

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation für Testkarten Fachdienste (eGK) der Generation 2

Version:	1. 34 .0
Revision:	294976721335
Stand:	12.11.2020 20 20.09.2023
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_TK_FD

Dokumenteninformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	24.07.15	freigegeben	gematik
1.1.0	19.10.18	Erweiterung des Dokuments für eGK-Testkarten der Generation 2.1	gematik
1.2.0	15.05.19	Einarbeitung P18.1	gematik
1.3.0	12.11.20	Neuorganisation der Testkartenkategorien, Änderung des Nummerierungsschemas KVNR, Bedingungen zur Neulieferung von Testkartensätzen hinzugefügt; Einarbeitung Scope-Themen zu R4.0.1	gematik
1.4.0	20.09.23	Einarbeitung Smartcard 23.1 Anpassung an den Stand der aktuellen Dokumentenlandschaft der TI , Bereitstellung eGK-Testkarten FD mit kontaktloser Schnittstelle , Anpassungen in der Bildungsvorschrift der KVNR für eGK-Testkarten FD , Trennung in eGK-Testkarten FD für die gematik und für andere	gematik

Inhaltsverzeichnis

1 Einführung des Dokumentes	5
1.1 Zielsetzung	5
1.2 Zielgruppe	7
1.3 Geltungsbereich	7
1.4 Abgrenzung des Dokuments	8
1.5 Methodik	8
2 Strukturen zu Herstellung von Testkarten FD	9
2.1 Testkarten FD	9
3 Vorgaben zu CV-Zertifikaten der Testkarten FD	10
3.1 CV-Zertifikate für Testkarten FD	10
3.1.1 Test-Root-CVC-CAs für Testkarten FD	10
3.1.2 Test-CVC-CA für Testkarten FD	10
4 Vorgaben zu symmetrischen Schlüsseln	11
4.1 Schlüsselableitung eGK-Testkarten FD	11
4.2 Konkrete Werte für Masterkey	11
4.2.1 Schlüsseldaten	12
4.2.2 Schlüsselbezeichner (KID)	12
4.3 Schlüsselableitung	13
4.3.1 Nomenklatur	13
4.3.2 Variante 1: gematik	13
4.3.2.1 Beispielgenerierung	14
4.3.3 Variante 2: Atos-Verfahren	15
4.3.3.1 Beispielgenerierung	16
4.3.4 Variante 3: G&D-Verfahren	16
5 Vorgaben für eGK-Testkarten FD	17
5.1 PIN- und PUK-Werte	17
5.1.1 PIN-Werte	17
5.1.2 PUK-Werte	17
5.1.3 CAN-Werte	17
5.2 Erstellung der Daten der Versicherten für Testkarten FD	18
5.2.1 Bereitstellung der Daten	18
5.3 Erstellung der X.509-Zertifikate für Testkarten FD	19
5.3.1 Erstellung der X.509-Zertifikate für Testkarten FD für ENC, ENCV, AUT und AUTN	19
5.3.2 OID-Vorgaben für die eGK-Testkarten FD	19
5.4 CV-Zertifikate für die eGK-Testkarten FD	20

5.5 Secret Keys SK.CMS.AES128, SK.VSD.AES128 und SK.VSDCMS.AES128 für die eGK-Testkarten FD	20
5.6 Optische Gestaltung der eGK-Testkarten FD	20
6 Anhang A – Verzeichnisse	24
6.1 Abkürzungen	24
6.2 Glossar	25
6.3 Abbildungsverzeichnis	25
6.4 Tabellenverzeichnis	25
6.5 Referenzierte Dokumente	26
6.5.1 Dokumente der gematik	26
6.6 Weitere Dokumente	27
7 Anhang B – Festlegungen	28
7.1 Festlegungen für die IK des Kostenträgers für eGK-Testkarten FD	28
7.2 Festlegungen zur IIN des Kartenherausgebers für Testkarten FD	28
7.3 Festlegungen zur KVNR für eGK-Testkarten FD	28
7.4 Definition der ICCSN	30
7.5 Kodierung der ICCSN für die Testkarte FD	30
8 Anhang C – Testkategorien RU/TU	32
8.1 Testkategorien RU	32
8.2 Testkategorien TU	33
8.3 Testkategorien RU / Testportal	45
8.4 Bereitstellung von Testkarten nach der Zulassung	45
9 Anhang D – Zuordnung KVNR-Nummernkreise	48
1 Einführung des Dokumentes	7
1.1 Zielsetzung	7
1.2 Zielgruppe	9
1.3 Geltungsbereich	9
1.4 Abgrenzung des Dokuments	10
1.5 Methodik	10
2 Strukturen zu Herstellung von Testkarten FD	11
3 Vorgaben zu CV-Zertifikaten der Testkarten FD	12
4 Vorgaben zu symmetrischen Schlüsseln	13
4.1 Schlüsselableitung eGK-Testkarten FD	13

4.2 Konkrete Werte für Masterkey.....	14
4.3 Schlüsselableitung.....	16
4.3.1 Nomenklatur	16
4.3.2 Variante 1: gematik	16
4.3.3 Variante 2: Atos Verfahren	18
4.3.4 Variante 3: G&D Verfahren.....	20
5 Vorgaben für eGK-Testkarten FD	21
5.1 PIN- und PUK-Werte.....	21
5.1.1 PIN-Werte	21
5.1.2 PUK-Werte	21
5.1.3 CAN-Werte	21
5.2 Erstellung der Daten der Versicherten für Testkarten FD	22
5.2.1 Bereitstellung der Daten	22
5.3 Erstellung der X.509-Zertifikate für Testkarten FD	22
5.3.1 Erstellung der X.509-Zertifikate für Testkarten FD für ENC, ENCV, AUT und AUTN	23
5.3.2 OID-Vorgaben für die eGK-Testkarten FD	23
5.4 CV-Zertifikate für die eGK-Testkarten FD	24
5.5 Secret Keys SK.CMS.AES128, SK.VSD.AES128 und SK.VSDCMS.AES128 für die eGK-Testkarten FD.....	24
5.6 Optische Gestaltung der eGK-Testkarten FD	24
6 Anhang A – Verzeichnisse	28
6.1 Abkürzungen	28
6.2 Glossar	29
6.3 Abbildungsverzeichnis.....	29
6.4 Tabellenverzeichnis	30
6.5 Referenzierte Dokumente	30
6.5.1 Dokumente der gematik.....	30
6.5.2 Weitere Dokumente.....	32
7 Anhang B – Festlegungen	33
7.1 Festlegungen für die IK des Kostenträgers für eGK-Testkarten FD	33
7.2 Festlegungen zur IIN des Kartenherausgebers für Testkarten FD	33
7.3 Festlegungen zur KVNR für eGK-Testkarten FD	34
7.3.1 Festlegungen zur KVNR für eGK-Testkarten FD für die gematik.....	34
7.3.2 Festlegungen zur KVNR für eGK-Testkarten FD für andere.....	35
7.4 Definition der ICCSN.....	36
7.5 Kodierung der ICCSN für die Testkarte FD	37
8 Anhang C – Bereitstellung von eGK-Testkarten FD für andere ..	38
8.1 Testkategorien RU (alt)	39

<u>8.2 Testkategorien TU (alt)</u>	<u>41</u>
<u>8.3 Testkategorien RU / Testportal</u>	<u>52</u>
<u>9 Anhang D – Zuordnung KVNR-Nummernkreise für eGK- Testkarten FD für andere</u>	<u>55</u>
<u>10 Anhang E - Bereitstellung von eGK-Testkarten FD für die gematik</u>	<u>64</u>
<u>10.1 Testdatenmanagement und Erkennbarkeit des Testdatentyps.....</u>	<u>64</u>
<u>10.2 Bereitstellung von Testkarten für die gematik.....</u>	<u>67</u>
<u>10.3 Erneute Bereitstellung von Testkarten für die gematik.....</u>	<u>67</u>
<u>11 Anhang F - Testvektoren</u>	<u>69</u>
<u>11.1 Testvektoren für Schlüsselableitung Variante 1: gematik.....</u>	<u>69</u>
<u>11.2 Testvektoren für Schlüsselableitung Variante 2: Atos</u>	<u>69</u>
<u>11.3 Testvektoren für Schlüsselableitung Variante 3: G&D</u>	<u>70</u>

1 Einführung des Dokumentes

1.1 Zielsetzung

In diesem Dokument werden die im Rahmen einer Personalisierung von eGK-Testkarten Fachdienste der ~~Generationen 2 und~~ [Generation 2.1](#) (eGK-Testkarten FD) 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 Fachdienste VSDM zu schreiben sind.

Weiterhin werden die Vorgaben zu symmetrischen Schlüsseln und die Schlüsselableitungen für eGK-Testkarten FD beschrieben.

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 (hier: eGK) 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.~~ Dazu wurden verschiedene Varianten einer eGK definiert wie beispielsweise: Testlaborkarte, Testkarte, Dummy-Karte. Dazu kommt die produktiv eingesetzte Echtkarte.


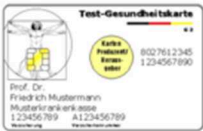
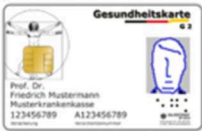

			
Testlaborkarte	Testkarte	Echtkarte	Dummy-Karte
Zulassung	Test	Wirkbetrieb	Promotion
Testlabor	Test- und Referenzumgebung	Produktiv-Umgebung	keine Funktion
Schwerpunkt: Betriebssystem (COS) und Objektsystem	Schwerpunkt: Funktionen und Abläufe	Schwerpunkt: Produktivbetrieb	Schwerpunkt: Look & Feel
CVC: 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 und der eGK-Spezifikationen zur Verwendung als eGK getestet werden. Die speziell dafür festgelegten Strukturen und Spezifikationen sind im Dokument [gemSpec_TLK_COS_G2] enthalten.

Testkarten

Testkarten dienen der Erprobung Testdurchführung in Testumgebungen mit Testdaten. Testkarten enthalten keine Echtdaten. Die in dieser Spezifikation spezifizierten Testkarten für den Test von Fachdiensten werden so personalisiert, dass ein Test von Fachanwendungen (z.B. mit Online-Anbindung an Systeme der TI) möglich ist möglich ist (etwa Online-Anbindung an Systeme der TI). Die in diesem Dokument spezifizierten Karten werden für den Test der Fachdienste VSDM und für den produktübergreifenden Test und den Ende-zu-Ende-Test der Fachanwendung VSDM genutzt. Eine mögliche Nutzung der Testkarten im Rahmen des Tests weiterer Anwendungen der TI wird von der gematik organisiert.

