieferten Datensätzen im spezifizierten Umfang extrahiert und an die jeweilige CA übertragen werden. ⌫

⌦ **Card-G2-A_2707 Erzeugung der X.509-Zertifikate für DF.ESIGN für die eGK-Testkarten GE**

Die X.509-Zertifikate für AUT, AUTN, ENC und ENCV in DF.ESIGN MÜSSEN von der jeweiligen CA in dem in [gemSpec_PKI]#5.1] vorgegebenen Format erstellt werden. Dabei MÜSSEN auch die Vorgaben von [gemSpec_PKI]#4.10] umgesetzt werden. ⌫

⌦ **Card-G2-A_2709 Schlüssellänge in DF.ESIGN für die eGK-Testkarten GE**

Als Schlüssellänge für die zu den jeweiligen X.509-Zertifikaten in DF.ESIGN gehörenden Schlüssel MÜSSEN die in der Spezifikation [gemSpec_eGK_ObjSys#5.5] festgelegten Werte verwendet werden. ⌫

⌦ **Card-G2-A_2710 Gültigkeitsdauer der X.509-Zertifikate für die eGK-Testkarten GE**

Um das Verhalten der Systeme bei abgelaufenen X.509-Zertifikaten in DF.ESIGN testen zu können, MÜSSEN als Gültigkeitszeitraum folgende Werte eingetragen werden:

1. bei 50% der Karten eine Woche
2. Bei 50% der Karten 5 Jahre ab Herstelldatum ⌫

⌦ **Card-G2-A_2711 Identische Gültigkeitsdauer für alle X.509-Zertifikate für die eGK-Testkarten GE**

Alle Zertifikate einer Karte (ENC, ENCV, AUT, AUTN, Pseudo-QES) MÜSSEN dieselbe Gültigkeitsdauer haben. ⌫

⌦ **Card-G2-A_2712 OCSP-Responder für X.509-Zertifikate in DF.ESIGN für die eGK-Testkarten GE**

Der jeweilige TSP MUSS für die von seiner CA gelieferten X.509-Zertifikate einen OCSP-Responder bereitstellen, über den die Gültigkeitsinformation zu den Zertifikaten online abgerufen werden kann. ⌫

⌦ **Card-G2-A_2713 Eintrag von "AuthorityInfoAccess" in X.509-Zertifikate in DF-ESIGN für die eGK-Testkarten GE**

Der Wert für "AuthorityInfoAccess" des OCSP-Responders MUSS in das entsprechende Datenfeld der X.509-Zertifikate in DF.ESIGN eingetragen werden. ⌫

⌦ **Card-G2-A_2714 Lieferung der X.509-Zertifikate für DF.ESIGN für die eGK-Testkarten GE**

Die X.509-Zertifikate für ENC und AUT MÜSSEN von der jeweiligen CA an den Testkartenhersteller geliefert werden. ⌫

5.2.2 Erstellung der X.509-Zertifikate für die Pseudo-QES bei der jeweiligen CA (Los 3 G2 und Los 4 G2) für die eGK-Testkarten GE

⌦ **Card-G2-A_2715 Anlegen von DF.QES für die eGK-Testkarten GE**

Das DF.QES MUSS vom Testkartenhersteller mit den in [gemSpec_eGK_ObjSys#5.1] angegebenen EFs, mit den definierten Security- und Access-Conditions und einem Zertifikat sowie einem Schlüsselpaar für eine Pseudo-QES angelegt werden. ⌫

⌦ **Card-G2-A_2716 Personalisierung des X.509-Zertifikats in DF.QES für die eGK-Testkarten GE**

Die zur Personalisierung der QES-Zertifikate notwendigen Daten MÜSSEN vom Testkartenhersteller aus den von der gematik gelieferten Datensätzen im spezifizierten Umfang extrahiert und an die jeweilige CA zur Erstellung von Zertifikaten für die Pseudo-QES übertragen werden. ⌫

⌦ **Card-G2-A_2717 Erzeugung der X.509-Zertifikate für DF.QES für die eGK-Testkarten GE**

Das Zertifikat für die optionale Pseudo-QES MUSS von der jeweiligen CA in dem in [gemSpec_PKI] vorgegebenen Format für die Pseudo-QES erstellt werden. ⌫

⌦ **Card-G2-A_2718 Schlüssellänge in DF.QES für die eGK-Testkarten GE**

Als Schlüssellänge für den zur Pseudo-QES gehörenden Schlüssel MUSS der in der Spezifikation [gemSpec_eGK_ObjSys#5.1] festgelegte Wert verwendet werden. ⌫

⌦ **Card-G2-A_2878 Vorgaben für die PIN.QES für die eGK-Testkarten GE**

Bei 50 % der eGK-Testkarten MUSS PIN.QES einheitlich auf den Wert 123456 gesetzt werden.

Bei 50% der eGK-Testkarten MUSS PIN.QES mit dem in der Spezifikation zugelassenen Transport-PIN-Verfahren (Transport-PIN 5-stellig) kodiert werden. Die Transport-PIN MUSS für diese Karten auf den Wert 54321 gesetzt werden.⌫

Anmerkung: Es wird empfohlen, bei der Umwandlung der Transport-PIN in eine Echt-PIN ebenfalls die Eingabe der Ziffernfolge 123456 als Echt-PIN vorzuschreiben.

⌦ **Card-G2-A_2719 OCSP-Responder für X.509-Zertifikate in DF-QES für die eGK-Testkarten GE**

Der jeweilige TSP MUSS für die von seiner CA gelieferten Zertifikate einen OCSP-Responder bereitstellen, von dem die Gültigkeitsinformation zu den Zertifikaten online abgerufen werden kann. ⌫

⌦ **Card-G2-A_2720 Eintrag von "AuthorityInfoAccess" in X.509-Zertifikate in DF-QES für die eGK-Testkarten GE**

© gematik – öffentlich

Der Wert für "AuthorityInfoAccess" MUSS in das entsprechende Datenfeld der X.509-Zertifikate in DF.QES eingetragen werden. ⌫

⌦ **Card-G2-A_2721 Lieferung der X.509-Zertifikate für DF.QES für die eGK-Testkarten GE**

Die Zertifikate für die Pseudo-QES MÜSSEN von der jeweiligen CA an den Testkartenhersteller geliefert werden. ⌫

5.2.3 OID-Vorgaben für eGK-Testkarten

⌦ **Card-G2-A_2722 OID-Vorgaben für die eGK-Testkarten GE**

In alle X.509-Zertifikate der Testkarten MÜSSEN gemäß [gemSpec_PKI] OIDs und Texte eingetragen werden. Die in Tab_TK_001 angegebenen Referenzbezeichnungen MÜSSEN über das Dokument [gemSpec_OID] aufgelöst werden.

Tabelle 1: Tab_TK_001 OID-Referenzen für eGK-Testkarten GE (verpflichtend)

Speicherort	OID-Referenz
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.CH.ENC.R2048, C.CH.ENCV.R2048, C.CH.AUT.R2048, C.CH.AUTN.R2048, falls vorhanden: C.CH.QES.R2048	oid_versicherter
CertificatePolicies, in allen Zertifikaten (C.CH.ENC.R2048, C.CH.ENCV.R2048, C.CH.AUT.R2048, C.CH.AUTN.R2048, falls vorhanden: C.CH.QES.R2048 oder C.CH.SIG.R2048)	oid_policy_gem_or_cp
CertificatePolicies in C.CH.ENC.R2048	oid_egk_enc
CertificatePolicies in C.CH.ENCV.R2048	oid_egk_encv
CertificatePolicies in C.CH.AUT.R2048	oid_egk_aut
CertificatePolicies in C.CH.AUTN.R2048	oid_egk_autn
CertificatePolicies in C.CH.SIG QES.R2048	oid_egk_qes

⌫

5.3 CV-Zertifikate für die eGK -Testkarten GE der Generation 2

Es gelten die Anforderungen aus Kapitel 3

5.4 Secret Keys SK.CMS.AES128, SK.VSD.AES128 und SK.VSDCMS.AES128 für die eGK-Testkarten GE der Generation 2

Es gelten die Anforderungen aus Kapitel 4

5.5 Optische Gestaltung der eGK Testkarten GE der Generation 2

Card-G2-A_2723 Maße der eGK-Testkarten GE

Für die Maße der eGK-Testkarten der Generation 2 MÜSSEN die Maße aus [gemSpec_eGK_OPT] gelten.

Card-G2-A_2724 optische Gestaltung der eGK-Testkarten GE ohne Bild

Die optische Gestaltung der Vorderseite der eGK-Testkarten der Generation 2 ohne Bild MUSS gemäß Abb_TK_004 (Ausnahme Produktionskennzeichnung, siehe Card-G2-A_2734) ausgeführt werden.

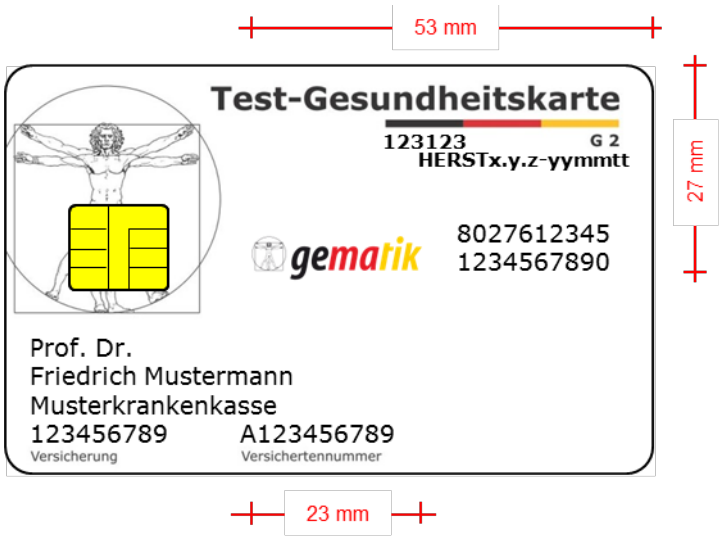


Abbildung 4: Abb_TK_004 Kartenvorderseite der eGK-Testkarten GE mit Personalisierung, ohne Bild, Bemaßung für Logo-Position, mit Produktionskennzeichnung

Card-G2-A_2725 optische Gestaltung der eGK-Testkarten GE mit Bild

Die optische Gestaltung der Vorderseite der eGK-Testkarten der Generation 2 mit Bild MUSS gemäß Abb_TK_005 (Ausnahme Produktionskennzeichnung, siehe Card-G2-A_2734) ausgeführt werden:

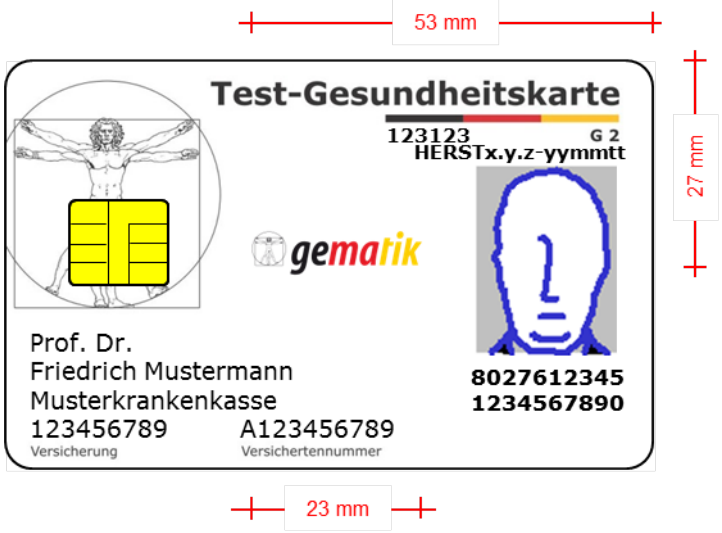


Abbildung 5: Abb_TK_005 Kartenvorderseite der eGK-Testkarten GE mit Personalisierung, mit Bild, Bemaßung für Logo-Position, mit Produktionskennzeichnung

⌫

Die Anordnung ICCSN ist beispielhaft.

⌦ **Card-G2-A_2734 Produktionskennzeichnung der eGK-Testkarten GE**

Der Hersteller KANN das fünfstellige Herstellerkürzel und die Versionsnummer des auf der Karte vorhandenen Objektsystems sowie eine Datumsangabe, im Format HERSTx.y.z-yymmtt (yymmtt = Jahr Monat Tag, je zweistellig mit jeweils führender Null) in der Schriftart Verdana True Type in der Größe 6 pt fett in Schwarz auf die Vorderseite (gemäß Abb_TK_004 und Abb_TK_005 rechtsbündig zum Text G2) oder auf die Rückseite (zusammen mit der ICCSN, falls kein EHIC-Feld vorhanden ist) drucken.

Die Werte für Herstellerkürzel und Versionsnummer MÜSSEN dabei den Werten aus DO_PI_InitialisiertesObjSys in EF.ATR des Objektsystems der eGK entsprechen.

Die Datumsangabe MUSS geeignet gewählt sein, um einzelne Produktionschargen der Personalisierung identifizieren zu können und MUSS im Datumsbereich zwischen Beauftragung und Lieferung der entsprechenden Produktionscharge liegen.