Testkarten müssen den technischen Spezifikationen entsprechen, wie sie in den Spezifikationen für die eGK ([gemSpec_COS] und [gemSpec_eGK_ObjSys] bzw. [gemSpec_eGK_ObjSys_G2.1]) beschrieben sind.

~~Die Testkarten enthalten keine Echtdaten.~~

~~Die in dieser Spezifikation spezifizierten Testkarten Fachdienste werden für den Test der Fachdienste VSDM und für den produktübergreifenden Test und den Ende-zu-Ende-Test der Fachanwendung VSDM genutzt.~~

~~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 Fachdienste bereitgestellt und wie die in den verschiedenen Teilen der Spezifikation festgelegten Daten für die Testkarten Fachdienste aufbereitet und in die Testkarten Fachdienste geladen bzw. aufgedruckt werden müssen. Außerdem wird die Layout-Ergänzung für Testkarten Fachdienste beschrieben.~~

1.2 Zielgruppe

Dieses Dokument ist für Kartenherausgeber, Hersteller von Karten (Chipkartenhersteller und -personalisierer), Trusted Service Provider (TSP) mit den Einheiten Certification Authority (CA) und OSCP-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 Herausgebern, 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 Personalisierung von Testkarten Fachdienste und legt die Abläufe, die Datenformate und die Verantwortung für die Erzeugung der zur Erstellung einer Testkarte Fachdienste benötigten Daten fest.

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.

1.4 Abgrenzung des Dokuments

~~Die~~Diese Spezifikation definiert Layout, Struktur, Inhalt und Umfang der Daten, die auf ~~die~~ eGK-Testkarten Fachdienste der Generation 2.1 geschrieben werden ~~müssen~~.

~~Die Festlegungen für diese eGK-Testkarten Fachdienste sind den folgenden Dokumenten zu entnehmen:~~

Spezifikation des Betriebssystems der eGK	{gemSpec_COS}
Spezifikation der eGK, Objektsystem (Generation 2)	{gemSpec_eGK_ObjSys}
Spezifikation der eGK, Objektsystem (Generation 2.1)	{gemSpec_eGK_ObjSys_G2.1}
Spezifikation der eGK, äußere Gestaltung	{gemSpec_eGK_OPT}
Befüllvorschrift für die Plattformanteile der Karten der TI (Generation 2)	{gemSpec_Karten_Fach_TIP}
Befüllvorschrift für die Plattformanteile der Karten der TI (Generation 2.1)	{gemSpec_Karten_Fach_TIP_G2.1}
Speicherstrukturen der Fachanwendung VSDM	{gemSpec_eGK_Fach_VSDM}
Inhalte der X.509-Zertifikate	{gemSpec_PKI}

Vorgaben zu eGK-Testkarten FD der Generation 1, Karten anderen Typs (etwa HBA oder SMC-B) oder anderer Generationen (etwa Generation 1 oder Generation 2) sind nicht Bestandteil des vorliegenden ~~Dokuments~~Dokumentes.

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.

Anforderungen werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke [<=] angeführten Inhalte.

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

2 Strukturen zu Herstellung von Testkarten FD

2.1 Testkarten FD

Die Herstellung von Testkarten kann von verschiedenen Herausgebern beauftragt werden. Hierzu gehören Kostenträger, Leistungserbringerorganisationen, Hersteller von Komponenten (z.B. eHealth-Kartenterminal, Konnektor) und weitere Organisationen im Gesundheitswesen. Die Rollen für die Herstellung von Testkarten entsprechen denen der Abb_TK_016, die Verantwortlichkeiten für die verschiedenen Teilaspekte kann der Herausgeber nach seinen Erfordernissen festlegen.

Hinweis: Teile von Abb TK 016 (etwa die Darstellung der CVC-Root RSA) sind obsolet.

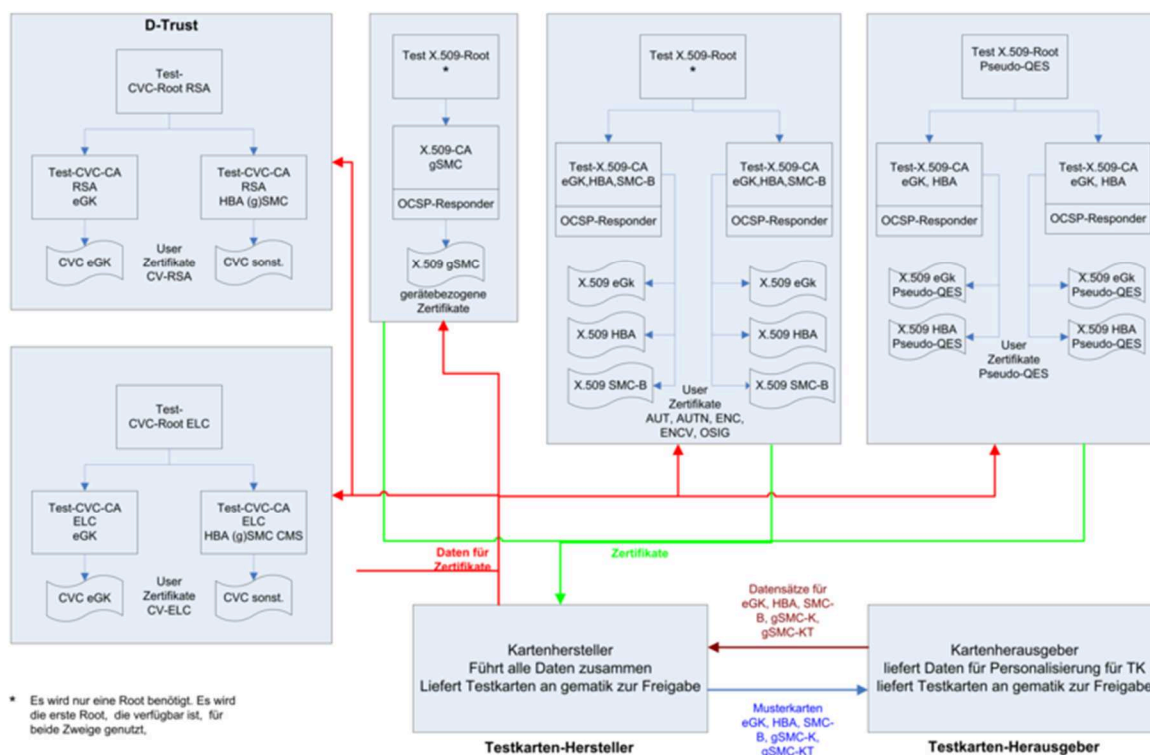


Abbildung 1: Abb_TK_016 Darstellung der Abläufe für die Erstellung von TestkartenFD (mit Test-PKI)

In den folgenden Kapiteln werden die Aufgaben der in Abb_TK_016 aufgeführten Entitäten bei der Erstellung von eGK-Testkarten FD beschrieben.

3 Vorgaben zu CV-Zertifikaten der Testkarten FD

~~3.1 CV-Zertifikate für Testkarten FD~~

~~3.1.1 Test-Root-CVC-CAs für Testkarten FD~~

Card-G2-A_3529 - CVC-CAs für Testkarten FD

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

[<=]

~~3.1.2 Test-CVC-CA für Testkarten FD~~

~~Card-G2-A_3530 – Bereitstellung von CV-Zertifikaten für eGK-Testkarten FD~~

~~Der Testkartenhersteller MUSS dafür sorgen, dass die eGK-Testkarten FD mit Test-CV-Zertifikaten für das Verfahren mit elliptischen Kurven (Schlüssellänge 256-bit) gemäß [gemSpec_PKI] ausgestattet sind.~~

~~[<=]~~

~~Card-G2-A_3531 – Erzeugung der CV-Zertifikate für Testkarten FD~~

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

~~[<=]~~

Card-G2-A_3532 - Lieferung der CV-Zertifikate für Testkarten FD

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

[<=]

4 Vorgaben zu symmetrischen Schlüsseln

4.1 Schlüsselableitung eGK-Testkarten FD

Testmaßnahmen zu Fachdiensten VSDM beinhalten unter anderem die Prüfung von Updates der VSD auf einer eGK und das Sperren und Entsperren durch das CMS. Diese Updates erfordern die Etablierung eines „trusted channel“ [beispielsweise](#) unter Verwendung symmetrischer Schlüssel, die sowohl auf der eGK als auch beim Fachdienst VSDM, der die jeweilige eGK unterstützt, [verfügbar sein müssen vorhanden sind](#). Die Automatisierung der Testmaßnahmen zu den Fachdiensten VSDM, u.a. auch eine Voraussetzung für ein Remote-Testing, setzt den Einsatz einer Kartensimulation als auch die Verwendung kartenindividueller Schlüssel voraus.

Die in diesem Dokument beschriebene Schlüsselableitung für eGK-Testkarten FD ermöglicht eine Generierung kartenindividueller Schlüssel zur Laufzeit der Testmaßnahmen und vermeidet somit eine Erfassung und Verwaltung sämtlicher in Testkarte verwendeter symmetrischer Schlüssel.

Die Herausgeber von Testkarten [müssen wählen](#) eine Variante aus den drei nachfolgend beschriebenen Verfahren [auswählen aus](#), um alle von ihnen herausgegebenen Musterkarten mit gemäß Schlüsselableitung generierten symmetrischen kartenindividuellen Schlüsseln zu personalisieren.

Card-G2-A_3533 - Bereitstellung symmetrischer Schlüssel für die Testkarten FD

Der Testkartenherausgeber MUSS die Testkarten mit symmetrischen kartenindividuellen Schlüsseln personalisieren, welche mit einer der drei nachfolgenden Varianten gebildet werden:

- Variante 1 – gematik,
- Variante 2 – atos
- Variante 3 – G&D

[<=]

~~Für jede der beschriebenen Varianten wurden für beispielhafte ICCSNs kartenindividuelle Schlüssel berechnet. Für die Testmaßnahmen ist es erforderlich, dass der jeweilige Kartenherausgeber~~

A_24092 - K Kartenherausgeber, KeyDerivation Variante benennen

~~Der Kartenherausgeber MUSS die von ihm [ausgewählte verwendete](#) Variante der Schlüsselableitung der [testdurchführenden testausführenden](#) Instanz ([etwa der gematik](#)) [benennen. \[<=\]](#)~~

~~benennt und die seinerseits berechneten symmetrischen Schlüssel für die in diesem Dokument beschriebenen ICCSNs kommuniziert.~~

~~In diesem Dokument werden Ableitungsalgorithmen angegeben, mit deren Hilfe sich kartenindividuelle symmetrische Schlüssel für AES-128 und AES-256 aus einem Masterkey und einem kartenindividuellen Merkmal herleiten lassen.~~

4.2 Konkrete Werte für Masterkey

Die in diesem Dokument enthaltenen Werte für Masterkeys dürfen ausschließlich für Testlaborkarten und für Testkarten der Generation 2 bzw. Generation 2.1 verwendet werden. Die Werte für Masterkey sind explizit NICHT zulässig für Karten, welche für die Aufnahme von echten Personendaten (scharfen Karten) bestimmt sind.