⌫

⌦ **Card-G2-A_2726 Kennzeichnung als eGK-Testkarten GE**

Dem Schriftzug „Gesundheitskarte“ gemäß [gemSpec_eGK_OPT] MUSS in gleicher Schriftart das Wort „Test-“ vorangestellt werden. ⌫

⌦ **Card-G2-A_2727 Schriftzug G2 auf eGK-Testkarten GE**

Der Schriftzug „G 2“ MUSS gemäß [gemSpec_eGK_OPT] aufgebracht werden. ⌫

⌦ **Card-G2-A_2728 Daten zur Person auf eGK-Testkarten GE**

Die zur Personalisierung der eGK-Testkarten notwendigen Daten MÜSSEN vom Kartenhersteller aus den von der gematik gelieferten Datensätzen im spezifizierten Umfang extrahiert und auf die Karten gedruckt werden. ⌫

⌦ **Card-G2-A_2729 Regeln für die Vergabe von IK, IIN und VKNR für die eGK-Testkarten GE**

Die Regeln für die Vergabe von IK der Krankenkasse, zur IIN des Kartenherausgebers und zur Versichertennummer, die im Anhang B festgelegt sind, MÜSSEN eingehalten werden. ⌫

⌦ **Card-G2-A_2730 BSI-Logo auf eGK-Testkarten GE**

Das BSI-Logo DARF NICHT auf die eGK-Testkarten aufgedruckt werden. ⌫

Für eGK-Testkarten ist eine Fotopersonalisierung nicht verpflichtend.

⌦ **Card-G2-A_2731 ICCSN für Testkarten GE**

Die ICCSN MUSS auf die eGK-Testkarten aufgedruckt werden. ⌫

⌦ **Card-G2-A_2732 ICCSN auf eGK-Testkarten GE mit Fotopersonalisierung**

Wird die eGK-Testkarte mit einem Foto gemäß [gemSpec_eGK_OPT] versehen, MUSS die ICCSN entweder an anderer Stelle der Vorderseite (Beispiel siehe Abbildung Abb_TK_005) oder auf die Rückseite (z. B. im dafür vorgesehenen EHIC-Feld, falls vorhanden) aufgedruckt werden. ⌫

⌦ **Card-G2-A_2733 ICCSN auf eGK-Testkarten GE ohne Fotopersonalisierung**

Bei eGK-Testkarten ohne Fotopersonalisierung KANN die ICCSN in der für das Fotovorgesehenen Fläche in zwei Zeilen mit je 10 Stellen je Zeile gemäß Abb_TK_004 aufgedruckt werden. Ausrichtung rechtsbündig zum Schriftzug „Gesundheitskarte“. Schrift analog der sonstigen Personalisierung auf der Vorderseite. ⌫

⌦ **Card-G2-A_3475 CAN-Aufdruck für die eGK-Testkarten GE**

Die in NEU-AFO_0001 definierte 6-stellige CAN MUSS in der Schriftart Verdana True Type in der Größe 6 pt fett in Schwarz an folgender Position auf die eGK-Testkarten gedruckt werden: Unterkante der Schrift 10,5 mm; linksbündig bei 50,00 mm (siehe Abb_TK_004 und Abb_TK_005)⌫

⌦ **Card-G2-A_2960 Logo der gematik auf den eGK-Testkarten GE**

Gemäß Abb_TK_004 und Abb_TK_005 MUSS das Logo der gematik (Datei „Bildvorlage Logo_Gematik_2012.eps“ bzw. „Logo_Gematik_2012_Transparent.png“) in einer Breite von 23 mm in folgender Position aufgedruckt werden:

- Linker Rand des Logos 53 mm vom rechten Rand entfernt.
- Schriftunterkante (Unterkante Mittellänge) 27 mm vom oberen Kartenrand entfernt.⌫

⌦ **Card-G2-A_2735 Rückseite der eGK-Testkarten GE**

Die Kartenrückseite der Testkarte MUSS entweder unbedruckt sein (mögliche Ausnahme siehe Card-G2-A_2732) oder mit einer entwerteten EHIC bedruckt werden.

Im Falle einer Bedruckung mit einer EHIC:

a) MUSS die Gestaltung der EHIC den Beschlüssen der Verwaltungskommission für die soziale Sicherheit der Wanderarbeitnehmer in der Europäischen Union entsprechen [Beschluss 190]. Die Gestaltung ist somit grundsätzlich vorgegeben.

b) MUSS die Entwertung durch Füllen der Felder der EHIC mit einer Reihe des Zeichens „X“ erfolgen (mögliche Ausnahme für das Feld ICCSN siehe Card-G2-A_2732). Dabei MUSS jedes Feld mit der Maximalanzahl von Stellen gefüllt werden.⌫

⌦ **Card-G2-A_2736 Nutzung der gematik-Vorlagen zur Bedruckung der eGK-Testkarten GE**

Für die Bedruckung der eGK-Testkarten mit den unveränderbaren Elementen MÜSSEN die entsprechenden Vorlagen genutzt werden, die im Download-Bereich der gematik-Website zur Verfügung gestellt sind. ⌫

5.6 Daten zur Erstellung von eGK-Testkarten GE der Generation 2

⌦ **Card-G2-A_2737 Datenlieferung durch die gematik für eGK-Testkarten GE**

Die gematik MUSS folgende Daten für die Produktion von eGK-Testkarten an den Kartenhersteller liefern:

- Auftragsformular mit den für alle Karten geltenden Daten:
- Stückzahl
- Datensätze für die eGK-Testkarten in dem vereinbarten Format.
- Datensätze mit den AES-Schlüsselpaaren SK.CMS.ENC.AES128, SK.CMS.MAC.AES128, SK.VSDCMS.ENC.AES128, SK.VSDCMS.MAC.AES128, SK.VSD.ENC.AES128 und SK.VSD.MAC.AES128
- Datensätze mit den AES-Schlüsselpaaren SK.CMS.ENC.AES256, SK.CMS.MAC.AES256, SK.VSDCMS.ENC.AES256, SK.VSDCMS.MAC.AES256, SK.VSD.ENC.AES256 und SK.VSD.MAC.AES256
- Datensatz mit den öffentlichen Schlüsseln gemäß Kapitel 3.2.1 und 3.2.2, falls nicht schon vorhanden.
- Datensatz mit dem öffentlichen CV-Schlüssel gemäß 3.2.2, falls nicht schon vorhanden. ⌫

5.7 Lieferung der eGK-Testkarten GE der Generation 2

⌦ **Card-G2-A_2738 Lieferung der eGK-Testkarten GE durch den Kartenhersteller**

Die eGK-Testkarten MÜSSEN vom Kartenhersteller an die gematik geschickt werden. Sie werden dort getestet, erfasst und anschließend weiter versendet. ⌫

6 Vorgaben für die HBA-Testkarten GE der Generation 2

⌦ **Card-G2-A_2739 Einhalten der HBA-Spezifikationen für die HBA-Testkarten GE**

Die HBA-Testkarten MÜSSEN alle Vorgaben der HBA-Spezifikation der Generation 2 mit Ausnahme der Optionen

- Option kontaktlose Schnittstelle
- Option USB-Schnittstelle
- Option Kryptobox

erfüllen. Dies betrifft sowohl die Bereitstellung der definierten Kommandos aus [gemSpec_COS] als auch die Einrichtung der definierten File-Struktur aus [gemSpec_HBA_ObjSys]. ⌫

⌦ **Card-G2-A_2961 Authentifizierung zur Kartenadministration der HBA-Testkarten GE**

Die Schlüsselobjekte für eines der oder beide Authentisierungsverfahren für

- symmetrische_Authentifizierung_für_CMS
- asymmetrische_Authentifizierung_für_CMS

KÖNNEN mit Schlüsseln befüllt werden.⌫

6.1 PIN- und PUK-Werte

6.1.1 PIN-Werte

⌦ **Card-G2-A_2740 Wert für PIN für die HBA-Testkarten GE**

Bei 50 % der HBA-Testkarten MÜSSEN PIN.CH, PIN.AUTO und PIN.SO einheitlich auf den Wert 123456 gesetzt werden.

Bei 50% der HBA-Testkarten MÜSSEN PIN.CH, PIN.AUTO und PIN.SO mit dem in der Spezifikation zugelassenen Transport-PIN-Verfahren (Transport-PIN 5-stellig) kodiert werden. Die Transport-PIN MUSS für diese Karten auf den Wert 54321 gesetzt werden.⌫

Anmerkung: Es wird empfohlen, bei der Umwandlung der Transport-PIN in eine Echt-PIN ebenfalls die Eingabe der Ziffernfolge 123456 als Echt-PIN vorzuschreiben.

6.1.2 PUK-Werte

⌦ **Card-G2-A_2741 Werte für PUK für die HBA-Testkarten GE**

Die zu den PINs (PIN.CH, PIN.AUTO, PIN.SO und PIN.QES) gehörenden PUK-Werte MÜSSEN bei den HBA-Testkarten einheitlich auf den Wert 12345678 gesetzt werden. ⌫

6.1.3 CAN-Wert

⌦ **Card-G2-A_3476 Wert für CAN für HBA-Testkarten GE**

Die für das PACE-Protokoll gefordert 6-stellige Ziffernfolge CAN MUSS bei den HBA-Testkarten GE einheitlich auf den Wert 123123 gesetzt werden. ⌫

6.2 Erstellung der X.509-Zertifikate für ENC und AUT der HBA-Testkarten GE bei der jeweiligen CA (Los 3 G2 und Los 4 G2)

⌦ **Card-G2-A_2962 Nutzung von fiktiven Leistungserbringerdaten für die HBA-Testkarten GE**

Die Zertifikate der HBA-Testkarten MÜSSEN Daten von fiktiven Leistungserbringern enthalten.⌫

⌦ **Card-G2-A_2742 Übertragung der Datensätze in die HBA-Testkarten GE**

Die zur Personalisierung der Zertifikate der HBA-Testkarten notwendigen Daten MÜSSEN vom Kartenhersteller aus den von der gematik gelieferten Datensätzen im spezifizierten Umfang extrahiert und an die jeweilige CA übertragen werden. ⌫

⌦ **Card-G2-A_2743 Erzeugung der X.509-Zertifikate für DF.ESIGN für die HBA-Testkarten GE**

Die Zertifikate für AUT und ENC MÜSSEN von der jeweiligen CA in dem in [gemSpec_PKI]#5.2] vorgegebenen Format erstellt werden. Dabei MÜSSEN auch die Vorgaben von [gemSpec_PKI]#4.10] umgesetzt werden. ⌫

⌦ **Card-G2-A_2744 Schlüssellänge in DF.ESIGN für die HBA-Testkarten GE**

Als Schlüssellänge für die zugehörenden Schlüssel MÜSSEN die in der Spezifikation [gemSpec_HBA_ObjSys#4.6.2] festgelegten Werte verwendet werden. ⌫

⌦ **Card-G2-A_2745 Gültigkeitsdauer der X.509-Zertifikate für die HBA-Testkarten GE**

Um das Verhalten der Systeme bei abgelaufenen X.509-Zertifikaten testen zu können, MÜSSEN als Gültigkeitszeitraum folgende Werte eingetragen werden:

1. bei 50% der Karten eine Woche
2. bei 50% der Karten 5 Jahre ab Herstelldatum ⌫

⌦ **Card-G2-A_2746 Identische Gültigkeitsdauer für alle X.509-Zertifikate für die HBA-Testkarten GE**

Alle X.509-Zertifikate einer Karte (ENC, AUT, Pseudo-QES) MÜSSEN dieselbe Gültigkeitsdauer haben. ⌫

⌦ **Card-G2-A_3044 Festlegung der Telematik-ID für HBA-Testkarten GE**

Die Telematik-ID für HBA-Testkarten GE MUSS mit folgenden Werten in die X.509-Zertifikate der jeweiligen HBA-Testkarte GE eingetragen werden:

Testkarten Ärztin/Arzt:: 1-HBA-Testkarte-<ICCSN15>

Testkarten Zahnärztin/Zahnarzt: 2-HBA-Testkarte-<ICCSN15>

Testkarten Psychotherapeut/-in: 4-HBA-Testkarte-<ICCSN15>

Für <ICCSN15> MÜSSEN die letzten 15 Stellen der ICCSN der jeweiligen Karte verwendet werden.⌫

⌦ **Card-G2-A_2747 OCSP-Responder für X.509-Zertifikate in DF.ESIGN für die HBA-Testkarten GE**

Der jeweilige TSP MUSS für die von seiner CA gelieferten X.509-Zertifikate einen OCSP-Responder bereitstellen, über den die Gültigkeitsinformation zu den Zertifikaten online abgerufen werden kann. ⌫

⌦ **Card-G2-A_2748 Eintrag von "AuthorityInfoAccess" in X.509-Zertifikate in DF-ESIGN für die HBA-Testkarten GE**

Der Wert für "AuthorityInfoAccess" des OCSP-Responders MUSS in das entsprechende Datenfeld der X.509-Zertifikate in DF.ESIGN eingetragen werden. ⌫

⌦ **Card-G2-A_2749 Lieferung der X.509-Zertifikate für DF.ESIGN für die HBA-Testkarten GE**

Die X.509-Zertifikate für ENC und AUT MÜSSEN von der jeweiligen CA an den Testkartenhersteller geliefert werden. ⌫

6.2.1 Erstellung der X.509-Zertifikate für die Pseudo-QES bei der jeweiligen CA (Los 3 G2 und Los 4 G2) für die HBA-Testkarten GE

⌦ **Card-G2-A_2750 Anlegen von DF.QES für die HBA-Testkarten GE**

Das DF.QES MUSS vom Testkartenhersteller mit den in [gemSpec_HBA_ObjSys#4.5.2] angegebenen EFs, mit den definierten Security- und Access-Conditions und einem Zertifikat sowie einem Schlüsselpaar für eine Pseudo-QES angelegt werden. ⌫

⌦ **Card-G2-A_2751 Personalisierung des X.509-Zertifikats in DF.QES für die HBA-Testkarten GE**

Die zur Personalisierung der QES-Zertifikate notwendigen Daten MÜSSEN vom Testkartenhersteller aus den von der gematik gelieferten Datensätzen im spezifizierten Umfang (siehe [gemSpec_PKI#5.2]) extrahiert und an die jeweilige CA zur Erstellung von Zertifikaten für die Pseudo-QES übertragen werden. ⌫

⌦ **Card-G2-A_2752 Erzeugung der X.509-Zertifikate für DF.QES für die HBA-Testkarten GE**

Die Zertifikate für die Pseudo-QES einschließlich der Attributzertifikate MÜSSEN von der jeweiligen CA in dem in [gemSpec_PKI#5.2] vorgegebenen Format für die Pseudo-QES erstellt werden. ⌫

⌦ **Card-G2-A_2753 Schlüssellänge in DF.QES für die HBA-Testkarten GE**

Als Schlüssellänge für den zur Pseudo-QES gehörenden Schlüssel MUSS der in der Spezifikation [gemSpec_HBA_ObjSys#4.5.2] festgelegte Wert verwendet werden. ⌫

⌦ **Card-G2-A_2879 Vorgaben für die PIN.QES für die HBA-Testkarten GE**

Bei 50 % der HBA-Testkarten MUSS PIN.QES einheitlich auf den Wert 123456 gesetzt werden.