Gemäß der Spezifikation des eGK Objektsystem ist jeweils ein AES-Schlüssel mit 128-bit Schlüssellänge oder mit 256-bit Schlüssellänge zu personalisieren.

Hinweis: Die im Folgenden genannten Werte für Masterkeys sind im Wesentlichen Oktettstrings, wobei jedes Oktett um eins inkrementiert wird. Alle Werte unterscheiden sich neben der Länge ansonsten nur im ersten Oktett.

4.2.1 Schlüsseldaten

Der Masterkey (MK) besteht aus einem Oktettstring von 32 Oktett Länge.

Tabelle 1: TAB_TK_FD_001 Masterkey (MK)

A 24093 - Testkarten Masterkey nicht für Echtkarten

Die folgenden Masterkey (MK) DÜRFEN NICHT für die Produktion von Echtkarten verwendet werden:

SchlüsselnameSchlüssel	Oktettstring
MK (gematik-Verfahren für Variante 1 (<u>alle Schlüssel</u>))	000102030405060708090A0B0C0D0E0F 101112131415161718191A1B1C1D1E1F
<u>MK für Variante 2 und 3:</u>	
MK.CMS.AES128.ENC	01010203 04050607 08090a0b 0c0d0e0f
MK.CMS.AES128.MAC	02010203 04050607 08090a0b 0c0d0e0f
MK.CMS.AES256.ENC	01010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
MK.CMS.AES256.MAC	02010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
MK.VSD.AES128.ENC	03010203 04050607 08090a0b 0c0d0e0f
MK.VSD.AES128.MAC	04010203 04050607 08090a0b 0c0d0e0f
<u>MK für Varianten 2 und 3</u>	

MK.CMS.AES.ENC und MK.CMS.AES256.ENC	01010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
MK.CMS.AES.MAC und MK.CMS.AES256.MAC	02010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
MK.VSD.AES.ENC und MK.VSD.AES256.ENC	03010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
MK.VSD.AES.MAC und MK.VSD.AES256.MAC	04010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f

[<=]

Hinweis: Die genannten Werte für Masterkeys sind im Wesentlichen Oktettstrings, wobei jedes Oktett um eins inkrementiert wird. Alle Werte unterscheiden sich neben der Länge ansonsten nur im ersten Oktett.

A 24094 - Testkarten CMS-Schlüssel personalisieren

Der Kartenherausgeber MUSS dafür sorgen, dass SK.CMS.AES128 oder SK.CMS.AES256 oder beide gemäß den Vorgaben der Objektsystemspezifikation personalisiert wird. [<=]

A 24098 - Testkarten VSD-Schlüssel personalisieren

Der Kartenherausgeber MUSS dafür sorgen, dass SK.VSD.AES128 oder SK.VSD.AES256 oder beide gemäß den Vorgaben der Objektsystemspezifikation personalisiert wird. [<=]

4.2.2 Schlüsselbezeichner (KID)

Tabelle 2: Schlüsselbezeichner (KID)

Schlüssel	Oktettstring
SK.CMS.AES128.ENC	'534B2E434D532E4145533132382E454E43'
SK.CMS.AES128.MAC	'534B2E434D532E4145533132382E4D4143'
SK.CMS.AES256.ENC	'534B2E434D532E4145533235362E454E43'
SK.CMS.AES256.MAC	'534B2E434D532E4145533235362E4D4143'
SK.VSD.AES128.ENC	'534B2E5653442E4145533132382E454E43'
SK.VSD.AES128.MAC	'534B2E5653442E4145533132382E4D4143'
SK.VSD.AES256.ENC	'534B2E5653442E4145533235362E454E43'
SK.VSD.AES256.MAC	'534B2E5653442E4145533235362E4D4143'

4.3 Schlüsselableitung

4.3.1 Nomenklatur

AES	Advanced Encryption Standard mit Schlüssellängen von 128 und 256 Bit
ENC	Verwendungszweck Verschlüsselung und Entschlüsselung
MAC	Verwendungszweck MAC Berechnung und MAC Verifizierung
MK	Master Key, wird zur Ableitung kartenindividueller Schlüssel verwendet
SK	Secret Key
	Verkettung von Oktettstrings
ICCSN	Individuelle 20-stellige Kartenseriennummer BCD codiert in 10 Oktetts
KID	Schlüsselbezeichner
MSB_N	Extraktion der N führenden (most significant) Byte
SHA256(x)	Berechnung eines SHA-256 Hashwertes für Daten "x"

4.3.2 Variante 1: gematik

~~In der Vorgängerversion dieses Dokumentes für Generation 1 wurde ein Hash-MAC basierendes Verfahren aus [ANSI X9.63#5.6.3] verwendet, welches dasselbe Prinzip verwendet, wie [TR-03111#4.3.3]. Das Hash-MAC Prinzip wird in diesem Dokument auf die kartenindividuellen Schlüssel der Testkarten FD angewendet.~~

~~Kartenindividuelle AES-Schlüssel werden in der eGK im Rahmen der Kartenadministration eingesetzt. Neben dem symmetrischen Schlüssel SK.CMS, den es seit der Generation 2 in allen Kartentypen gibt (eGK, HBA, ...), ist dies die Schlüssel SK.VSD.~~

~~Anders als in [TR-03111#4.3.3.2] vorgeschlagen, wird in diesem Dokument für alle Schlüssellängen von AES stets SHA-256 verwendet um den Implementierungsaufwand zu reduzieren. Es gilt:~~

Die Schlüsselableitung beruht auf einer Modifikation des Verfahrens aus [EMV_Book-2] Anhang A1.4.3 zur Erzeugung von 16 bzw. 32 Byte langen AES-Schlüsseln.

Hierbei wird die ICCSN mit einem schlüsselindividuellen Bezeichner ([KID](#)) konkateniert. Die Berechnung des Schlüssels erfolgt dann durch AES-Verschlüsselung des zugehörigen Hashwertes mit dem Masterkey. Soweit notwendig wird der berechnete Schlüssel auf die benötigte Länge gekürzt.

~~Als Schlüsselbezeichner wird der~~

[A 24099 - Schlüsselableitung Variante 1: gematik](#)

~~Der Kartenherausgeber MUSS dafür sorgen, dass im Rahmen der Schlüsselableitung gemäß der Variante 1 (gematik) folgender Algorithmus verwendet wird:~~

~~Für Schlüssel mit Schlüsselname, erweitert um die Schlüsselverwendung, aus der Spezifikation des eGK-Objektsystems verwendet (s.u.).~~

1. **SK 128** ~~= MSB 16~~ (bit: SK.128 = AES-ECB-ENC[MK](MSB 16(SHA256(ICCSN~~H || KID~~))))))
2. **SK** Für Schlüssel mit 256 bit: SK.256 = AES-ECB-ENC[MK](SHA256(ICCSN~~H || KID~~)))

Die Werte für MK sind A 24093 zu entnehmen. Die Werte für KID der folgenden Tabelle:

Schlüssel	Oktettstring
SK.CMS.AES128.ENC	'534B2E434D532E4145533132382E454E43'
SK.CMS.AES128.MAC	'534B2E434D532E4145533132382E4D4143'
SK.CMS.AES256.ENC	'534B2E434D532E4145533235362E454E43'
SK.CMS.AES256.MAC	'534B2E434D532E4145533235362E4D4143'
SK.VSD.AES128.ENC	'534B2E5653442E4145533132382E454E43'
SK.VSD.AES128.MAC	'534B2E5653442E4145533132382E4D4143'
SK.VSD.AES256.ENC	'534B2E5653442E4145533235362E454E43'
SK.VSD.AES256.MAC	'534B2E5653442E4145533235362E4D4143'

[<=]