Bei 50% der HBA-Testkarten MUSS PIN.CH mit dem in der Spezifikation zugelassenen Transport-PIN-Verfahren (Transport-PIN 5-stellig) kodiert werden. Die Transport-PIN MUSS für diese Karten auf den Wert 54321 gesetzt werden.⌫

Anmerkung: Es wird empfohlen, bei der Umwandlung der Transport-PIN in eine Echt-PIN ebenfalls die Eingabe der Ziffernfolge 123456 als Echt-PIN vorzuschreiben.

⌦ **Card-G2-A_2754 OCSP-Responder für X.509-Zertifikate in DF-QES für die HBA-Testkarten GE**

Der jeweilige TSP MUSS für die von seiner CA gelieferten Zertifikate einen OCSP-Responder bereitstellen, von dem die Gültigkeitsinformation zu den Zertifikaten online abgerufen werden kann. ⌫

⌦ **Card-G2-A_2755 Eintrag von "AuthorityInfoAccess" in X.509-Zertifikate in DF-QES für die HBA-Testkarten GE**

Der Wert für "AuthorityInfoAccess" MUSS in das entsprechende Datenfeld der X.509-Zertifikate in DF.QES eingetragen werden. ⌫

⌦ **Card-G2-A_2756 Lieferung der X.509-Zertifikate für DF.QES für die HBA-Testkarten GE**

Die Zertifikate einschließlich der Attributzertifikate für die Pseudo-QES MÜSSEN von der jeweiligen CA an den Testkartenhersteller geliefert werden. ⌫

6.2.2 OID-Vorgaben für die HBA-Testkarten GE

⌦ **Card-G2-A_2757 OID-Vorgaben für die HBA-Testkarten GE**

In die X.509-Zertifikate der HBA-Testkarten der Generation 2 MÜSSEN gemäß den Festlegungen durch die Leistungserbringerorganisationen OIDs und Texte eingetragen werden. In Tab_TK_002 sind die Referenzbezeichnungen angegeben. Die zugehörigen OIDs/Texte befinden sich im Dokument [gemSpec_OID].

Tabelle 2: Tab_TK_002 OID-Referenzen für HBA-Testkarten GE (verpflichtend)

Speicherort	OID-Referenz
Admission: ProfessionItem und ProfessionOID in allen Basiszertifikaten (C.HP.QES.R2048, C.HP.AUT.R2048, C.HP.ENC.R2048) für Ärzte	oid_arzt
Admission: ProfessionItem und ProfessionOID in allen Basiszertifikaten (C.HP.QES.R2048, C.HP.AUT.R2048, C.HP.ENC.R2048) für Zahnärzte	oid_zahnarzt
Admission: ProfessionItem und ProfessionOID in allen Basiszertifikaten	oid_apotheker

Speicherort	OID-Referenz
(C.HP.QES.R2048, C.HP.AUT.R2048, C.HP.ENC.R2048) für Apotheker	
Admission: ProfessionItem und ProfessionOID in allen Basiszertifikaten (C.HP.QES.R2048, C.HP.AUT.R2048, C.HP.ENC.R2048) für Psychotherapeuten	oid_psychotherapeut
CertificatePolicies, alle Zertifikate	oid_policy_gem_or_cp
CertificatePolicies in C.HP.ENC.R2048	oid_hba_enc
CertificatePolicies in C.HP.QES-AC1.R2048	oid_hba_qes
CertificatePolicies in C.HP.AUT.R2048	oid_hba_aut

⌫

6.3 CV-Zertifikate für die HBA-Testkarten GE der Generation 2

Es gelten die Vorgaben aus Kapitel 3.

6.4 Secret Keys SK.CMS.AES128 und SK.CMS.AES256 für die HBA-Testkarten GE der Generation 2

Es gelten die Anforderungen aus Kapitel 4

6.5 Optische Gestaltung der HBA-Testkarten GE der Generation 2

⌦ **Card-G2-A_2758 optische Gestaltung der HBA-Testkarten GE**

Die optische Gestaltung der Vorderseite der HBA-Testkarten der Generation 2 MUSS gemäß Abb_TK_006 ausgeführt werden:

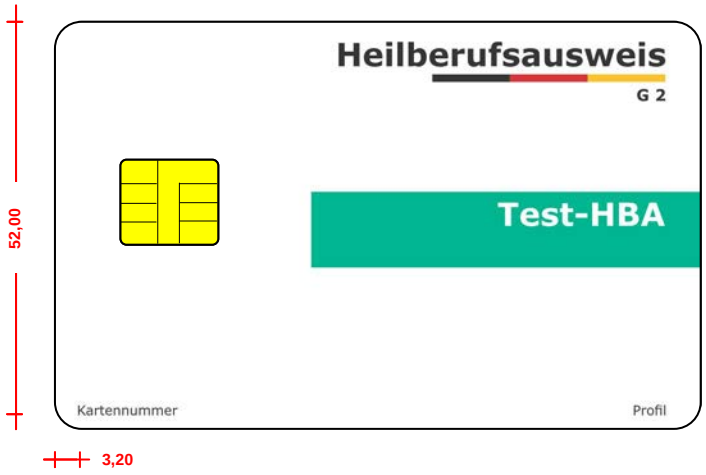


Abbildung 6: Abb_TK_006 Kartenvorderseite der HBA-Testkarten GE, konstante Elemente

⌫

⌦ **Card-G2-A_2759 Schriftzug „Heilberufsausweis“ für die Beschriftung der HBA-Testkarten GE**

Der Schriftzug „Heilberufsausweis“ und rechtsbündig darunter ein Block in den nationalen Farben MÜSSEN vorhanden sein, um den Anwendungsbereich des HBAs zu kennzeichnen. ⌫

⌦ **Card-G2-A_2760 Kennzeichnung „Generation“ für die Beschriftung der HBA-Testkarten GE**

Die Zugehörigkeit der HBA-Testkarten zur Generation 2 MUSS optisch erkennbar sein. Deshalb MUSS unter dem Block in den nationalen Farben rechtsbündig die Zeichenfolge „G 2“ eingefügt werden. ⌫

⌦ **Card-G2-A_2761 Positionierung Schriftzug „Heilberufsausweis“ für die Beschriftung der HBA-Testkarten GE**

Die Maße aus Abb_TK_006 bezüglich der Position der Elemente „Schriftzug Heilberufsausweis“ und „Kennzeichnung Generation“ des HBA MÜSSEN eingehalten werden. ⌫

⌦ **Card-G2-A_2762 Schriftart Schriftzug Heilberufsausweis für die Beschriftung der HBA-Testkarten GE**

Für das Wort „Heilberufsausweis“ des HBA MUSS die Schriftart Verdana True Type in der Größe 12 pt fett in Schwarz verwendet werden. ⌫

⌦ **Card-G2-A_2763 Farbblock für die Beschriftung der HBA-Testkarten GE**

Die HBA-Testkarten MÜSSEN durch einen auffälligen Farbblock in Türkis (HKS 53) gekennzeichnet werden. ⌫

⌦ **Card-G2-A_2764 Beschriftung der HBA-Testkarten GE mit „Test-HBA“**

Die Beschriftung „Test-HBA“ MUSS in diesem Farbbalken in Verdana True Type fett 22 pt ausgeführt werden.⌫

⌦ **Card-G2-A_2765 Negativdruck für die Beschriftung der HBA-Testkarten GE mit „Test-HBA“**

Die Beschriftung „Test-HBA“ SOLL vorzugsweise im Negativdruck erfolgen. ⌫

⌦ **Card-G2-A_2766 Alternative zum Negativdruck für die Beschriftung der HBA-Testkarten GE mit „Test-HBA“**

Die Ausführung der Beschriftung „Test-HBA“ KANN in Schwarz verwendet werden, wenn die Anfertigung des Negativdrucks hohen Aufwand verursachen würde. ⌫

⌦ **Card-G2-A_2767 Rolle des Karteninhabers der HBA-Testkarten GE**

In dem Farbblock MUSS bei der Personalisierung die Rolle des Karteninhabers im Klartext in Verdana True Type fett 22 pt, Farbe Schwarz, rechtsbündig zu „Heilberufsausweis“ und „Test-HBA“ aufgedruckt werden (Beispiel Arzt siehe Abb_TK_007).⌫

⌦ **Card-G2-A_2768 Kennzeichnung der Generation G2 für die HBA-Testkarten GE**

Der Schriftzug „G 2“ MUSS in Verdana True Type 6 pt fett, Farbe Schwarz, rechtsbündig zu „Heilberufsausweis“ und dem Block in den nationalen Farben aufgebracht werden. ⌫

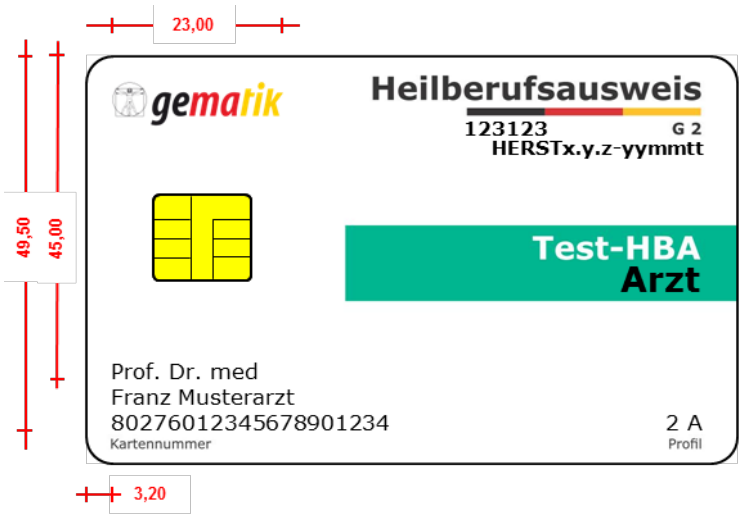


Abbildung 7: Abb_TK_007 Kartenvorderseite, Personalisierung für Ärztin/Arzt (beispielhaft) mit CAN, mit Produktionskennzeichnung

⌦ **Card-G2-A_2769 Daten zu Karteninhaber und Profil für die HBA-Testkarten GE**

Die zur Personalisierung der HBA-Testkarten notwendigen Daten MÜSSEN vom Kartenhersteller aus den von der gematik gelieferten Datensätzen im vorgegebenen Umfang (siehe [Card-G2-A_2770]) extrahiert und auf die Karten gedruckt werden. ⌫

⌦ **Card-G2-A_2770 Platzierung der Daten zum Karteninhaber für die HBA-Testkarten GE**

Die Daten zum Karteninhaber (Titel, Name und ICCSN) MÜSSEN gemäß Abb_TK_007 über dem Schriftzug „Kartennummer“ dreizeilig (jeder Bestandteil in einer Zeile) linksbündig aufgedruckt werden. ⌫

⌦ **Card-G2-A_2773 Produktionskennzeichnung der HBA-Testkarten GE**

Der Hersteller KANN gemäß Abb_TK_007 das fünfstellige Herstellerkürzel und die Versionsnummer des auf der Karte vorhandenen Objektsystems sowie eine Datumsangabe, im Format HERSTx.y.z-yymmtt (yymmtt = Jahr Monat Tag, je zweistellig mit jeweils führender Null) in der Schriftart Verdana True Type in der Größe 6 pt fett in Schwarz rechtsbündig zum Text G2 auf die Vorderseite drucken.

Die Werte für Herstellerkürzel und Versionsnummer MÜSSEN dabei den Werten aus DO_PI_InitialisiertesObjSys in EF.ATR des Objektsystems des HBA entsprechen.

Die Datumsangabe MUSS geeignet gewählt sein, um einzelne Produktionschargen der Personalisierung identifizieren zu können und MUSS im Datumsbereich zwischen Beauftragung und Lieferung der entsprechenden Produktionscharge liegen. ⌫

⌦ **Card-G2-A_2771 Platzierung der Daten zum Profil für die HBA-Testkarten GE**

Der Zahlenwert des Profils MUSS gemäß Abb_TK_007 über dem Schriftzug „Profil“ rechtsbündig aufgedruckt werden. ⌫

⌦ **Card-G2-A_2880 Bedruckung der HBA-Testkarten GE mit Herstellerangaben**

Im Bereich zwischen dem Farbblock gemäß [Card-G2-A_2763] und dem Schriftzug „Heilberufsausweis“ KÖNNEN Informationen zum Kartenhersteller aufgedruckt werden.⌫

⌦ **Card-G2-A_2772 Quelle für Daten zum Karteninhaber und zum Profil für die HBA-Testkarten GE**

Die Daten zum Heilberufler und zum zugehörigen Profil (Arzt = Profil 2 A, Zahnarzt = Profil 2 ZA, Apotheker = Profil 3, Psychotherapeut = Profil 4) MÜSSEN dem jeweils verwendeten Datensatz entnommen werden. ⌫

Für die HBA-Testkarten ist keine Fotopersonalisierung vorgesehen.