4.3.2.1 Beispielgenerierung

~~iccsn = 80276883110761400005~~

~~SK.CMS.AES128.ENC = 1596958D6848403879F49D4CC089EDD7~~

~~SK.CMS.AES128.MAC = A161324DE494507F603CF9E8B35BA92A~~

~~SK.CMS.AES256.ENC = 7772AF336AF2F5FD7E925AFE86F6F53A847127AF17576520158E8D5B29B88CF7~~

~~SK.CMS.AES256.MAC = FF84DADFEE1E160BF9D6C3AE00967DDDA6EE534DE9E5C5E7BFB279D9A130EBF6~~

~~SK.VSD.AES128.ENC = 9C4C1D0B98F1779376AC9F3C5ACA02CE~~

~~SK.VSD.AES128.MAC = 96FD00847B158C557662AF0E324299FC~~

~~SK.VSD.AES256.ENC = F4EDBA04E3253E6C008DDB72AF08B4FEF9BE68F8512B03FFADCB9ACE7563E0F0~~

~~SK.VSD.AES256.MAC = D9D921537BF0C8507A8444E5E9E0AE694287343ACB81304BC628BA6ABB6A1A4E~~

~~iccsn = 80276881031971421010~~

~~SK.CMS.AES128.ENC = D4DD0F4966CE13B1C8A91BE4B17972F4~~

~~SK.CMS.AES128.MAC = 7C5DCBD4ED461C85ED4AC54B92C7F821~~

~~SK.CMS.AES256.ENC = 59D0C921AEAB21782587A68D90B355B71A9F651405B07878BB216AAF7FF5D580~~

~~SK.CMS.AES256.MAC = 175B09EE81B44315CF6B85EAE14A94A8E22CC74CE06A251363150D8A0DD1EFE7~~

~~SK.VSD.AES128.ENC = 24A379C27C6A93A27D2095D2D8CFAE72~~

```
SK.VSD.AES128.MAC = FA4BCC22476AC5F287213FFFC9A80EE5
SK.VSD.AES256.ENC = 8F533C6371DDA6F957959B1B01DD8D549E5FE8C386722584FE800B57E6A208D3
SK.VSD.AES256.MAC = FB90558ADC407B1FC545380B38D71023532CD520F518AF186C59CBC9FD97E62F

icesn = 80276881190000003706
SK.CMS.AES128.ENC = 7CA08936B5E10527ED1A7AA49F931F02
SK.CMS.AES128.MAC = FD82005E7EBD041A24B285D295EE9F30
SK.CMS.AES256.ENC = 96B1C02977E8BB949BDF5B9BB33633C63DC34E9735DCD1090B650C9D044A8468
SK.CMS.AES256.MAC = FCFFA3067491771BB5B6B8BD7DE090E4855E2CB2DCCFC5020B519E1D79AF02E3
SK.VSD.AES128.ENC = BC87ADF84BDBDA62B18614BFE6FCB1C2
SK.VSD.AES128.MAC = E21CF109AE2F85FC2A465DAB622A2AD5
SK.VSD.AES256.ENC = AC7128316159603BAC3F999DC9D7B6DC51D3F035F6439DCB18DB3F750ED702CA
SK.VSD.AES256.MAC = 404E0CA76DCFA92DABB563EA23F57EFF5195872DD0F13385164C8113AD5B1906

icesn = 80276881190000003723
SK.CMS.AES128.ENC = 84F2C37EB9A894A7EE716971DC95511A
SK.CMS.AES128.MAC = 564D02F053D1A181862AAA614F51608E
SK.CMS.AES256.ENC = 7872010703E6D523BE2AA9CDBD629685A266E1C54EC6DBB63BED4A3F97240065
SK.CMS.AES256.MAC = 8F82E9B4901C4A7B2D7C731459B6940C0F8E729420A5046479A726861FFE3CB5
SK.VSD.AES128.ENC = 10D2308E9DFFA822402C48AA3A594083
SK.VSD.AES128.MAC = 00B4EBF8307DFF695530D9F3DCE10DBE
SK.VSD.AES256.ENC = 778C16D9E74780829574CC016AAA24A82C87CAE6C327BE5B5211C07E2EAE4ACE
SK.VSD.AES256.MAC = B91F79FD0787C5457A4D5EFD22E3DF897D7A8D8B01D827D1A020927AB1898539

icesn = 80276881500000001416
SK.CMS.AES128.ENC = 5BEDAB2F527A2ADB65ED458686554C36
SK.CMS.AES128.MAC = DE996C091F5D6F25E9B76B411611D15A
SK.CMS.AES256.ENC = E1F1A979C65A141C7CCA549304272B99A2BD32A615C2A3C3A50C6430CAD1829F
SK.CMS.AES256.MAC = 8CB848323D16293DE405B8B4FC7D7E1353936EC5C782F6C2A876C65AAE7C8575
SK.VSD.AES128.ENC = 0495F3524AE773910B71A16E99B3A04F
SK.VSD.AES128.MAC = D446F73FB3AAD1B4CD885AC02C5F0EAC
SK.VSD.AES256.ENC = 4C3D3CF423506BD47AADBE000B513EB8E62DA345A275CB54E251D036898CA54A
SK.VSD.AES256.MAC = FF21F6762314A62020F178B43906382FC817F05DF4D03E30DB1D946D556A1468
```

4.3.3 Variante 2: Atos Verfahren

Die Länge des ~~erzeugten SK (im Algorithmus dargestellt als ICC-MK)~~ abgeleiteten SK entspricht der Länge des übergebenen MK ~~(im Algorithmus dargestellt als IMK)~~, d.h. zur Erzeugung von z.B. eines AES-256 Schlüssels muss ein MK mit 32 Bytes (= 256 Bits) übergeben werden.

Das Verfahren basiert auf der EMV-Spezifikation, Integrated Circuit Card, Specifications for Payment Systems, Book 2 "Security and Key Management", Version 4.3, November

2011, Annex A1.4.3 (Option C). Siehe
<http://www.emvco.com/specifications.aspx?id=223>Siehe
<http://www.emvco.com/specifications.aspx?id=223>.

~~In Ergänzung zur EMV Spezifikation gilt:~~

~~PAN = ICCSN~~

~~PAN Sequence Number = not present~~

~~$Y^* = Y \text{ XOR } 0\text{xFFFFFFFFFFFFFFFFFFFFFFFF}$~~

~~Somit gilt:~~

~~$SK = ICC - MK = \text{Leftmost } k \text{ bits of } \{AES(IMK)[Y] || AES(IMK)[Y^*]\}$~~

~~wobei:~~

~~$k = \text{Anzahl der Bits des zu erzeugenden AES-Schlüssels (z. B. } k \text{ gleich } 128, 192 \text{ oder } 256)$~~

~~$Y = 0\text{x}0000000000 || \text{ICCSN-Bytes} || 0\text{x}00$~~

~~ICCSN-Bytes = BCD-kodierte ICCSN (10 Bytes)~~

4.3.3.1 Beispielgenerierung

~~Mit der ICCSN~~

~~80276001040000000001~~

~~ergeben sich mit obigen Masterkeys folgende SK-~~

A 24100 - Schlüsselableitung Variante 2: Atos

Der Kartenausgeber MUSS dafür sorgen, dass im Rahmen der Schlüsselableitung gemäß der Variante 2 (Atos) folgender Algorithmus verwendet wird:

1. $Y = '00\ 0000\ 0000' || \text{ICCSN} || '00'$

1.2. Für Schlüssel: mit

a. 128 bit ist ein Masterkey (MK) mit 128 bit zu verwenden:
 $SK = AES\text{-}ECB\text{-}ENC[MK](Y)$

b. 256 bit ist ein Masterkey (MK) mit 256 bit zu verwenden:

i. $Y^* = Y \text{ XOR } 'FFFF\ FFFF\ FFFF\ FFFF\ FFFF\ FFFF\ FFFF\ FFFF'$

ii. $SK = AES\text{-}ECB\text{-}ENC[MK](Y || Y^*)$

[<=]

~~icesn = 80276001040000000001~~

~~SK.CMS.AES128.ENC = 83B71CA85A0F940FD154409AC67AE0DB~~

~~SK.CMS.AES128.MAC = FA65036CC682E440903A9BA7F90E0F2C~~

~~SK.CMS.AES256.ENC = FA9E833E3584F7B2F27F08E2E9C4B72D4112B78A4236AF799ADF6A25584A1848~~

~~SK.CMS.AES256.MAC = FF9690C39521DD9BC7DD8D8B33B741A8888BDE8FA8DEF8DCA840079FF646AAE8~~

~~SK.VSD.AES128.ENC = 47E68B915481A7A6B772D58AB55CC48C~~

~~SK.VSD.AES128.MAC = F602F5C2F838B8230F0B623131B9A35B~~

~~SK.VSD.AES256.ENC = C82DE2D3878F8257C452F0E355A1212E2D5A3F4F96CBC4503885D3CF593C9018~~

~~SK,VSD,AES256,MAC = 1F3901DD3274FC85822853276D369BA408B5AFEE6FA2804FE42115EF0C314804~~

4.3.4 Variante 3: G&D Verfahren

Das Verfahren besteht aus einer Kombination von Hashwert-Bildung und AES-Verschlüsselung. Durch das Extrahieren der führenden Oktette aus dem Chifftrat wird die geeignete Schlüssellänge sichergestellt. ~~Die Verwendung des Datentyps „Oktettstring“ ist äquivalent zu [gemSpec_COS].~~

~~Schritt 1: HASH#1 = SHA_256(ICCSN)~~

~~Input: ICCSN als Oktettstring der Länge 10 Oktett, BCD-codiert.~~

~~Output: Oktettstring, Hash-Wert der Länge 32 Oktett~~

~~Verfahren: Bildung eines Hashwertes nach [FIPS 180-4#6.2]~~

~~Schritt 2: ENC#1 = AES_ECB(HASH#1, MK)~~

~~Input: HASH#1, Oktettstring der Länge 32 Oktett, MK, Masterkey der Länge 32 Oktett (256 Bit)~~

~~Output: Oktettstring, Chifftrat (ciphertext) der Länge 32 Oktett~~

~~Verfahren: AES-Verschlüsselung von HASH#1 im ECB-Modus mit dem Masterkey der Länge 256 Bit nach [FIPS 197]~~

~~Schritt 3: KEY#1 = Extract_MSByte (ENC#1, 16/32)~~

~~Input: ENC#1, Oktettstring der Länge 32 Oktett, 16/32, Integer, Anzahl der zu extrahierenden Elemente~~

~~Output: Oktettstring der Länge 16/32 Oktett (128/256 Bit)~~

~~Verfahren: Extrahieren der führenden Oktette, Sicherstellung der geeigneten Schlüssellänge~~

A 24101 - Schlüsselableitung Variante 3: G&D

Der Kartenausgeber MUSS dafür sorgen, dass im Rahmen der Schlüsselableitung gemäß der Variante 3 (G&D) folgender Algorithmus verwendet wird: In der Variante 3 sind nur MK-Werte mit 32 Oktett (256 bit) zulässig.

1. Für Schlüssel mit 128 bit: SK.128 = AES-ECB-ENC[MK](MSB_16 (SHA256(ICCSN)))

2. Für Schlüssel mit 256 bit: SK.256 = AES-ECB-ENC[MK](SHA256(ICCSN))

[<=]

5 Vorgaben für eGK-Testkarten FD

Card-G2-A_3534-01~~Card-G2-A_3534~~ - Einhalten der eGK-Spezifikationen für die eGK-Testkarten FD

Die eGK-Testkarten FD MÜSSEN alle Vorgaben [\[gemSpec_eGK_ObjSys_G2.1\]](#) erfüllen.~~[<=der eGK-Spezifikation erfüllen. Dies betrifft sowohl die Bereitstellung der definierten Kommandos aus [gemSpec_COS], als auch die Einrichtung der definierten File-Struktur aus [gemSpec_eGK_ObjSys] bzw. [gemSpec_eGK_ObjSys_G2.1].~~
[<=]

Hinweis: Gemäß

~~Card-G2-A_3535—3534-*~~ wird unter anderem nun gefordert, dass**Optionale Eigenschaften in der Objektsystem-Spezifikation der** eGK-Testkarten FD
Die optionalen Funktionspakete

nun auch verpflichtend mit der Option_kontaktlose_Schnittstelle auszustatten sind.

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

5.1 KÖNNEN umgesetzt werden.[<=]

5.2 PIN- und PUK-Werte

5.2.1 PIN-Werte

Card-G2-A_3536 - Werte für PIN.CH für die eGK-Testkarten FD

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

[<=]

5.2.2 PUK-Werte

Card-G2-A_3537 - Werte für PUK für die eGK-Testkarten FD

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

[<=]

5.2.3 CAN-Werte

Card-G2-A_3538 - CAN-Erzeugung für die eGK-Testkarten FD

Wenn die kontaktlose Schnittstelle umgesetzt ist, MUSS für die Erzeugung der CAN gelten:

1. Der Hersteller kann eine einzige CAN definieren, die für alle Karten genutzt wird.
2. Der Hersteller kann für jede Karte eine individuelle CAN definieren.