⌦ **Card-G2-A_3477 CAN-Aufdruck für die HBA-Testkarten GE**

Die in Card-G2-A_3476 definierte 6-stellige CAN MUSS auf die HBA-Testkarten in der Schriftart Verdana True Type in der Größe 6 pt fett in Schwarz an folgender Position auf den HBA gedruckt werden: Unterkante der Schrift 10,5 mm; linksbündig bei 50,00 mm (siehe Abb_TK_007)⌫

⌦ **Card-G2-A_2963 Logo der gematik auf den HBA-Testkarten GE**

Gemäß Abb_TK_007 MUSS das Logo der gematik (Datei „Bildvorlage Logo_Gematik_2012.eps“ bzw. „Logo_Gematik_2012_Transparent.png“) in einer Breite von 23 mm in folgender Position aufgedruckt werden:

- Linker Rand des Logos 3,2 mm vom linken Rand der Karte entfernt
- Schriftunterkante (Unterkante Mittellänge) in gleicher Position wie die Unterkante des Balkens in den nationalen Farben. ⌫

⌦ **Card-G2-A_2774 Farbe der Kartenrückseite der HBA-Testkarten GE**

Die Kartenrückseiten der HBA-Testkarten MÜSSEN weiß sein. ⌫

⌦ **Card-G2-A_2775 Nutzung der gematik-Vorlagen zur Bedruckung der HBA-Testkarten GE**

Für die Bedruckung der HBA-Testkarten mit den unveränderbaren Elementen MÜSSEN die entsprechenden Vorlagen genutzt werden, die im Download-Bereich der gematik-Website (www.gematik.de) zur Verfügung gestellt sind. ⌫

6.6 Daten zur Erstellung von HBA-Testkarten GE der Generation 2

⌦ **Card-G2-A_2776 Datenlieferung durch die gematik für die HBA-Testkarten GE**

Die gematik MUSS folgende Daten für die Produktion von HBA-Testkarten an den Kartenhersteller liefern:

- Auftragsformular mit den für alle Karten geltenden Daten

- Stückzahl
- Datensätze für die HBA-Testkarten in dem vereinbarten Format.
- Datensatz mit dem AES-Schlüsselpaar SK.CMS.ENC.AES128 und SK.CMS.MAC.AES128, falls nicht schon vorhanden.
- Datensatz mit dem AES-Schlüsselpaar SK.CMS.ENC.AES256, SK.CMS.MAC.AES256, falls nicht schon vorhanden.
- Datensatz mit dem öffentlichen CV-Schlüssel gemäß 3.2.2, falls nicht schon vorhanden. ⌫

6.7 Lieferung der HBA-Testkarten GE der Generation 2

⌦ **Card-G2-A_2777 Lieferung der HBA-Testkarten GE durch den Kartenhersteller**

Die HBA-Testkarten MÜSSEN vom Kartenhersteller an die gematik geschickt werden. Sie werden dort getestet, erfasst und anschließend weiter versendet. ⌫

© gematik – öffentlich

7 Vorgaben für die SMC-B-Testkarten GE der Generation 2

⌦ **Card-G2-A_2778 Einhalten der SMC-B-Spezifikationen für die SMC-B-Testkarten GE**

Die SMC-B-Testkarten der Generation 2 MÜSSEN alle Vorgaben der SMC-B-Spezifikation mit Ausnahme der Option

- Option USB-Schnittstelle

erfüllen. Dies betrifft sowohl die Bereitstellung der definierten Kommandos aus [gemSpec_COS] als auch die Einrichtung der definierten File-Struktur aus [gemSpec_SMC-B_ObjSys]. ⌫

⌦ **Card-G2-A_2964 Authentifizierung zur Kartenadministration der SMC-B-Testkarten GE**

Die Schlüsselobjekte für eines der oder beide Authentisierungsverfahren für

- symmetrische_Authentifizierung_für_CMS
- asymmetrische_Authentifizierung_für_CMS

KÖNNEN mit Schlüsseln befüllt werden.⌫

7.1 PIN- und PUK-Werte

7.1.1 PIN-Werte

⌦ **Card-G2-A_2779 Wert für PIN.SMC und für PIN.CONF für die SMC-B-Testkarten GE**

Bei 50 % der SMC-B-Testkarten MÜSSEN PIN.SMC und PIN.CONF einheitlich auf den Wert 123456 gesetzt werden.

Bei 50% der SMC-B-Testkarten MÜSSEN PIN.SMC und PIN.CONF mit dem in der Spezifikation zugelassenen Transport-PIN-Verfahren (Transport-PIN 5-stellig) kodiert werden. Die Transport-PIN MUSS für diese Karten auf den Wert 54321 gesetzt werden.⌫

Anmerkung: Es wird empfohlen, bei der Umwandlung der Transport-PIN in eine Echt-PIN ebenfalls die Eingabe der Ziffernfolge 123456 als Echt-PIN vorzuschreiben.

7.1.2 PUK-Werte

⌦ **Card-G2-A_2780 Werte für PUK für die SMC-B-Testkarten GE**

Die zu den PINs gehörenden PUK-Werte MÜSSEN bei den SMC-B-Testkarten einheitlich auf den Wert 12345678 gesetzt werden. ⌫

7.2 Erstellung der X.509-Zertifikate für die SMC-B-Testkarten GE

⌦ **Card-G2-A_2965 Nutzung von fiktiven Leistungserbringerorganisationen für die SMC-B-Testkarten GE**

Die Zertifikate der SMC-B-Testkarten FD MÜSSEN Daten von fiktiven Leistungserbringerorganisationen enthalten. ⌫

⌦ **Card-G2-A_2781 Übertragung der Datensätze in die SMC-B-Testkarten GE**

Die zur Personalisierung der Zertifikate der SMC-B-Testkarten notwendigen Daten MÜSSEN vom Kartenhersteller aus den von der gematik gelieferten Datensätzen im spezifizierten Umfang extrahiert und an die jeweilige CA übertragen werden. ⌫

⌦ **Card-G2-A_2782 Erzeugung der X.509-Zertifikate für DF.ESIGN für die SMC-B-Testkarten GE**

Die Zertifikate für AUT, ENC, OSIG und SMKT-AUT MÜSSEN von der jeweiligen CA in dem in [gemSpec_PKI]#5.3] vorgegebenen Format erstellt werden. Dabei MÜSSEN auch die Vorgaben von [gemSpec_PKI]#4.10] umgesetzt werden. ⌫

⌦ **Card-G2-A_2783 Schlüssellänge in DF.ESIGN für die SMC-B-Testkarten GE**

Als Schlüssellänge für die zugehörenden Schlüssel MÜSSEN die in der Spezifikation [gem_SMC-B_ObjSys#4.7.1] festgelegten Werte verwendet werden. ⌫

⌦ **Card-G2-A_2784 Gültigkeitsdauer der X.509-Zertifikate für die SMC-B-Testkarten GE**

Um das Verhalten der Systeme bei abgelaufenen X.509-Zertifikaten testen zu können, MÜSSEN als Gültigkeitszeitraum folgende Werte eingetragen werden:

1. bei 50% der Karten eine Woche
2. bei 50% der Karten 5 Jahre ab Herstelldatum ⌫

⌦ **Card-G2-A_2785 Identische Gültigkeitsdauer für alle X.509-Zertifikate für die SMC-B-Testkarten GE**

Alle X.509-Zertifikate einer Karte MÜSSEN dieselbe Gültigkeitsdauer haben. ⌫

⌦ **Card-G2-A_3045 Festlegung der Telematik-ID für SMC-B-Testkarten GE**

Die Telematik-ID für SMC-B-Testkarten GE MUSS mit folgenden Werten in die X.509-Zertifikate der jeweiligen Testkarten-SMC-B GE eingetragen werden:

Testkarten Betriebsstätte Arzt 1-SMC-B-Testkarte-<ICCSN15>

Testkarten Zahnarztpraxis: 2-SMC-B-Testkarte-<ICCSN15>

Testkarten Betriebsstätte Psychotherapeut: 4-SMC-B-Testkarte-<ICCSN15>

Testkarten Krankenhaus: 5-SMC-B-Testkarte-<ICCSN15>

Für <ICCSN15> MÜSSEN die letzten 15 Stellen der ICCSN der jeweiligen Karte verwendet werden.⌫

⌦ **Card-G2-A_2786 OCSP-Responder für X.509-Zertifikate in DF.ESIGN für die SMC-B-Testkarten GE**

Der jeweilige TSP MUSS für die von seiner CA gelieferten X.509-Zertifikate AUT, ENC und OSIG einen OCSP-Responder bereitstellen, über den die Gültigkeitsinformation zu den Zertifikaten online abgerufen werden kann. ⌫

⌦ **Card-G2-A_2787 Eintrag von "AuthorityInfoAccess" in X.509-Zertifikate in DF-ESIGN für die SMC-B-Testkarten GE**

Der Wert für "AuthorityInfoAccess" des OCSP-Responders MUSS in das entsprechende Datenfeld der X.509-Zertifikate in DF.ESIGN eingetragen werden. ⌫

⌦ **Card-G2-A_2788 Lieferung der X.509-Zertifikate für DF.ESIGN für die SMC-B-Testkarten GE**

Die X.509-Zertifikate für AUT, ENC, OSIG und SMKT-AUT MÜSSEN von der jeweiligen CA an den Testkartenhersteller geliefert werden. ⌫

7.2.1 OID-Vorgaben für die SMC-B-Testkarten der Generation 2

⌦ **Card-G2-A_2789 OID-Vorgaben für die SMC-B-Testkarten GE**

In die X.509-Zertifikate der SMC-B-Testkarten der Generation 2 MÜSSEN gemäß den Festlegungen durch die ausgebenden Organisationen OIDs und Texte eingetragen werden. In Tab_TK_003 sind die Referenzbezeichnungen angegeben. Die zugehörigen OIDs/Texte befinden sich im Dokument [gemSpec_OID].

Tabelle 3: Tab_TK_003 OID-Referenzen für SMC-B-Testkarten GE (verpflichtend)

Speicherort	OID-Referenz
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.HCI.OSIG.R2048, C.HCI.AUT.R2048, C.HCI.ENC.R2048) für Praxen Ärzte	oid_praxis_arzt
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.HCI.OSIG.R2048, C.HCI.AUT.R2048, C.HCI.ENC.R2048) für Praxen Zahnärzte	oid_zahnarztpraxis
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.HCI.OSIG.R2048, C.HCI.AUT.R2048, C.HCI.ENC.R2048) für Praxen Psychotherapeuten	oid_praxis_psychotherapeut
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.HCI.OSIG.R2048, C.HCI.AUT.R2048, C.HCI.ENC.R2048) für Apotheken	oid_öffentliche_apotheke
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.HCI.OSIG.R2048, C.HCI.AUT.R2048, C.HCI.ENC.R2048) für Krankenhäuser	oid_krankenhaus
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.HCI.OSIG.R2048, C.HCI.AUT.R2048, C.HCI.ENC.R2048) für Kostenträger	oid_kostenträger
Admission: ProfessionOID im Zertifikat C.SMKT.AUT.R2048	oid_kt
CertificatePolicies, in allen Zertifikaten (C.HCI.OSIG.R2048, C.HCI.AUT.R2048, C.HCI.ENC.R2048, C.SMKT.AUT.R2048)	oid_policy_gem_or_cp

© gematik – öffentlich

Speicherort	OID-Referenz
CertificatePolicies in C.HCI.ENC.R2048	oid_smc_b_enc
CertificatePolicies in C.HCI.AUT.R2048	oid_smc_b_aut
CertificatePolicies in C.HCI.OSIG.R2048	oid_smc_b_osig
CertificatePolicies in C.SMKT.AUT.R2048	oid_smkt_aut

7.3 CV-Zertifikate für die SMC-B-Testkarten GE der Generation 2

Es gelten die Vorgaben aus Kapitel 3.

7.4 Secret Keys SK.CMS.AES128 für die SMC-B-Testkarten GE der Generation 2

Es gelten die Anforderungen aus Kapitel 4

7.5 Optische Gestaltung der SMC-B-Testkarten GE der Generation 2

Card-G2-A_2790 optische Gestaltung der SMC-B-Testkarten GE

Für die äußere Gestaltung der SMC-B-Testkarten der Generation 2 MÜSSEN die Maße gemäß [gemSpec_SMC_OPT] eingehalten werden. Die optische Gestaltung der Vorderseite der SMC-B-Testkarten der Generation 2 MUSS gemäß Tab_TK_008 (Ausnahme Produktionskennzeichnung, siehe Card-G2-A_2804) ausgeführt werden:

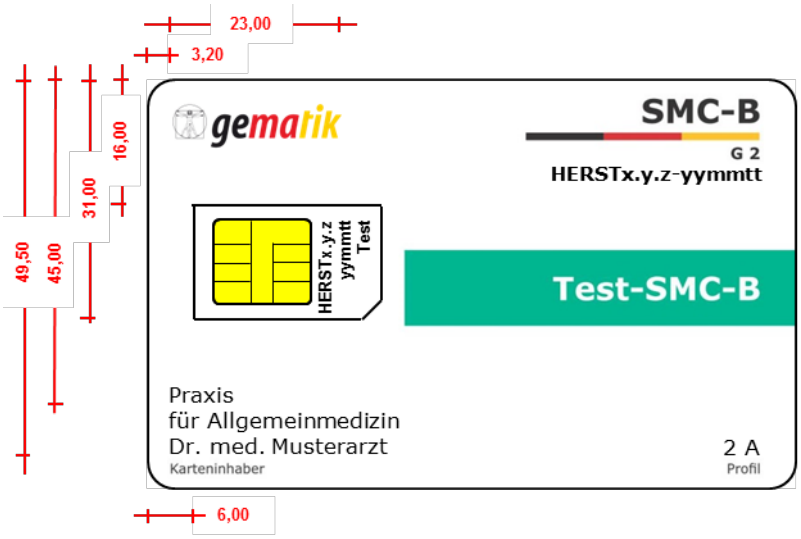


Abbildung 8: Abb_TK_008 Kartenvorderseite SMC-B -Testkarten GE, mit Produktionskennzeichnung