[<=]

5.3 Erstellung der Daten der Versicherten für Testkarten FD

5.3.1 Bereitstellung der Daten

Card-G2-A_3539 - Nutzung von fiktiven Versichertendaten für die eGK-Testkarten FD

Die Testkarten FD SOLLEN Daten von fiktiven Versicherten enthalten.

[<=]

Card-G2-A_3540 - Keine Nutzung von echten Versicherten für die eGK-Testkarten FD

Die Testkarten FD DÜRFEN NICHT Echtdaten von Versicherten enthalten.

[<=]

Card-G2-A_3541 - Übertragung der Datensätze in die eGK-Testkarten FD

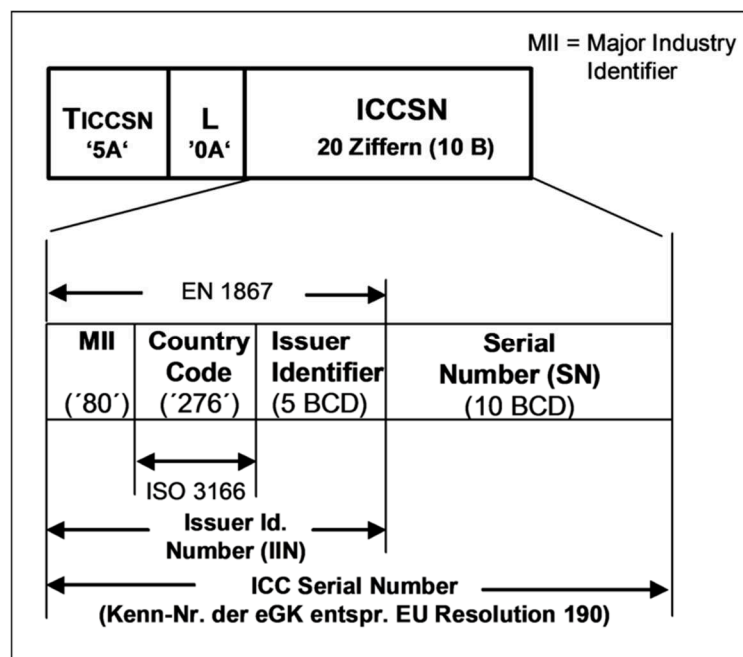
Die vom Kartenherausgeber gelieferten Daten MÜSSEN vom Testkartenkartenhersteller in die entsprechenden EFs geschrieben werden. In diesen Datensätzen sind die ICCSN-Werte gemäß den in Tab_TK_008 zusammengefassten Vorgaben enthalten.

[<=]

~~Card-G2-A_3542 - Wert für den Issuer Identifier für die eGK-Testkarten FD~~

~~Als Wert für den Issuer Identifier MUSS der für den Kartenherausgeber von der GS1 Germany GmbH – Maarweg 133 – 50825 Köln zugewiesene Wert verwendet werden, wobei die führenden Ziffern 00 für Testkarten FD durch 88 ersetzt werden MÜSSEN (siehe Anhang B2).~~

~~[<=]~~



~~Abbildung 3: Abb_TK_003 ICCSN für Gesundheitskarten~~

5.4 Erstellung der X.509-Zertifikate für Testkarten FD

5.4.1 Erstellung der X.509-Zertifikate für Testkarten FD für ENC, ENCV, AUT und AUTN

Card-G2-A_3543 - Erzeugung der X.509-Zertifikate für DF.ESIGN für die eGK-Testkarten FD

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_3544 - Schlüssellänge in DF.ESIGN für die eGK-Testkarten FD~~

~~Als Schlüssellänge für die zu den jeweiligen X.509-Zertifikaten in DF.ESIGN gehörenden Schlüssel MÜSSEN die in der Spezifikation [gemSpec_eGK_ObjSys bzw. [gemSpec_eGK_ObjSys_G2.1] festgelegten Werte verwendet werden.~~

~~[<=]~~

Card-G2-A_3545 - Identische Gültigkeitsdauer für alle X.509-Zertifikate für die eGK-Testkarten FD

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

[<=]

Card-G2-A_3546 - OCSP-Responder für X.509-Zertifikate in DF.ESIGN für die eGK-Testkarten FD

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_3547 - Eintrag von "AuthorityInfoAccess" in X.509-Zertifikate in DF-ESIGN für die eGK-Testkarten FD

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

[<=]

Card-G2-A_3548 - Lieferung der X.509-Zertifikate für DF.ESIGN für die eGK-Testkarten FD

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

[<=]

5.4.2 OID-Vorgaben für die eGK-Testkarten FD

Card-G2-A_3549 - OID-Vorgaben für die eGK-Testkarten FD

In alle X.509-Zertifikate der eGK-Testkarten FD MÜSSEN gemäß [gemSpec_PKI] und [gemRL_TSL_SP_CP] 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 FD (verpflichtend)

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

Alle angegebenen Zertifikate beziehen sich bei eGK-Testkarten FD der Generation 2 auf die Ausprägung R2048, bei eGK-Testkarten FD der Generation G2.1 auf die Ausprägungen R2048 und E256.

[<=]

5.5 CV-Zertifikate für die eGK-Testkarten FD

Es gelten die Anforderungen aus Kapitel 3

5.6 Secret Keys SK.CMS.AES128, SK.VSD.AES128 und SK.VSDCMS.AES128 für die eGK-Testkarten FD

Es gelten die Anforderungen aus Kapitel 4.

5.7 Optische Gestaltung der eGK-Testkarten FD

Card-G2-A_3550 - Maße der eGK-Testkarten FD

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

[<=]

Card-G2-A_3551 - optische Gestaltung der eGK-Testkarten FD ohne Bild

Die optische Gestaltung der Vorderseite der eGK-Testkarten FD ohne Bild MUSS gemäß Abb_TK_017 (Ausnahme Releasekennzeichnung, siehe Card-G2-A_3553) ausgeführt werden.

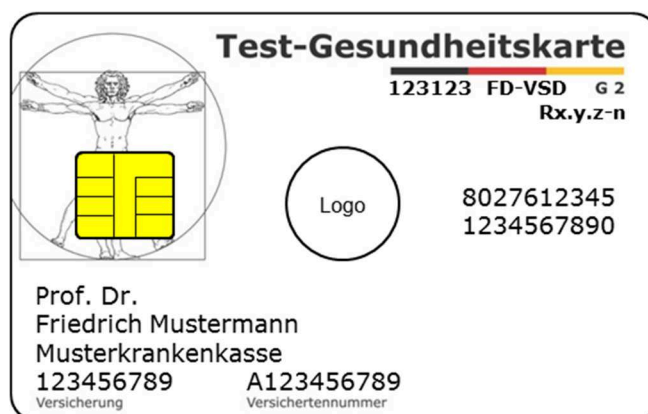


Abbildung 2: Abb_TK_017 Kartenvorderseite eGK-Testkarte FD der Generation 2 mit Personalisierung und CAN, ohne Bild, mit Releasekennzeichnung

[<=]

Card-G2-A_3552 - optische Gestaltung der eGK-Testkarten FD mit Bild

Die optische Gestaltung der Vorderseite der eGK-Testkarten F mit Bild MUSS gemäß Abb_TK_018 (Ausnahme Releasekennzeichnung, siehe Card-G2-A_3553) ausgeführt werden:

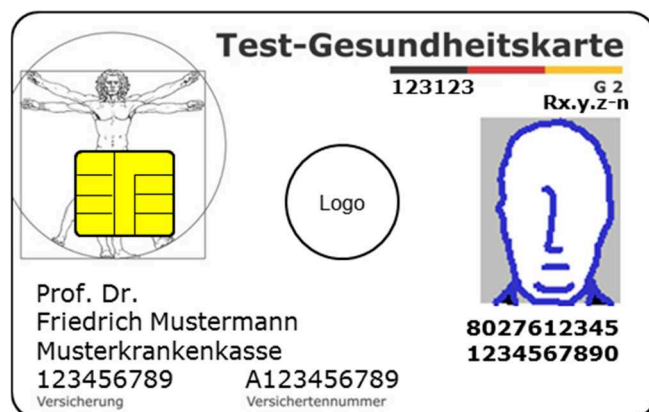


Abbildung 3: Abb_TK_018 Kartenvorderseite eGK-Testkarte FD der Generation 2 mit Personalisierung, mit Bild, mit CAN, mit Releasekennzeichnung

[<=]

Die Anordnung ICCSN ist jeweils beispielhaft.

Card-G2-A_3553 - Kennzeichnung der Releasezugehörigkeit für die eGK-Testkarten FD

Der Hersteller KANN das Release, nach dessen Spezifikationsstand die eGK-Testkarten hergestellt worden sind, im Format Rx.y.z-n in der Schriftart Verdana True Type in der

Größe 6 pt fett in Schwarz auf die Vorderseite (gemäß Abb_TK_017 und Abb_TK_018 rechtsbündig zur Kennzeichnung der Generation) oder auf die Rückseite (zusammen mit der ICCSN, falls kein EHIC-Feld vorhanden ist) drucken.

Die konkrete Zeichenkette für „Rx.y.z-n“ wird durch die gematik vorgegeben.

[<=]

Card-G2-A_3554 - Kennzeichnung als eGK-Testkarten FD

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

[<=]

Card-G2-A_3555-01 ~~Card-G2-A_3555~~ - Kennzeichnung der Generation der eGK-Testkarten FD

Die Generation der eGK-Testkarten FD MUSS optisch unterscheidbar sein. Deshalb MUSS unter dem Block der nationalen Farben rechtsbündig die folgende Zeichenfolge eingefügt werden:

- für eGK-Testkarten FD der Generation 2.1 die Zeichenfolge „G 2¹“.

~~für eGK-Testkarten FD der Generation 2.1 die Zeichenfolge „G 2.1“.~~ [<=]

Card-G2-A_3556 - Daten zur Person auf der eGK-Testkarten FD

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

[<=]

Card-G2-A_3557 - Regeln für die Vergabe von IK, IIN und VKNR für die eGK-Testkarten FD

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_3558 - BSI-Logo auf eGK-Testkarten FD

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

[<=]

Für eGK-Testkarten ist eine Fotopersonalisierung nicht verpflichtend.