⌫

⌦ **Card-G2-A_2791 Schriftzug „SMC-B“ für die Beschriftung der SMC-B-Testkarten GE**

Der Schriftzug „SMC-B“ und rechtsbündig darunter ein Block in den nationalen Farben MÜSSEN vorhanden sein, um den Anwendungsbereich der SMC-B zu kennzeichnen. ⌫

⌦ **Card-G2-A_2792 Kennzeichnung „Generation“ für die Beschriftung der SMC-B-Testkarten GE**

Die Zugehörigkeit der SMC-B-Testkarten zur Generation 2 MUSS optisch erkennbar sein. Deshalb MUSS unter dem Block in den nationalen Farben rechtsbündig die Zeichenfolge „G 2“ eingefügt werden. ⌫

⌦ **Card-G2-A_2793 Positionierung Schriftzug „SMC-B“ für die Beschriftung der SMC-B -Testkarten GE**

Die Maße aus Abb_TK_008 bezüglich der Position der Elemente „Schriftzug SMC-B“ und „Kennzeichnung Generation“ der SMC-B MÜSSEN eingehalten werden. ⌫

⌦ **Card-G2-A_2794 Schriftart Schriftzug SMC-B für die Beschriftung der SMC-B-Testkarten GE**

Für das Wort „SMC-B“ der SMC-B MUSS die Schriftart Verdana True Type in der Größe 12 pt fett in Schwarz verwendet werden. ⌫

⌦ **Card-G2-A_2795 Farbblock für die Beschriftung der SMC-B-Testkarten GE**

Die SMC-B-Testkarten MÜSSEN durch einen auffälligen Farbblock in Türkis (HKS 53) gekennzeichnet werden. ⌫

⌦ **Card-G2-A_2796 Beschriftung der SMC-B-Testkarten GE mit „Test-SMC-B“**

Die Beschriftung „Test-SMC-B“ MUSS in dem Farbbalken in Verdana True Type fett 22 pt ausgeführt werden.⌫

⌦ **Card-G2-A_2797 Negativdruck für die Beschriftung der SMC-B-Testkarten GE mit „Test-SMC-B“**

Die Beschriftung „Test-SMC-B“ SOLL vorzugsweise im Negativdruck erfolgen. ⌫

⌦ **Card-G2-A_2798 Alternative zum Negativdruck für die Beschriftung der SMC-B-Testkarten GE mit „Test-SMC-B“**

Die Ausführung der Beschriftung „Test-SMC-B“ KANN in Schwarz verwendet werden, wenn die Anfertigung des Negativdrucks unverhältnismäßigen Aufwand verursacht. ⌫

⌦ **Card-G2-A_2800 Kennzeichnung der Generation G2 der SMC-B-Testkarten GE**

Der Schriftzug „G 2“ MUSS in Verdana True Type 6 pt fett, Farbe Schwarz, rechtsbündig zu „SMC-B“ und dem Block in den nationalen Farben aufgebracht werden. ⌫

© gematik – öffentlich

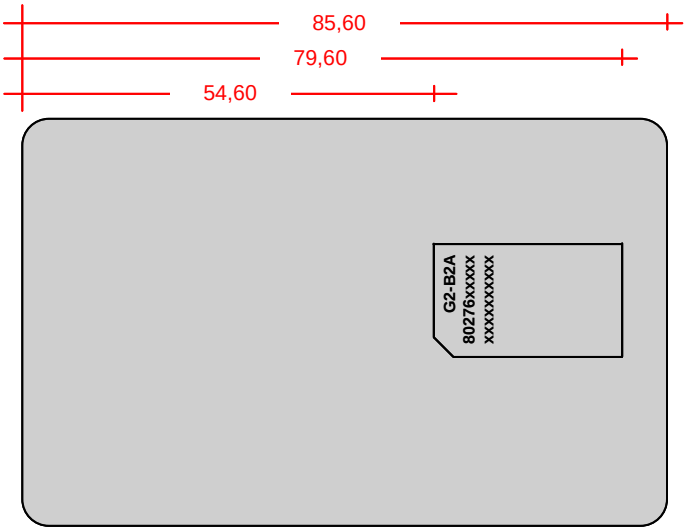


Abbildung 9: Abb_TK_009 Kartenrückseite SMC Typ B mit Kodierung

⌦ **Card-G2-A_2801 Quelle für Daten zum Karteninhaber und zum Profil für die SMC-B-Testkarten GE**

Die Daten zur Institution und zum zugehörigen Profil (Arztpraxis, Krankenhaus = Profil 2 A, Zahnarztpraxis = Profil 2 ZA, Apotheke = Profil 3, Psychotherapeutische Praxis = Profil 4, Kostenträger = Profil 8) MÜSSEN aus den von der gematik gelieferten Datensätzen extrahiert und auf die Karten gedruckt werden.⌫

⌦ **Card-G2-A_2802 Platzierung der Daten zur Institution für die SMC-B-Testkarten GE**

Die Daten zur Institution (Name) und ggfls. weitere Informationen zur Karte MÜSSEN gemäß Abb_TK_008 über dem Schriftzug „Karteninhaber“ maximal dreizeilig linksbündig aufgedruckt werden. Die Zeilen werden von oben nach unten nummeriert, d.h., Zeile 3 ist die Zeile direkt über dem Schriftzug „Karteninhaber“ ⌫

⌦ **Card-G2-A_2803 Platzierung der Daten zum Profil für die SMC-B-Testkarten GE**

Der Zahlenwert des Profils MUSS gemäß Abb_TK_008 über dem Schriftzug „Profil“ rechtsbündig aufgedruckt werden. ⌫

⌦ **Card-G2-A_2804 Produktionskennzeichnung der SMC-B-Testkarten GE**

Der Hersteller KANN gemäß Abb_TK_008 das fünfstellige Herstellerkürzel und die Versionsnummer des auf der Karte vorhandenen Objektsystems, im Format HERSTx.y.z sowie eine Datumsangabe, im Format yymmtt (yymmtt = Jahr Monat Tag, je zweistellig mit jeweils führender Null) in der Schriftart Verdana True Type in der Größe 6 pt fett in Schwarz rechtsbündig zum Text G2 auf die Vorderseite drucken.

Die Werte für Herstellerkürzel und Versionsnummer MÜSSEN dabei den Werten aus DO_PI_InitialisiertesObjSys in EF.ATR des Objektsystems der SMC-B entsprechen.

Die Datumsangabe MUSS geeignet gewählt sein, um einzelne Produktionscharge- der Personalisierung identifizieren zu können und MUSS im Datumsbereich zwischen Beauftragung und Lieferung der entsprechenden Produktionscharge liegen.

⌫

⌦ **Card-G2-A_2966 Logo der gematik der SMC-B auf SMC-B-Testkarten GE**

Gemäß Abb_TK_008 MUSS das Logo der gematik (Datei „Bildvorlage Logo_Gematik_2012.eps“ bzw. „Logo_Gematik_2012_Transparent.png“) in einer Breite von 23 mm in folgender Position aufgedruckt werden:

- Linker Rand des Logos 3,2 mm vom linken Rand der Karte entfernt
- Schriftunterkante (Unterkante Mittellänge) in gleicher Position wie die Unterkante des Balkens in den nationalen Farben. ⌫

⌦ **Card-G2-A_2805 Kartenvorderseite des ID-000-Bereiches der SMC-B-Testkarten GE**

Auf der Vorderseite MUSS in dem als ID-000-Format verbleibenden Ausschnitt gemäß Abb_TK_008 in Verdana True Type 6 pt in der ersten Zeile G 2 aufgedruckt werden. Die zweite Zeile MUSS den Schriftzug „SMC-B“, gefolgt von einem Doppelpunkt, einem Leerzeichen und der Profilnummer, enthalten. Zeile 3 MUSS mit dem Wort „Test“ bedruckt werden. (Ausnahme Produktionskennzeichnung, siehe Card-G2-A_3518) ⌫

⌦ **Card-G2-A_3518 Produktionskennzeichnung auf der Kartenvorderseite des ID-000-Bereiches der SMC-B-Testkarten GE**

Der Hersteller KANN auf der Vorderseite in dem als ID-000-Format verbleibenden Ausschnitt in Verdana True Type 6 pt in der ersten Zeile hinter „G 2“ das fünfstellige Herstellerkürzel und die Versionsnummer des auf der Karte vorhandenen Objektsystems sowie eine Datumsangabe, im Format HERSTx.y.z-yymmtt (yymmtt = Jahr Monat Tag, je zweistellig mit jeweils führender Null) aufdrucken (siehe Abb_TK_008).

Die Werte für Herstellerkürzel und Versionsnummer MÜSSEN dabei den Werten aus DO_PI_InitialisiertesObjSys in EF.ATR des Objektsystems der SMC-B entsprechen.

Die Datumsangabe MUSS geeignet gewählt sein, um einzelne Produktionschargen der Personalisierung identifizieren zu können und MUSS im Datumsbereich zwischen Beauftragung und Lieferung der entsprechenden Produktionscharge liegen. ⌫

⌦ **Card-G2-A_2881 Bedruckung der Kartenvorderseite der SMC-B-Testkarten GE mit Herstellerangaben**

Im freibleibenden Bereich zwischen dem Farbblock gemäß Card-G2-A_2795 und den darüber befindlichen unveränderbaren Merkmalen KÖNNEN Informationen zum Kartenhersteller aufgedruckt werden. ⌫

⌦ **Card-G2-A_2806 Kartenrückseite des ID-000-Bereiches der SMC-B-Testkarten GE**

Auf der Rückseite der SMC-B -Testkarten MUSS zur eindeutigen Zuordnung der SMC-B gemäß Abb_TK_009 in dem als ID-000-Format verbleibenden Ausschnitt linksbündig und um 90° nach links gedreht

- in einer ersten Zeile „G 2“, gefolgt von „-„, „B“ und der Profilnummer

- in der zweiten Zeile die ersten zehn Ziffern der ICCSN
- in der dritten Zeile die letzten zehn Ziffern der ICCSN

aufgedruckt werden.

Für die Bedruckung MUSS eine nichtproportionale Schriftart (z.B. Courier) in einer Größe verwendet werden, die den zur Verfügung stehenden Platz optimal ausnutzt.

Der Bereich, in dem der Chip der Karte positioniert ist, DARF NICHT bedruckt werden. ⌫

⌦ **Card-G2-A_2807 Nutzung der gematik-Vorlagen zur Bedruckung der SMC-B-Testkarten GE**

Für die Bedruckung der SMC-B-Testkarten mit den unveränderbaren Elementen MÜSSEN die entsprechenden Vorlagen genutzt werden, die im Download-Bereich der gematik-Website (www.gematik.de) zur Verfügung gestellt sind. ⌫

7.6 Daten zur Erstellung von SMC-B-Testkarten GE der Generation 2

⌦ **Card-G2-A_2808 Datenlieferung durch die gematik für die SMC-B-Testkarten GE**

Die gematik MUSS folgende Daten für die Produktion von SMC-B-Testkarten an den Kartenhersteller liefern:

- Auftragsformular mit den für alle Karten geltenden Daten:
- Stückzahl
- Datensätze mit Testinstitutionsdaten für die SMC-B-Testkarten in dem vereinbarten Format.
- Datensatz mit dem AES-Schlüsselpaar SK.CMS.ENC.AES128 und SK.CMS.MAC.AES128, falls nicht schon vorhanden.
- Datensatz mit dem AES-Schlüsselpaar SK.CMS.ENC.AES256, SK.CMS.MAC.AES256, falls nicht schon vorhanden.
- Datensatz mit dem öffentlichen CV-Schlüssel gemäß 3.2.2, falls nicht schon vorhanden. ⌫

7.7 Lieferung der SMC-B-Testkarten GE der Generation 2

⌦ **Card-G2-A_2809 Lieferung der SMC-B-Testkarten GE durch den Kartenhersteller**

Die SMC-B-Testkarten MÜSSEN vom Kartenhersteller an die gematik geschickt werden. Sie werden dort getestet, erfasst und anschließend weiter versendet. ⌫

8 Vorgaben für die gSMC-K-Testkarten GE der Generation 2

⌦ **Card-G2-A_2810 Einhalten der gSMC-K-Spezifikationen für die gSMC-K-Testkarten GE**

Die gSMC-K-Testkarten MÜSSEN alle Vorgaben der gSMC-K-Spezifikation mit Ausnahme der Optionen

- Option_lange_Lebensdauer_im_Feld
- Option USB-Schnittstelle

erfüllen. Dies betrifft sowohl die Bereitstellung der definierten Kommandos aus [gemSpec_COS] als auch die Einrichtung der definierten File-Struktur aus [gemSpec_gSMC-K_ObjSys]. ⌫

⌦ **Card-G2-A_2967 Authentifizierung zur Kartenadministration der gSMC-K-Testkarten GE**

Die Schlüsselobjekte für eines der oder beide Authentisierungsverfahren für

- symmetrische_Authentifizierung_für_CMS
- asymmetrische_Authentifizierung_für_CMS

KÖNNEN mit Schlüsseln befüllt werden.⌫

8.1 PIN- Werte

8.1.1 PIN-Werte

⌦ **Card-G2-A_2811 Wert für die PINs für die gSMC-K-Testkarten GE**

Bei 50 % der gSMC-K-Testkarten MÜSSEN PIN.AK, PIN.NK, PIN.Pers, PIN.SAK, PIN.BNetzA_RCA und PIN.TSL_CA einheitlich auf den Wert 123456789012 gesetzt werden.