Card-G2-A_3559 - ICCSN für die eGK-Testkarten FD

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

[<=]

Card-G2-A_3560 - ICCSN auf eGK-Testkarten FD mit Fotopersonalisierung

Wird die eGK-Testkarte FD mit einem Foto gemäß [gemSpec_eGK_OPT] versehen, MUSS die ICCSN entweder an anderer Stelle der Vorderseite (Beispiel siehe Abbildung Abb_TK_018) oder auf die Rückseite (z. B. im dafür vorgesehenen EHIC-Feld, falls vorhanden) aufgedruckt werden.

[<=]

Card-G2-A_3561 - ICCSN auf eGK-Testkarten FD ohne Fotopersonalisierung

Bei eGK-Testkarten FD ohne Fotopersonalisierung KANN die ICCSN in der für das Foto vorgesehenen Fläche in zwei Zeilen mit je 10 Stellen je Zeile gemäß Abb_TK_017 aufgedruckt werden. Ausrichtung rechtsbündig zum Schriftzug „Gesundheitskarte“. Schrift analog der sonstigen Personalisierung auf der Vorderseite.

[<=]

Card-G2-A_3562 - CAN-Aufdruck für die eGK-Testkarten FD

Wenn die kontaktlose Schnittstelle umgesetzt ist, MUSS die in Card-G2-A_3538 definierte 6-stellige CAN 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_017 und Abb_TK_018).

[<=]

Card-G2-A_3563 - Logo des Kartenherausgebers der eGK auf eGK-Testkarten FD

An der in Abb_TK_017 und Abb_TK_018 festgelegten Stelle MUSS das Logo des Kartenherausgebers der eGK-Testkarten FD aufgedruckt werden.

[<=]

Card-G2-A_3564 - Entwerteter EHIC-Aufdruck auf der Rückseite der eGK-Testkarten FD

Die Kartenrückseite der Testkarte KANN 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_3565 - Nutzung der gematik-Vorlagen zur Bedruckung der eGK-Testkarten FD

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

[<=]

6 Anhang A – Verzeichnisse

6.1 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)
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

Kürzel	Erläuterung
OCSP	Online Certificate Status Protocol
PIN	Persönliche Identifikationsnummer
PuK	Public Key (öffentlicher Schlüssel)
PUK	Pin Unblocking Key
PrK	Private Key (privater Schlüssel)
TLV	Tag Length Value
TSP	Trusted Service Provider (früher CA genannt)
XML	Universelle Datenbeschreibungssprache (Extensible Markup Language)
ZDA	Zertifizierungsdiensteanbieter

6.2 Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

6.3 Abbildungsverzeichnis

Abbildung 1: Abb_TK_001 Definition der verschiedenen Kartentypen am Beispiel der eGK	8
Abbildung 2: Abb_TK_016 Darstellung der Abläufe für die Erstellung von TestkartenFD (mitTest-PKI)	11
Abbildung 3: Abb_TK_003 ICCSN für Gesundheitskarten	22
Abbildung 4: Abb_TK_017 Kartenvorderseite eGK-Testkarte FD der Generation 2 mit Personalisierung und CAN, ohne Bild, mit Releasekennzeichnung	25
Abbildung 5: Abb_TK_018 Kartenvorderseite eGK-Testkarte FD der Generation 2 mit Personalisierung, mit Bild, mit CAN, mit Releasekennzeichnung	25
Abbildung 6: Abb_TK_015 Aufbau einer ICCSN	37
Abbildung 1: Abb_TK_016 Darstellung der Abläufe für die Erstellung von TestkartenFD (mitTest-PKI)	11
Abbildung 2: Abb_TK_017 Kartenvorderseite eGK-Testkarte FD der Generation 2 mit Personalisierung und CAN, ohne Bild, mit Releasekennzeichnung	25
Abbildung 3: Abb_TK_018 Kartenvorderseite eGK-Testkarte FD der Generation 2 mit Personalisierung, mit Bild, mit CAN, mit Releasekennzeichnung	25

Abbildung 4: Abb TK 015 Aufbau einer ICCSN	37
--	----

6.4 Tabellenverzeichnis

Tabelle 1: TAB_TK_FD_001 Masterkey (MK)	14
Tabelle 2: Schlüsselbezeichner (KID)	15
Tabelle 3: Tab_TK_001 OID-Referenzen für eGK-Testkarten FD (verpflichtend).....	24
Tabelle 4: TAB_TK_FD_007 Issuer Identification Number	33
Tabelle 5: Aufbau der KVNR.....	36
Tabelle 6: Tab_TK_008 Kodierung der ICCSN für Testkarten FD	38
Tabelle 7: TAB_TK_FD_009 Kategorisierung der Testkarten eGK Fachdienste VSDM für die RU.....	39
Tabelle 8: TAB_TK_FD_010 Kategorisierung der Testkarten eGK Fachdienste VSDM für die TU.....	41
Tabelle 9: TAB_TK_FD_012 Kriterien zur Neulieferung von Testkarten	53
Tabelle 10: TAB_TK_FD_011 Zuordnung der KVNR-Nummernkreise.....	56
Tabelle 1: Tab TK 001 OID-Referenzen für eGK-Testkarten FD (verpflichtend).....	24
Tabelle 2: TAB TK FD 007 Issuer Identification Number	33
Tabelle 3: TAB TK FD 014 Aufbau der KVNR für eGK Testkarten FD für die gematik	35
Tabelle 4 TAB TK FD 015 Zuordnung zweite Stelle der KVNR zu Fachdienstbetreibern VSDM	35
Tabelle 5: TAB TK FD 016 Aufbau der KVNR	36
Tabelle 6: TAB TK FD 009 Kategorisierung der Testkarten eGK Fachdienste VSDM für die RU.....	39
Tabelle 7: TAB TK FD 010 Kategorisierung der Testkarten eGK Fachdienste VSDM für die TU.....	41
Tabelle 8: TAB TK FD 011 Zuordnung der KVNR-Nummernkreise	56
Tabelle 9 TAB TK FD 017 Definition von Testdatentypen und Zuordnung des Vornamens des Testversicherten	65
Tabelle 10: TAB TK FD 012 Kriterien zur Neulieferung von eGK-Testkarten FD für die gematik	68

6.5 Referenzierte Dokumente

6.5.1 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 jeweils gültige Versionsnummer entnehmen Sie bitte der aktuellen, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemKPT_Test]	gematik: Testkonzept der TI
[gemPers_eGK]	gematik: Übergabeschnittstelle für die Kartenproduktion von eGKs der Generation 2 Anmerkung: Die endgültige Festlegung der Formate erfolgt in Abstimmung mit den Testkartenherstellern
[gemRL_TSL_SP_CP]	gematik: Certificate Policy - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[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_ObjSys_G2.1]	gematik: Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem für eGK der Generation 2.1
[gemSpec_eGK_OPT]	gematik: Spezifikation der elektronischen Gesundheitskarte Äußere Gestaltung für eGK der Generation 2
[gemSpec_Karten_Fach_TIP]	gematik: Befüllvorschriften für die Plattformanteile der Karten der TI
[gemSpec_Karten_Fach_TIP_G2.1]	gematik: Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1
[gemSpec_OID]	gematik: Spezifikation OID
[gemSpec_PKI]	gematik: Spezifikation PKI

[gemSpec_TLK_COS_G2]	gematik: Spezifikation der Testlaborkarte COS / Objektsysteme
[gemSpec_eGK_Fach_VSDM]	gematik: Speicherstrukturen der eGK für die Fachanwendung VSDM

6.5.2 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
EMV Book-2	EMV® Integrated Circuit Card, Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.4, October 2022 https://www.emvco.com/emv-technologies/emv-contact-chip/

7 Anhang B – Festlegungen

Für die eGK-Testkarten FD wird neben allgemeinen Festlegungen unterschieden zwischen eGK-Testkarten, die der gematik bereitzustellen sind ("eGK-Testkarten FD für die gematik") und Karten, welche die Kostenträger oder deren FDB VSDM für andere Nutzer herausgeben ("eGK-Testkarten FD für andere"). Allgemeine Festlegungen benennen dementsprechend nur "eGK-Testkarten FD" bzw. "Testkarten FD" (ohne weitere Zusätze).

Änderungen an den Festlegungen zur Bildung der KVNR bedürfen einer gemeinsamen Abstimmung zwischen gematik und dem betrieblichen VSDM Gremium des GKV-SV (BUAG). Damit soll vermieden werden, dass es zu ungewollten Überschneidungen bei der Bildung der KVNRs bei Herausgabe an die gematik oder andere Nutzer kommt.

7.1 Festlegungen für die IK des Kostenträgers für eGK-Testkarten FD

Card-G2-A_3566 - Festlegung der IK für eGK-Testkarten FD

Für die Testkarten FD MUSS die IK des Kartenherausgebers verwendet werden.
[<=]

7.2 Festlegungen zur IIN des Kartenherausgebers für Testkarten FD

Card-G2-A_3567 - IIN des Kartenherausgebers für Testkarten FD

Die Issuer Identification Number MUSS, wie in TAB_TK_FD_007 angegeben, gebildet werden.

Tabelle 2: TAB_TK_FD_007 Issuer Identification Number

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

[<=]

Card-G2-A_3568 - Issuer Identifier (Herausgeberkennung) für Testkarten FD

Als Issuer Identifier (Herausgeberkennung) für die Testkarten FD MUSS folgender Wert verwendet werden:

Ziffern 1 – 2: 88

Ziffern 3 – 5: die Ziffern 3 – 5 des von der GSI für den Kartenherausgeber vergebenen Wertes für den Issuer Identifier (Herausgeberkennung). Der Issuer Identifier ist Bestandteil der ICCSN (siehe TAB_TK_FD_008)

[<=]

7.3 Festlegungen zur KVNR für eGK-Testkarten FD

Card-G2-A_3569-01~~Card-G2-A_3569~~ - Regel zur Bildung des unveränderlichen Teils der KVNR für Testkarten FD

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

Vorschrift für die Bildung des unveränderlichen Teils der KVNR:

1 Buchstabe (A-Z),

8 Ziffern (0-9) und

1 Prüfziffer (0-9).

Der Buchstabe und die 8 Ziffern sind für jede Testkarte eindeutig zu vergeben. Werte mit mehr als drei aufeinander folgenden gleichen Ziffern in der gesamten Ziffernfolge inkl. Prüfziffer werden ausgeschlossen.

[<=]

Für die eGK-Testkarten im Rahmen der Zulassungstest der Fachdienste VSDM-FD gilt:

Card-G2-A_3572-01 - Bereitstellung der KVNR für die Testkarte FD

Der Kartenherausgeber für die eGK Testkarten FD MUSS sicherstellen, dass die KVNR

1. der von von ihm ausgegebenen Karten eineindeutig ist und

1.2. den Regeln gemäß Card-G2-A_3569 und A_24047 bzw. Card-G2-A_3570-01-* entsprechen

[<=]

7.3.1 Festlegungen zur KVNR für eGK-Testkarten FD für die gematik

Für die Bildung~~Aufbau~~ der KVNR ~~bei~~ für eGK-Testkarten FD für die gematik gilt:

Für den Aufbau der KVNR der Testkarten für die Zulassungstests der Fachdienste VSDM A_24047 - Aufbau der KVNR bei eGK-Testkarten FD für die gematik

Für den Aufbau der KVNR der eGK Testkarten FD für die gematik MÜSSEN folgende Vorgaben umgesetzt werden, um die einzelnen Testkarten, deren Zuordnung zum ausgebenden FDB VSDM und den damit verknüpften Kostenträger schnell anhand der aufgedruckten Versichertennummer unterscheiden zu können:

Tabelle 3: TAB TK FD 014 Aufbau der KVNR für eGK Testkarten FD für die gematik

<u>1. Stelle</u>	<u>Buchstabe "F".</u>
<u>2. Stelle</u>	<u>Index für den bereitstellenden FDB VSDM.</u>
<u>3. Stelle</u>	<u>Index für den Kostenträger, der vom FDB VSDM bereitgestellt wurde.</u>
<u>4. bis 9. Stelle</u>	<u>laufende Nummer</u>
<u>10. Stelle</u>	<u>P = Prüzfiffer gemäß Vorgabe</u>

Die Versichertennummer wird gemäß den Vorgaben zur optischen Gestaltung auf der Vorderseite der Testkarte aufgedruckt.

[<=]

Tabelle 4 TAB TK FD 015 Zuordnung zweite Stelle der KVNR zu Fachdienstbetreibern VSDM

<u>Wert der 2. Stelle der KVNR</u>	<u>Zugeordneter Fachdienstbetreiber VSDM</u>
<u>1</u>	<u>ARGE AOK-Rechenzentrum</u>
<u>2</u>	<u>BITMARCK Technik GmbH</u>
<u>3</u>	<u>gkv informatik</u>
<u>4</u>	<u>IT S Care - IT-Services für den Gesundheitsmarkt</u>
<u>5</u>	<u>itsc GmbH</u>
<u>6</u>	<u>kubus IT</u>
<u>7</u>	<u>Mobil ISC GmbH</u>
<u>8</u>	<u>Techniker Krankenkasse</u>
<u>9</u>	<u>Worldline</u>

7.3.2 Festlegungen zur KVNR für eGK-Testkarten FD für andere

Für die Bildung der KVNR für eGK-Testkarten FD für andere gilt:

Card-G2-A 3570-02 - Aufbau der KVNR bei eGK-Testkarten FD für andere

Für den Aufbau der KVNR der eGK-Testkarten FD für andere MÜSSEN folgende Vorgaben umgesetzt werden, um die einzelnen Testkarten und Testkategorien schnell anhand der aufgedruckten Versichertennummer unterscheiden zu können:
und eine klare Trennung von eGK-Testkarten FD für die gematik gewährleisten zu können:

Tabelle 5: TAB TK FD 016 Aufbau der KVNR

1. + 3. Stelle	Oberkennung Kostenträger (z.B. A, 1 für AOK)
4. - 5. Stelle	Ausdifferenzierung Kostenträger bei AOK, BKK, IKK (z.B. A,1,06 für AOK Bayern), ansonsten gemäß Vorgabe frei belegbar
6. - 8. Stelle	Testfallkategorie gemäß TAB_TK_FD_009 bzw. TAB_TK_FD_010 (z.B. 201 = Umzug innerhalb einer Stadt)
2. + 9. Stelle	laufende Nummer (00 bis 99 dezimal) für mehrere Karten mit gleicher Kategorie und Kostenträger. Bei laufenden Nummern < 10 ist die 2. Stelle der KVNR = 0.
10. Stelle	P = Prüfziffer gemäß Vorgabe

Die Versichertennummer wird gemäß den Vorgaben zur optischen Gestaltung auf der Vorderseite der Testkarte aufgedruckt.

[<=]

Die gültigen Werte für die Oberkennung (Stellen 1,3) und die Kostenträgernummer (Stellen 4-5) der einzelnen Krankenkassen sind im Anhang D in TAB_TK_FD_011 aufgeführt.

Card-G2-A_3571—gleiche aufeinander folgende Ziffern in der KVNR für die Testkarte FD

Die Testkarte FD DARF NICHT eine KVNR mit mehr als drei gleiche aufeinander folgende Ziffern enthalten.

[<=]

Eine Prüfung des Verbots der Nutzung von mehr als drei aufeinander folgenden gleichen Ziffern erfolgt bei der Erstellung der KVNR.

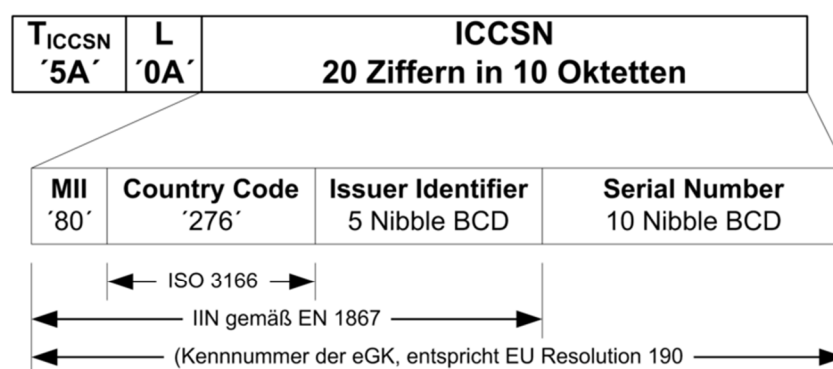
Card-G2-A_3572—Bereitstellung der KVNR für die Testkarte FD

7.4 Die KVNR für die eGK-Testkarten FD, die nach dieser Spezifikation erstellt werden, MÜSSEN vom Kartenherausgeber entsprechend den angegebenen Regeln erstellt werden. Der Kartenherausgeber MUSS sicherstellen, dass die KVNR für die von

~~ihm ausgegebenen Karten eindeutig ist.~~
~~[<=]~~

7.5 Definition der ICCSN

Die ICCSN einer Chipkarte 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 Identifier

Abbildung 4: Abb_TK_015 Aufbau einer ICCSN

7.6 Kodierung der ICCSN für die Testkarte FD

~~Card-G2-A 3573-01~~~~Card-G2-A-3573~~ - Vorgaben zur Bildung der ICCSN für die Testkarte FD

Um eine leichtere Zuordnung von Testkarten FD 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 6).~~~~Card-G2-A 3567 und Card-G2-A 3568 festgelegt.~~ Die Kodierung für die Stellen 11 bis 20 der ICCSN für Testkarten FD ist eine Zählnummer, die vom Kartenherausgeber festgelegt wird. Die ICCSNs werden vom Kartenherausgeber generiert und mit den jeweiligen Datensätzen an den Testkartenhersteller übermittelt oder vom Testkartenhersteller mit einem mit dem Kartenherausgeber abgestimmten Verfahren erzeugt.

~~[<=]~~

8 Tab_TK_008 Kodierung der ICCSN für Anhang C – Bereitstellung von eGK-Testkarten FD für andere

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

[<=]

Anhang C—Dieses Kapitel enthält die alten Kategoriedefinitionen, die in der Version 1.3 dieses Dokumentes definiert wurden. Die Beschreibung bleibt erhalten, damit die alte Definition nachvollziehbar bleibt. Bei Bedarf ist es möglich, sie im Rahmen der Herausgabe von eGK-Testkarten FD für andere zu nutzen, sofern die damit verbundene Testdaten-Funktionalität ebenfalls erhalten bleibt. Ansonsten bleiben die Kategoriennummern, solange reserviert, wie bereits herausgegebene eGK-Testkarten FD diese Kategorien nutzen und noch gültig sind. Eine Freigabe der Nummernbereiche bedarf der Abstimmung zwischen der gematik und dem betrieblichen VSDM Gremium des GKV-SV (BUAG). Damit werden Konflikte mit bereits von der gematik in Nutzung befindlichen Testkarten FD verhindert.

8.1 Testkategorien RU/~~TU~~ (alt)

~~8.2 Testkategorien RU~~

In der folgenden Tabelle TAB_TK_FD_009 sind informativ die ehemaligen Testkategorien für die Testkarten für den produktübergreifenden Test in der RU dargestellt.

~~Card G2 A_3574 — Bereitstellung Testkartensatz RU durch Fachdienstbetreiber VSDM~~

~~Jeder Fachdienstbetreiber VSDM MUSS der gematik im Rahmen der Zulassungstests der Fachdienste VSDM jeweils 10 Testkartensätze gemäß TAB_TK_FD_009 für die RU liefern.~~[<=]

Tabelle 6: TAB_TK_FD_009 Kategorisierung der Testkarten eGK Fachdienste VSDM für die RU

Kat .	Kat . alt	Ausprägung	Update - flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
400	069	physisch	VSDD	ja	Umzug in anderen KV-Bezirk + Zuordnung bes. Personengruppe	Änderung der Straßenadr./WO P + bes. Personengruppe "nichts" zu 4 (ALG II) bzw. zurück -> Änderung von PD, VD und GVD
401	069	physisch	VSDD	ja	siehe Kat. 400	siehe Kat. 400
402	069	physisch	VSDD	ja	siehe Kat. 400	siehe Kat. 400

Kat.	Kat. alt	Ausprägung	Update - flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
403	069	physisch	VSDD	ja	siehe Kat. 400	siehe Kat. 400
404	069	physisch	VSDD	ja	siehe Kat. 400	siehe Kat. 400
405	069	physisch	VSDD	ja	siehe Kat. 400	siehe Kat. 400
406	069	physisch	VSDD	ja	siehe Kat. 400	siehe Kat. 400
407	069	physisch	VSDD	ja	siehe Kat. 400	siehe Kat. 400
408	069	physisch	VSDD	ja	siehe Kat. 400	siehe Kat. 400
409	069	physisch	VSDD	ja	siehe Kat. 400	siehe Kat. 400
410	090	physisch	CMS	ja	Sperrung der Gesundheitsanwendungen	DISABLE DF.HCA (an einem ungeraden Tag) und zurück (an einem geraden Tag)
411	090	physisch	CMS	ja	siehe Kat. 410	siehe Kat. 410
412	090	physisch	CMS	ja	siehe Kat. 410	siehe Kat. 410
413	090	physisch	CMS	ja	siehe Kat. 410	siehe Kat. 410
414	090	physisch	CMS	ja	siehe Kat. 410	siehe Kat. 410
415	090	physisch	CMS	ja	siehe Kat. 410	siehe Kat. 410
416	090	physisch	CMS	ja	siehe Kat. 410	siehe Kat. 410
417	090	physisch	CMS	ja	siehe Kat. 410	siehe Kat. 410
418	090	physisch	CMS	ja	siehe Kat. 410	siehe Kat. 410
419	090	physisch	CMS	ja	siehe Kat. 410	siehe Kat. 410

Für Festlegungen zum Flip/Flop-Verfahren siehe [gemKPT_Test].