Bei 25% der gSMC-K-Testkarten MÜSSEN PIN.AK, PIN.NK, PIN.Pers PIN.SAK, PIN.BNetzA_RCA und PIN.TSL_CA mit dem in der Spezifikation zugelassenen Transport-PIN-Verfahren (Leer-PIN) kodiert werden.

Bei 25% der gSMC-K-Testkarten MÜSSEN PIN.AK, PIN.NK, PIN.Pers PIN.SAK, PIN.BNetzA_RCA und PIN.TSL_CA mit dem in der Spezifikation zugelassenen Transport-PIN-Verfahren (Transport-PIN 5stellig) kodiert werden. Die Transport-PIN MUSS für diese Karten auf den Wert 54321 gesetzt werden. ⌫

Anmerkung: Es wird empfohlen, bei der Umwandlung der Transport-PIN in eine Echt-PIN ebenfalls die Eingabe der Ziffernfolge123456789012 als Echt-PIN vorzuschreiben.

Anmerkung: Für die PINs der gSMC-K gibt es gemäß [gemSpec_gSMC-K_ObjSys] keine PUKs.

8.2 Erstellung der X.509-Zertifikate der gSMC-K-Testkarten GE

⌦ **Card-G2-A_2813 Übertragung der Datensätze in die gSMC-K-Testkarten GE**

Die zur Personalisierung der Zertifikate der gSMC-K-Testkarten notwendigen Daten MÜSSEN vom Kartenhersteller aus den von der gematik gelieferten Datensätzen im spezifizierten Umfang extrahiert und an die jeweilige CA übertragen werden. ⌫

⌦ **Card-G2-A_2814 Erzeugung der X.509-Zertifikate für die gSMC-K-Testkarten GE**

Die Zertifikate für der SMC-K MÜSSEN von der jeweiligen CA in dem in [gemSpec_PKI]#5.6] vorgegebenen Format erstellt werden. Dabei MÜSSEN auch die Vorgaben von [gemSpec_PKI]#4.10] umgesetzt werden. ⌫

⌦ **Card-G2-A_2815 Schlüssellängen für die gSMC-K-Testkarten GE**

Als Schlüssellänge für die zugehörenden Schlüssel MÜSSEN die in der Spezifikation [gemSpec_gSMC-K_ObjSys] festgelegten Werte verwendet werden. ⌫

⌦ **Card-G2-A_2816 Gültigkeitsdauer der X.509-Zertifikate für die gSMC-K-Testkarten GE**

Um das Verhalten der Systeme bei abgelaufenen X.509-Zertifikaten testen zu können, MÜSSEN als Gültigkeitszeitraum folgende Werte eingetragen werden:

1. bei 50% der Karten eine Woche
2. bei 50% der Karten 5 Jahre ab Herstelldatum ⌫

⌦ **Card-G2-A_2817 Identische Gültigkeitsdauer für alle X.509-Zertifikate für die gSMC-K-Testkarten GE**

Alle X.509-Zertifikate einer Karte MÜSSEN dieselbe Gültigkeitsdauer haben. ⌫

⌦ **Card-G2-A_2818 OCSP-Responder für X.509-Zertifikate für die gSMC-K-Testkarten GE**

Der jeweilige TSP MUSS für die von seiner CA gelieferten Zertifikate außer den in [Card-G2-A_2819] genannten einen OCSP-Responder bereitstellen, über den die Gültigkeitsinformation zu den Zertifikaten online abgerufen werden kann. ⌫

⌦ **Card-G2-A_2819 kein OCSP-Responder für X.509-Zertifikate aus DF.AK und DF.SAK für die gSMC-K-Testkarten GE**

Für die X.509-Zertifikate in DF.AK und DF.SAK DARF KEIN OCSP-Dienst bereitgestellt werden. ⌫

⌦ **Card-G2-A_2820 Eintrag von "AuthorityInfoAccess" in X.509-Zertifikate für die gSMC-K-Testkarten GE**

Der Wert für "AuthorityInfoAccess" des OCSP-Responders MUSS in das entsprechende Datenfeld der X.509-Zertifikate eingetragen werden. ⌫

⌦ **Card-G2-A_2821 Lieferung der X.509-Zertifikate für die gSMC-K-Testkarten GE**

Die X.509-Zertifikate MÜSSEN von der jeweiligen CA an den Testkartenhersteller geliefert werden. ⌫

8.2.1 OID-Vorgaben für die gSMC-K-Testkarten GE der Generation 2

⌦ **Card-G2-A_2822 OID-Vorgaben für die gSMC-K-Testkarten GE**

In die X.509-Zertifikate der gSMC-K-Testkarten der Generation 2 MÜSSEN gemäß den Festlegungen durch die ausgebenden Organisationen OIDs und Texte eingetragen werden. In Tab_TK_004 sind die Referenzbezeichnungen angegeben. Die zugehörigen OIDs/Texte befinden sich im Dokument [gemSpec_OID].

Tabelle 4: Tab_TK_004 OID-Referenzen für gSMC-K-Testkarten GE der Generation 2 (verpflichtend)

Speicherort	OID-Referenz
Admission: ProfessionItem und ProfessionOID in den Zertifikaten des DF.NK	oid_nk
Admission: ProfessionItem und ProfessionOID in den Zertifikaten des DF.AK	oid_ak
CertificatePolicies für alle Zertifikate	oid_policy_gem_or_cp
CertificatePolicies in C.AK.AUT.R2048	oid_ak_aut
CertificatePolicies in C.NK.VPN.R2048	oid_nk_vpn
CertificatePolicies in C.SAK.AUT.R2048	oid_sak_aut

⌫

8.3 CV-Zertifikate für die gSMC-K-Testkarten GE der Generation 2

Es gelten die Anforderungen aus Kapitel 3

8.4 Secret Key SK.CMS.AES128 für die gSMC-K-Testkarten GE der Generation 2

Es gelten die Anforderungen aus Kapitel 4

8.5 Optische Gestaltung der gSMC-K-Testkarten GE der Generation 2

⌦ **Card-G2-A_2823 optische Gestaltung der gSMC-K-Testkarten GE**

Für die äußere Gestaltung der gSMC-K-Testkarten der Generation 2 MÜSSEN die Maße gemäß [gemSpec_SMC_OPT] eingehalten werden. Die optische Gestaltung der Vorderseite der gSMC-K-Testkarten der Generation 2 MUSS gemäß Abb_TK_010 (Ausnahme Produktionskennzeichnung, siehe Card-G2-A_3519) ausgeführt werden, die der Rückseite gemäß Abb_TK_011.

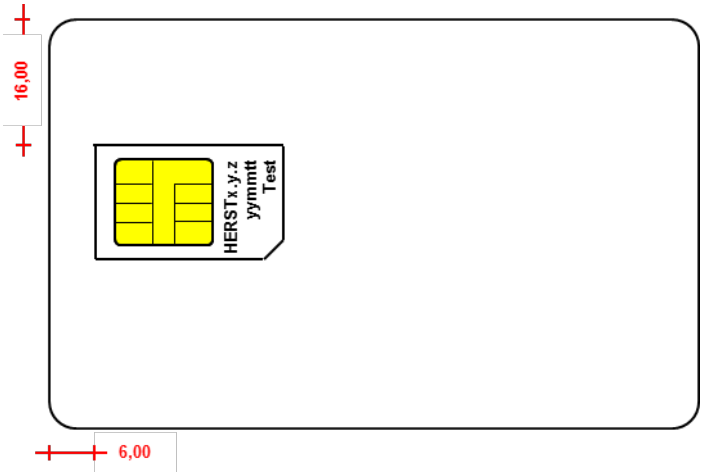


Abbildung 10: Abb_TK_010 Kartenvorderseite gSMC-K-Testkarten GE, mit Produktionskennzeichnung

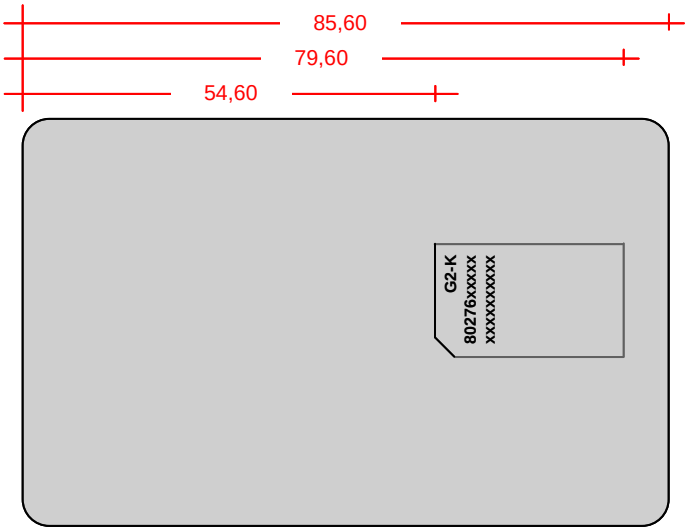


Abbildung 11: Abb_TK_011 Kartenrückseite gSMC-K-Testkarten GE mit Kodierung

⌫

⌦ **Card-G2-A_2824 Kartenvorderseite des ID-000-Bereiches der gSMC-K-Testkarten GE**

Auf der Vorderseite MUSS gemäß Abb_TK_010 in dem als ID-000-Format verbleibenden Ausschnitt in Verdana True Type 6 pt in der ersten Zeile G 2 aufgedruckt werden. Die zweite Zeile MUSS den Schriftzug „gSMC-K:“ enthalten. Zeile 3 MUSS mit dem Wort „Test“ bedruckt werden. (Ausnahme Produktionskennzeichnung, siehe Card-G2-A_3519) ⌫

⌦ **Card-G2-A_3519 Produktionskennzeichnung auf der Kartenvorderseite des ID-000-Bereiches der gSMC-K-Testkarten GE**

Der Hersteller KANN auf der Vorderseite gemäß Abb_TK_010 in dem als ID-000-Format verbleibenden Ausschnitt in Verdana True Type 6 pt in der ersten Zeile hinter G 2 das fünfstellige Herstellerkürzel und die Versionsnummer des auf der Karte vorhandenen Objektsystems, im Format HERSTx.y.z sowie eine Datumsangabe, im Format yymmtt (Jahr Monat Tag, je zweistellig mit jeweils führender Null) aufdrucken.

Die Werte für Herstellerkürzel und Versionsnummer MÜSSEN dabei den Werten aus DO_PI_InitialisiertesObjSys in EF.ATR des Objektsystems der gSMC-K entsprechen.

Die Datumsangabe MUSS geeignet gewählt sein, um einzelne Produktionschargen der Personalisierung identifizieren zu können und MUSS im Datumsbereich zwischen Beauftragung und Lieferung der entsprechenden Produktionscharge liegen.⌫

⌦ **Card-G2-A_2825 Kartenrückseite des ID-000-Bereiches der gSMC-K-Testkarten GE**

Auf der Rückseite der gSMC-K -Testkarten MUSS zur eindeutigen Zuordnung der gSMC-K gemäß Abb_TK_011 in dem als ID-000-Format verbleibenden Ausschnitt linksbündig und um 90° nach links gedreht

- in einer ersten Zeile „G 2“, gefolgt von „-„ und „K“
- in der zweiten Zeile die ersten zehn Ziffern der ICCSN.
- in der dritten Zeile die letzten zehn Ziffern der ICCSN.

aufgedruckt werden.

Für die Bedruckung MUSS eine nichtproportionale Schriftart (z.B. Courier) in einer Größe verwendet werden, die den zur Verfügung stehenden Platz optimal ausnutzt.

Der Bereich, in dem der Chip der Karte positioniert ist, DARF NICHT bedruckt werden. ⌫

8.6 Daten zur Erstellung von gSMC-K-Testkarten GE der Generation 2

⌦ **Card-G2-A_2826 Datenlieferung durch die gematik für die gSMC-K-Testkarten GE**

Die gematik MUSS folgende Daten für die Produktion von gSMC-K-Testkarten an den Kartenhersteller liefern:

- Auftragsformular mit den für alle Karten geltenden Daten
- Stückzahl
- Datensätze für die gSMC-K-Testkarten in dem vereinbarten Format.
- Datensatz mit dem AES-Schlüsselpaar SK.CMS.ENC.AES128 und SK.CMS.MAC.AES128, falls nicht schon vorhanden.
- Datensatz mit dem AES-Schlüsselpaar SK.CMS.ENC.AES256, SK.CMS.MAC.AES256, falls nicht schon vorhanden.
- Datensatz mit dem öffentlichen CV-Schlüssel gemäß 3.2.2, falls nicht schon vorhanden.
- Datensatz mit den Kennummern, die auf die Rückseite des ID-000-Ausschnitts gedruckt werden müssen. ⌫

8.7 Lieferung der gSMC-K-Testkarten GE der Generation 2

⌦ **Card-G2-A_2827 Lieferung der gSMC-K-Testkarten GE durch den Kartenhersteller**

Die gSMC-K-Testkarten MÜSSEN vom Kartenhersteller an die gematik geschickt werden. Sie werden dort getestet, erfasst und anschließend weiter versendet. ⌫

9 Vorgaben für die gSMC-KT-Testkarten GE der Generation 2

⌦ **Card-G2-A_2828 Einhalten der gSMC-KT-Spezifikationen für die gSMC-KT-Testkarten GE**

Die gSMC-KT-Testkarten MÜSSEN alle Vorgaben der gSMC-KT-Spezifikation mit Ausnahme der Optionen

- Option_lange_Lebensdauer_im_Feld
- Option USB-Schnittstelle
- Option PACE

erfüllen. Dies betrifft sowohl die Bereitstellung der definierten Kommandos aus [gemSpec_COS] als auch die Einrichtung der definierten File-Struktur aus [gemSpec_gSMC-KT_ObjSys]. ⌫

⌦ **Card-G2-A_2968 Authentifizierung zur Kartenadministration der gSMC-KT-Testkarten GE**

Die Schlüsselobjekte für eines der oder beide Authentisierungsverfahren für

- symmetrische_Authentifizierung_für_CMS
- asymmetrische_Authentifizierung_für_CMS

KÖNNEN mit Schlüsseln befüllt werden.⌫

9.1 Erstellung der X.509-Zertifikate der gSMC-KT-Testkarten GE

⌦ **Card-G2-A_2829 Übertragung der Datensätze in die gSMC-KT-Testkarten GE**

Die zur Personalisierung der Zertifikate der gSMC-KT-Testkarten notwendigen Daten MÜSSEN vom Kartenhersteller aus den aus den von der gematik gelieferten Datensätzen im spezifizierten Umfang extrahiert und an die jeweilige CA übertragen werden. ⌫

⌦ **Card-G2-A_2830 Erzeugung der X.509-Zertifikate für die gSMC-KT-Testkarten GE**

Die Zertifikate der gSMC-KT MÜSSEN von der jeweiligen CA in dem in [gemSpec_PKI]#5.5] vorgegebenen Format erstellt werden. Dabei MÜSSEN auch die Vorgaben von [gemSpec_PKI]#4.10] umgesetzt werden. ⌫

⌦ **Card-G2-A_2831 Schlüssellänge für die gSMC-KT-Testkarten GE**

Als Schlüssellänge für die zugehörenden Schlüssel MÜSSEN die in der Spezifikation [gemSpec_gSMC-KT_ObjSys] festgelegten Werte verwendet werden. ⌫

⌦ **Card-G2-A_2832 Gültigkeitsdauer der X.509-Zertifikate für die gSMC-KT-Testkarten GE**

Um das Verhalten der Systeme bei abgelaufenen X.509-Zertifikaten testen zu können, MÜSSEN als Gültigkeitszeitraum folgende Werte eingetragen werden:

1. bei 50% der Karten eine Woche
2. bei 50% der Karten 5 Jahre ab Herstelldatum ⌫

⌦ **Card-G2-A_2833 Identische Gültigkeitsdauer für alle X.509-Zertifikate für die gSMC-KT-Testkarten GE**

Alle X.509-Zertifikate einer Karte MÜSSEN dieselbe Gültigkeitsdauer haben. ⌫

⌦ **Card-G2-A_2834 kein OCSP-Responder für X.509-Zertifikate der gSMC-KT-Testkarten GE**

Für die X.509-Zertifikate der gSMC-KT-Testkarten DARF KEIN OCSP-Dienst bereitgestellt werden. ⌫

⌦ **Card-G2-A_2835 Lieferung der X.509-Zertifikate für die gSMC-KT-Testkarten GE**

Die X.509-Zertifikate MÜSSEN von der jeweiligen CA an den Testkartenhersteller geliefert werden. ⌫

9.1.1 OID-Vorgaben für die gSMC-KT-Testkarten GE der Generation 2

⌦ **Card-G2-A_2836 OID-Vorgaben für die gSMC-KT-Testkarten GE**

In die X.509-Zertifikate der gSMC-KT-Testkarten der Generation 2 MÜSSEN gemäß den Festlegungen durch die ausgebenden Organisationen OIDs und Texte eingetragen werden. In der folgenden Tabelle sind die Referenzbezeichnungen angegeben. Die zugehörigen OIDs/Texte befinden sich im Dokument [gemSpec_OID].

Tabelle 5: OID-Referenzen für die gSMC-KT-Testkarten GE der Generation 2 (verpflichtend)

Speicherort	OID-Referenz
Admission: ProfessionItem und Profession OID in den Zertifikaten des DF.KT	oid_smkt
CertificatePolicies für alle Zertifikate	oid_policy_gem_or_cp
CertificatePolicies in C.SMKT.AUT.R2048	oid_smkt_aut

⌫

9.2 CV-Zertifikate für die gSMC-KT-Testkarten GE der Generation 2

Es gelten die Anforderungen aus Kapitel 3

9.3 Secret Keys SK.CMS.AES128 für die gSMC-KT-Testkarten GE der Generation 2

Es gelten die Anforderungen aus Kapitel 4

9.4 Optische Gestaltung der gSMC-KT-Testkarten GE der Generation 2

Card-G2-A_2837 optische Gestaltung der gSMC-KT-Testkarten GE

Für die äußere Gestaltung der gSMC-KT-Testkarten der Generation 2 MÜSSEN die Maße gemäß [gemSpec_SMC_OPT] eingehalten werden. Die optische Gestaltung der Vorderseite der gSMC-KT-Testkarten der Generation 2 MUSS gemäß Abb_TK_012 (Ausnahme Produktionskennzeichnung, siehe Card-G2-A_3520) ausgeführt werden, die der Rückseite gemäß Abb_TK_013.

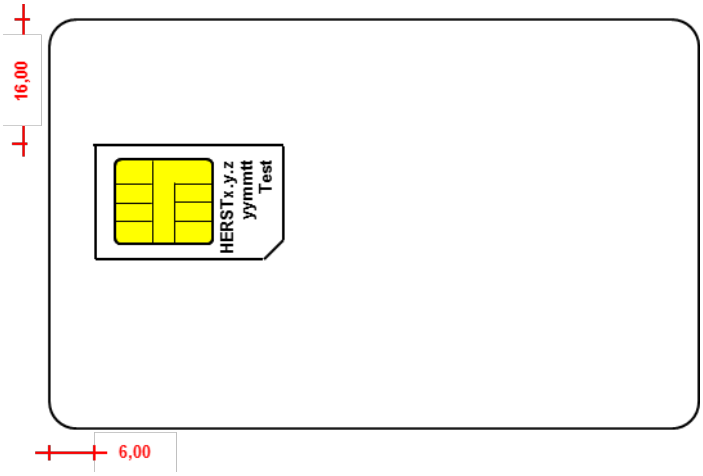


Abbildung 12: Abb_TK_012 Kartenvorderseite gSMC-KT-Testkarten GE, mit Produktionskennzeichnung

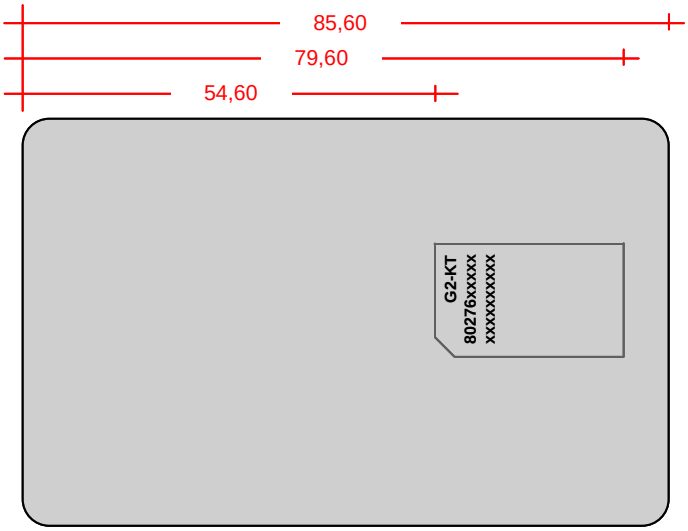


Abbildung 13: Abb_TK_013 Kartenrückseite gSMC-KT-Testkarten GE mit Kodierung

⌫

⌦ **Card-G2-A_2838 Kartenvorderseite des ID-000-Bereiches der gSMC-KT-Testkarten GE**

Auf der Vorderseite der gSMC-KT-Testkarten MUSS gemäß Abb_TK_012 in dem als ID-000-Format verbleibenden Ausschnitt in Verdana True Type 6 pt in der ersten Zeile G 2 aufgedruckt werden. Die zweite Zeile MUSS den Schriftzug „gSMC-KT:“ enthalten. Zeile 3 MUSS mit dem Wort „Test“ bedruckt werden. (Ausnahme Produktionskennzeichnung, Card-G2-A_3520) ⌫

⌦ **Card-G2-A_3520 Produktionskennzeichnung auf der Kartenvorderseite des ID-000-Bereiches der gSMC-KT-Testkarten GE**

Der Hersteller KANN auf der Vorderseite der gSMC-KT-Testkarten gemäß Abb_TK_012 in dem als ID-000-Format verbleibenden Ausschnitt in Verdana True Type 6 pt in der ersten Zeile hinter G 2 das fünfstellige Herstellerkürzel und die Versionsnummer des auf der Karte vorhandenen Objektsystems, im Format HERSTx.y.z, sowie eine Datumsangabe, im Format yymmtt (Jahr Monat Tag, je zweistellig mit jeweils führender Null) aufdrucken.

Die Werte für Herstellerkürzel und Versionsnummer MÜSSEN dabei den Werten aus DO_PI_InitialisiertesObjSys in EF.ATR des Objektsystems der gSMC-KT entsprechen.

Die Datumsangabe MUSS geeignet gewählt sein, um einzelne Produktionschargen der Personalisierung identifizieren zu können und MUSS im Datumsbereich zwischen Beauftragung und Lieferung der entsprechenden Produktionscharge liegen. ⌫

⌦ **Card-G2-A_2839 Kartenrückseite des ID-000-Bereiches der gSMC-KT-Testkarten GE**

Auf der Rückseite der gSMC-KT -Testkarten MUSS zur eindeutigen Zuordnung der gSMC-KT gemäß Abb_TK_013 in dem als ID-000-Format verbleibenden Ausschnitt linksbündig und um 90° nach links gedreht

- in einer ersten Zeile „G 2“, gefolgt von „-„ und „KT“
- in der zweiten Zeile die ersten zehn Ziffern der ICCSN.
- in der dritten Zeile die letzten zehn Ziffern der ICCSN.

aufgedruckt werden.

Für die Bedruckung MUSS eine nichtproportionale Schriftart (z.B. Courier) in einer Größe verwendet werden, die den zur Verfügung stehenden Platz optimal ausnutzt.

Der Bereich, in dem der Chip der Karte positioniert ist, DARF NICHT bedruckt werden. ⌫

9.5 Daten zur Erstellung von gSMC-KT-Testkarten GE der Generation 2

⌦ **Card-G2-A_2840 Datenlieferung durch die gematik für die gSMC-KT-Testkarten GE**

Die gematik MUSS folgende Daten für die Produktion von SMC-KT-Testkarten an den Kartenhersteller liefern:

- Auftragsformular mit den für alle Karten geltenden Daten.
- Stückzahl
- Datensätze für die gSMC-KT-Testkarten in dem vereinbarten Format.
- Datensatz mit dem AES-Schlüsselpaar SK.CMS.ENC.AES128 und SK.CMS.MAC.AES128, falls nicht schon vorhanden.
- Datensatz mit dem AES-Schlüsselpaar SK.CMS.ENC.AES256, SK.CMS.MAC.AES256, falls nicht schon vorhanden.
- Datensatz mit dem öffentlichen CV-Schlüssel gemäß 3.2.2, falls nicht schon vorhanden.⌫

9.6 Lieferung der gSMC-KT-Testkarten GE der Generation 2

⌦ **Card-G2-A_2841 Lieferung der gSMC-KT-Testkarten GE durch den Kartenhersteller**

Die gSMC-KT-Testkarten MÜSSEN vom Kartenhersteller an die gematik geschickt werden. Sie werden dort getestet, erfasst und anschließend weiter versendet. ⌫

© gematik – öffentlich

Anhang A - Verzeichnisse

A1 - Abkürzungen

Kürzel	Erläuterung
AUT	Authentifizierung
BSI	Bundesamt für die Sicherheit in der Informationstechnik
BÄK	Bundesärztekammer
BCD	Binär kodierte Dezimalzahl
CA	Certification Authority (jetzt TSP genannt)
CVC	Card Verifiable Certificate
DF	Dedicated File
EF	Elementary File
ELC	Elliptic Curve Cryptography, Kryptographie mittels elliptischer Kurven
eGK	elektronische Gesundheitskarte
EHIC	Europäische Krankenversichertenkarte
ENV	Verschlüsselung (Encryption)
gSMC	gerätespezifische Security Module Card (gSMC-K und gSMC-KT)
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-B)

Kürzel	Erläuterung
SMC-K	Security Module Card des Konnektors
TLV	Tag Length Value
TSP	Trusted Service Provider (früher CA genannt)
XML	Universelle Datenbeschreibungssprache (Extensible Markup Language)
ZDA	Zertifizierungsdiensteanbieter

A2 - Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 - Abbildungsverzeichnis

Abbildung 1: Abb_TK_001 Definition der verschiedenen Kartentypen am Beispiel der eGK 7
Abbildung 2: Abb_TK_002 Darstellung der Abläufe für die Erstellung von Testkarten G2 (mit Test-PKI) 10
Abbildung 3: Abb_TK_003 ICCSN für Gesundheitskarten 16
Abbildung 4: Abb_TK_004 Kartenvorderseite der eGK-Testkarten GE mit Personalisierung, ohne Bild, Bemaßung für Logo-Position, mit Produktionskennzeichnung 20
Abbildung 5: Abb_TK_005 Kartenvorderseite der eGK-Testkarten GE mit Personalisierung, mit Bild, Bemaßung für Logo-Position, mit Produktionskennzeichnung 21
Abbildung 6: Abb_TK_006 Kartenvorderseite der HBA-Testkarten GE, konstante Elemente 28
Abbildung 7: Abb_TK_007 Kartenvorderseite, Personalisierung für Ärztin/Arzt (beispielhaft) mit CAN, mit Produktionskennzeichnung 30
Abbildung 8: Abb_TK_008 Kartenvorderseite SMC-B -Testkarten GE, mit Produktionskennzeichnung 36
Abbildung 9: Abb_TK_009 Kartenrückseite SMC Typ B mit Kodierung 38
Abbildung 10: Abb_TK_010 Kartenvorderseite gSMC-K-Testkarten GE, mit Produktionskennzeichnung 44
Abbildung 11: Abb_TK_011 Kartenrückseite gSMC-K-Testkarten GE mit Kodierung 44
Abbildung 12: Abb_TK_012 Kartenvorderseite gSMC-KT-Testkarten GE, mit Produktionskennzeichnung 49
Abbildung 13: Abb_TK_013 Kartenrückseite gSMC-KT-Testkarten GE mit Kodierung 50
Abbildung 14: Abb_TK_014 Bedeutung der Zifferngruppen der IK des Kostenträgers 56

Abbildung 15: Abb_TK_015 Aufbau einer ICCSN 59

A.4 – Tabellenverzeichnis

Tabelle 1: Tab_TK_001 OID-Referenzen für eGK-Testkarten GE (verpflichtend) 19

Tabelle 2: Tab_TK_002 OID-Referenzen für HBA-Testkarten GE (verpflichtend) 27

Tabelle 3: Tab_TK_003 OID-Referenzen für SMC-B-Testkarten GE (verpflichtend) 35

Tabelle 4: Tab_TK_004 OID-Referenzen für gSMC-K-Testkarten GE der Generation 2 (verpflichtend) 43

Tabelle 5: OID-Referenzen für die gSMC-KT-Testkarten GE der Generation 2 (verpflichtend) 48

Tabelle 6: Tab_TK_006 Festlegungen für die IK des Kostenträgers 56

Tabelle 7: Tab_TK_009 Berechnung der Prüfziffer der IK-Nummer für die Testkarten GE 57

Tabelle 8: Tab_TK_007 Issuer Identification Number.....57

Tabelle 9: Tab_TK_010 Berechnung der Prüfziffer des unveränderlichen Teils der KVNR 58

Tabelle 10: Tab_TK_011 Berechnung der Prüfziffer der kompletten KVNR 58

Tabelle 11: Tab_TK_008 Kodierung der ICCSN für die Testkarten GE.....60

A5 - Referenzierte Dokumente

A5.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer entnehmen Sie bitte der aktuellsten, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS) - Elektrische Schnittstelle für Karten (eGK, SMC und HBA) der Generation 2
[gemSpec_eGK_ObjSys]	gematik: Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem für eGK der Generation 2
[gemSpec_eGK_OPT]	gematik: Spezifikation der elektronischen Gesundheitskarte Äußere Gestaltung für eGK der Generation 2

© gematik – öffentlich

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_HBA_ObjSys]	gematik: Spezifikation HBA Objektsystem
[gemSpec_SMCB_ObjSys]	gematik: Spezifikation SMC-B Objektsystem
[gemSpec_gSMC-K_ObjSys]	gematik: Spezifikation der gSMC-K Objektsystem
[gemSpec_gSMC-KT_ObjSys]	gematik: Spezifikation der gSMC-KT Objektsystem
[gemSpec_HBA_ObjSys]	gematik: Spezifikation HBA Objektsystem
[gemSpec_OID]	gematik: Spezifikation OID
[gemSpec_PKI]	gematik: Spezifikation PKI
[gemSpec_SMC_OPT]	gematik: Gemeinsame optische Merkmale der SMC
[gemSpec_SMC-B_ObjSys]	gematik: Spezifikation SMC-B Objektsystem für SMC-B der Generation 2
[gemSpec_TLK_COS_G2]	gematik: Spezifikation der Testlaborkarte COS/Objektsysteme

A5.2 - Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2119
[BAEK_HBA_Cert]	Bundesärztekammer Zertifikatsprofile für X.509 Basiszertifikate, V2.3.2
[BAEK_HBA_Attr]	Bundesärztekammer Zertifikatsprofile für X.509 Attributzertifikate, V2.3.2

Anhang B - Festlegungen

B1 - Festlegungen für die IK des Kostenträgers für die eGK-Testkarten GE

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

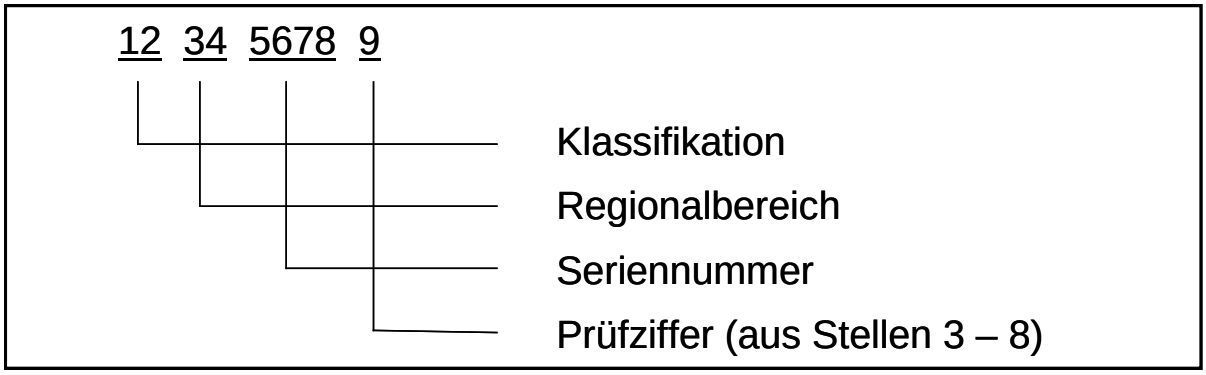


Abbildung 14: Abb_TK_014 Bedeutung der Zifferngruppen der IK des Kostenträgers

Tabelle 6: Tab_TK_006 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 Prüfziffer wird mit dem Modulo-10-Verfahren und den Faktoren 2-1-2-1-2-1 berechnet. Aus dem Produkt von Ziffer und Faktor wird jeweils die Quersumme berechnet. Die Quersummen werden addiert; der aus der dabei erhaltenen Summe mit der Funktion Modulo 10 gebildete Wert ist die Prüfziffer. Ein Beispiel zeigt Tab_TK_009.

Tabelle 7: Tab_TK_009 Berechnung der Prüfziffer der IK-Nummer für die Testkarten GE

Stelle	1	2	3	4	5	6	7	8	9
IK ohne Prüfziffer	1	0	4	9	4	0	0	0	
Faktor			2	1	2	1	2	1	
Ergebnis Zahl x Faktor			8	9	8	0	0	0	
Quersummen			8	9	8	0	0	0	
Summe Quersummen (SQ)									25
Prüfziffer (Modulo 10 von SQ)									5
Teil 2 KVNR mit Prüfziffer (IK des KT)	1	0	4	9	4	0	0	0	5

Festlegung:

⌦ **Card-G2-A_2842 Festlegung der IK für die Testkarten GE**

Für die Testkarten MUSS die von der gematik bereitgestellte IK verwendet werden. ⌫

B2 - Festlegungen zur IIN des Kartenherausgebers für die eGK-Testkarten GE

⌦ **Card-G2-A_2843 IIN des Kartenherausgebers für die Testkarten GE**

Die Issuer Identification Number MUSS gemäß [gemSpec_eGK_ObjSys], wie in Tab_TK_007 angegeben, gebildet werden.

Tabelle 8: Tab_TK_007 Issuer Identification Number

MII für Gesundheitswesen	Country Code Germany	Issuer Identifier (Herausgeberkennung) für einen bestimmten Kartenherausgeber
‘80’	‘276’	... (5 BCD)

⌫

⌦ **Card-G2-A_2844 Issuer Identifier (Herausgeberkennung) für die Testkarten GE**

Als Issuer Identifier (Herausgeberkennung) für die Testkarten MUSS der für die gematik vergebene Wert 88 311 verwendet werden. Der Issuer Identifier ist Bestandteil der ICCSN (siehe Tab_TK_008) ⌫

B3 - Festlegungen zur KVNR für die eGK-Testkarten GE

⌦ **Card-G2-A_2845 Regel zur Bildung des unveränderlichen Teils der KVNR der Testkarten GE**

Da die Auswertung der Prüfziffer durch Systeme der Leistungserbringer (auch bei Testkarten) möglich ist, MÜSSEN die unveränderlichen Teile der KVNR für Testkarten gemäß folgender Vorschrift korrekt gebildet werden:

Vorschrift für die Bildung des 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 Faktoren 1-2-1-2-1-2-1-2-1-2 berechnet. Der Buchstabe wird dabei durch eine zweistellige Zahl ersetzt, das A mit 01, das B mit 02, …, und das Z mit 26. Aus dem Produkt von Ziffer und Faktor wird jeweils die Quersumme berechnet. Die Quersummen werden addiert; der aus der dabei erhaltenen Summe mit der Funktion Modulo 10 gebildete Wert ist die Prüfziffer. Ein Beispiel zeigt Tab_TK_010.

Tabelle 9: Tab_TK_010 Berechnung der Prüfziffer des unveränderlichen Teils der KVNR

Stelle		1	2	3	4	5	6	7	8	9	10
KVNR ohne Prüfziffer		A	0	0	0	5	0	0	0	1	
Umsetzen Buchstabe-Zahl	0	1	0	0	0	5	0	0	0	1	
Faktor	1	2	1	2	1	2	1	2	1	2	
Ergebnis Zahl x Faktor	0	2	0	0	0	10	0	0	0	2	
Quersummen	0	2	0	0	0	1	0	0	0	2	
Summe Quersummen											5
Prüfziffer (Modulo 10)											5
KVNR mit Prüfziffer		A	0	0	0	5	0	0	0	1	5

Vorschrift für die Bildung der kompletten KVNR (diese wird für die Erstellung von Testkarten nicht benötigt):

Hierfür müssen die oben genannten Regeln zur Bildung der Prüfziffer auf die Konkatenation der KVNR (10 Stellen) und der IK des Kostenträgers (9 Stellen) angewendet werden. Ein Beispiel zeigt Tab_TK_011

Tabelle 10: Tab_TK_011 Berechnung der Prüfziffer der kompletten KVNR

	unveränderbarer Teil der KVNR											veränderbarer Teil der KVNR (IK des KT)									
Stelle		1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10
KVNR mit Prüfziffer		A	0	0	0	5	0	0	0	1	5										
Umsetzen Buchstabe-Zahl	0	1	0	0	0	5	0	0	0	1	5	1	0	4	9	4	0	0	0	5	
Faktor	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	
Ergebnis Zahl x Faktor	0	2	0	0	0	10	0	0	0	2	5	2	0	8	9	8	0	0	0	10	
Quersummen	0	2	0	0	0	1	0	0	0	2	5	2	0	8	9	8	0	0	0	1	
Summe Quersummen (SQ)																					38
Prüfziffer (Modulo 10 von SQ))																					8
gesamte KVNR mit Prüfziffer		A	0	0	0	5	0	0	0	1	5	1	0	4	9	4	0	0	0	5	8

Das Ergebnis ist die 20-stellige KVNR.

⌦ **Card-G2-A_2846 gleiche aufeinander folgende Ziffern in der KVNR der Testkarten GE**

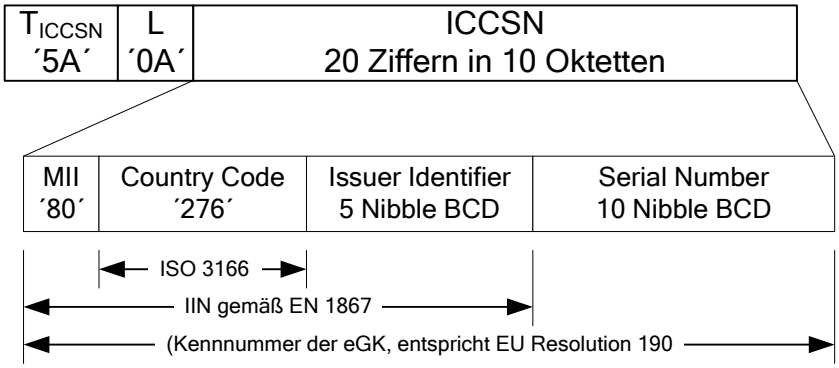
Eine Prüfung des Verbots der Nutzung von mehr als drei aufeinander folgenden gleichen Ziffern erfolgt bei der Erstellung der KVNR. KVNR für Testkarten DÜRFEN ebenfalls NICHT mehr als drei gleiche aufeinander folgende Ziffern enthalten. ⌫

⌦ **Card-G2-A_2847 Bereitstellung der KVNR für die Testkarten GE**

Die KVNR für die eGK-Testkarten, die nach dieser Spezifikation erstellt werden, MÜSSEN von der gematik entsprechend den angegebenen Regeln erstellt und mit den jeweiligen Datensätzen an den Testkartenhersteller übermittelt werden. ⌫

B4 - Definition der ICCSN

Die ICCSN einer eGK muss weltweit eindeutig sein. Der Aufbau der ICCSN ist in Abb_TK_015 dargestellt.



Abkürzungen:
ICCSN = Integrated Chip Card Serial Number
IIN = Issuer Identification Number
MII = Major Industry Indentifier

Abbildung 15: Abb_TK_015 Aufbau einer ICCSN

B5 - Kodierung der ICCSN für Testkarten GE

⌦ **Card-G2-A_2848 Vorgaben zur Bildung der ICCSN für die Testkarten GE**

Um eine leichtere Zuordnung von Testkarten zu erlauben, MÜSSEN bestimmte Stellen der ICCSN entsprechend kodiert werden. Die Kodierung der Stellen 1 bis 10 ist bereits in den vorhandenen Spezifikationen festgelegt und MUSS gemäß Anhang B4 erfolgen (siehe auch Tabelle 4). Die Kodierung für die Stellen 11 bis 20 der ICCSN für Testkarten ist eine Zählnummer, die von der gematik festgelegt ist.

Die ICCSNs werden von der gematik generiert und mit den jeweiligen Datensätzen an den Testkartenhersteller übermittelt.

Tabelle 11: Tab_TK_008 Kodierung der ICCSN für die Testkarten GE

Stelle der ICCSN	Inhalt
1	8
2	0
3	2
4	7
5	6
6	8
7	8
8	3
9	1
10	1
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	

⌫