8.38.2 Testkategorien TU (alt)

In der folgenden Tabelle TAB_TK_FD_010 sind [informativ](#) die [ehemaligen](#) Testkategorien für die Testkarten für den Produkttest der Fachdienste VSDM und den produktübergreifenden Test in der TU dargestellt.

~~Card G2-A_3575-01 – Bereitstellung Testkartensatz TU durch Fachdienstbetreiber VSDM~~

~~Jeder Fachdienstbetreiber VSDM MUSS der gematik im Rahmen der Zulassungstests der Fachdienste VSDM jeweils zwei Testkartensätze gemäß TAB_TK_FD_010 für die TU liefern. Bei mandantenfähigen Fachdiensten MUSS der Fachdienstbetreiber zusätzlich jeweils zwei Testkartensätze gemäß TAB_TK_FD_010 für einen zusätzlichen Mandaten liefern.~~

~~[<=]~~

~~Card G2-A_3576 – Bereitstellung Testkarten durch Anbieter~~

~~Jeder Anbieter von Fachdiensten VSDM (Krankenkasse) MUSS der gematik im Rahmen der Zulassungstests der Fachdienste VSDM mindestens 2 physische Testkarten bereitstellen und durch den Betreiber seiner Fachdienste verwalten lassen. Für diese Testkarten sind mindestens die Kategorien 244 (vormals 069) und 260 (vormals 090) zu verwenden.~~

~~[<=]~~

Hinweis:

Wegen Card-G2-A_3571-3569-01 wird generell auf die Vergabe von Kategorienummern mit drei gleichen Ziffern, für physische Testkarten zusätzlich auf zwei gleiche führende Ziffern verzichtet.

Die Vergabe der KVNR kann für die virtuellen Testkarten von der Festlegung zum Aufbau der KVNR (siehe Card-G2-A_3570-0102) abweichen, da virtuelle Testkarten unter Verwendung der eindeutigen ICCSN adressiert werden.

Tabelle 7: TAB_TK_FD_010 Kategorisierung der Testkarten eGK Fachdienste VSDM für die TU

Kat.	Kat. alt	Ausprägung	Update-flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
200	010	physisch	VSDD	ja	Änderung des Ortsnamens, Strassennamens und Anschriftenzusatzes	Änderung am Ende von vollen Feldern incl. Sonderzeichen
201	010	physisch	VSDD	ja	siehe Kat. 200	siehe Kat. 200
201	010	physisch	VSDD	ja	siehe Kat. 200	siehe Kat. 200

Kat. .	Kat. alt	Ausprägung	Update -flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
203	015	physisch	VSDD	ja	Umzug in anderen KVBezirk	Änderung der Adresse / WOP -> WOP soll zu PLZ und Ort passen
210	028	physisch	VSDD	ja	Zuordnung zu einem DMP	von "ohne Zuordnung" zu 1 (Diab. Typ 2 und zurück)
211	028	physisch	VSDD	ja	siehe Kat. 210	siehe Kat. 210
212	028	physisch	VSDD	ja	siehe Kat. 210	siehe Kat. 210
213	028	physisch	VSDD	ja	siehe Kat. 210	siehe Kat. 210
220						Diese Kategorie ist absichtlich unbelegt. Die bisherige Definition wurde durch Kategorie 235 ersetzt.
221						Diese Kategorie ist absichtlich unbelegt. Die bisherige Definition wurde durch Kategorie 236 ersetzt.
222						Diese Kategorie ist absichtlich unbelegt. Die bisherige Definition wurde durch Kategorie 237 ersetzt.
223						Diese Kategorie ist absichtlich unbelegt. Die bisherige Definition wurde durch Kategorie 238 ersetzt.

Kat.	Kat. alt	Ausprägung	Update -flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
230	041	physisch	VSDD	ja	Änderung der Versichertenart	von Mitglied auf Familienversicherter bzw. zurück
231	041	physisch	VSDD	ja	siehe Kat. 230	siehe Kat. 230
232	041	physisch	VSDD	ja	siehe Kat. 230	siehe Kat. 230
233	041	physisch	VSDD	ja	siehe Kat. 230	siehe Kat. 230
234	041	physisch	VSDD	ja	siehe Kat. 230	siehe Kat. 230
235	036	physisch	VSSD	ja	Zuordnung zu besonderer Personengruppe	von „ohne Zuordnung“ zu 4 (Sozialhilfeempfänger) bzw. zurück. (Dieser Eintrag ersetzt die vormalige Kategorie 220, siehe Hinweis)
236	036	physisch	VSSD	ja	siehe Kat. 235	sehe Kat. 235 (Dieser Eintrag ersetzt die vormalige Kategorie 221, siehe Hinweis)
237	036	physisch	VSSD	ja	siehe Kat. 235	sehe Kat. 235 (Dieser Eintrag ersetzt die vormalige Kategorie 222., siehe Hinweis)
238	036	physisch	VSSD	ja	siehe Kat. 235	sehe Kat. 235 (Dieser Eintrag ersetzt die vormalige Kategorie 223, siehe Hinweis)
240	056	physisch	VSDD	ja	Änderung des abrechnenden Kostenträgers	von "ohne" zu Angabe einer Kennung, Name und Lcode bzw. zurück

Kat. .	Kat. alt	Ausprägung	Update- flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
241	064	physisch	VSDD	ja	Setzen des VersicherungsschutzEn de	von "ohne Angabe" auf 31.12.20xx und zurück (xx = aktuelles Jahr minus 1)
242	067	physisch	VSDD	ja	Verlängern des Versicherungsschutzes	von 31.12.20xx auf 31.12.20xy und zurück (xx = aktuelles Jahr minus 1)(xy = aktuelles Jahr)
243	069	physisch	VSDD	ja	Umzug in anderen KV- Bezirk + Zuordnung bes. Personengruppe	Änderung der Straßenadr./WOP + bes. Personengruppe "nichts" zu 4 (ALG II) bzw. zurück -> Änderung von PD, VD und GVD
244	069	physisch	VSDD	ja	siehe Kat. 243	siehe Kat. 243
245	069	physisch	VSDD	ja	siehe Kat. 243	siehe Kat. 243

Kat.	Kat. alt	Ausprägung	Update-flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
250	085	physisch	-	nein	Karte mit gesperrtem AUT Zertifikat	<p>Online gesperrtes Zertifikat, aber DF.HCA enabled aktiviert</p> <p>Hinweis zur Bereitstellung: Methode zur Erstellung der Karte:</p> <ul style="list-style-type: none"> FDB stellt eGK mit einmaliger Sperren-Operation bereit (wie Kategorie 260, aber kein Flip-Flop) Gematik führt die Sperren-Operation aus (-> Zertifikat wird gesperrt und DF.HCA auf disabled gesetzt wird deaktiviert) Gematik reaktiviert danach mit eigenem Tooling DF.HCA wieder, das Zertifikat bleibt dadurch gesperrt
251	085	physisch	-	nein	siehe Kat. 250	siehe Kat. 250
252	085	physisch	-	nein	siehe Kat. 250	siehe Kat. 250
253	-	physisch	-	nein	eGK ohne Update	

Kat. .	Kat. alt	Ausprägung	Update -flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
260	090	physisch	CMS	ja	Sperren der Gesundheitsanwendungen	DISABLE DEACTIVATE DF.HCA (an einem ungeraden Tag) und zurück (an einem geraden Tag)
261	090	physisch	CMS	ja	siehe Kat. 260	siehe Kat. 260
262	090	physisch	CMS	ja	siehe Kat. 260	siehe Kat. 260
263	090	physisch	CMS	ja	siehe Kat. 260	siehe Kat. 260
264	091	physisch	CMS	ja	Entsperren der Gesundheitsanwendungen	ENABLE ACTIVATE DF.HCA und zurück, Flip-Flop-Rhythmus entgegengesetzt zu Kategorien 260
265	091	physisch	CMS	ja	siehe Kat. 264	siehe Kat. 264
266	091	physisch	CMS	ja	siehe Kat. 264	siehe Kat. 264
267	091	physisch	CMS	ja	siehe Kat. 264	siehe Kat. 264
270	-	physisch	-	nein		Für spätere Anwendungen, ohne Flip-Flop
271	-	physisch	-	nein		
272	-	physisch	-	nein		
273	-	physisch	-	nein		
274	-	physisch	-	nein		
275	-	physisch	-	nein		
276	-	physisch	-	nein		
277	-	physisch	-	nein		
278	-	physisch	-	nein		

Kat. .	Kat. alt	Ausprägung	Update -flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
279	-	physisch	-	nein		
300	017	virtuell	VSDD	ja	Änderung der Hausnummer	
301	017	virtuell	VSDD	ja	siehe Kat. 300	
302	017	virtuell	VSDD	ja	siehe Kat. 300	
303	017	virtuell	VSDD	ja	siehe Kat. 300	
304	017	virtuell	VSDD	ja	siehe Kat. 300	
305	017	virtuell	VSDD	ja	siehe Kat. 300	
306	017	virtuell	VSDD	ja	siehe Kat. 300	
310	037	virtuell	VSDD	ja	Änderung Zuordnung zu besonderer Personengruppe	von "ohne Zuordnung" zu 6 (BVG) bzw. zurück
311	037	virtuell	VSDD	ja	siehe Kat. 310	siehe Kat. 310
312	037	virtuell	VSDD	ja	siehe Kat. 310	siehe Kat. 310
313	037	virtuell	VSDD	ja	siehe Kat. 310	siehe Kat. 310
314	037	virtuell	VSDD	ja	siehe Kat. 310	siehe Kat. 310
315	037	virtuell	VSDD	ja	siehe Kat. 310	siehe Kat. 310
320	042	virtuell	VSDD	ja	Änderung der Versichertenart	von Familienversicherter auf Rentner bzw. zurück
321	042	virtuell	VSDD	ja	siehe Kat. 320	siehe Kat. 320
322	042	virtuell	VSDD	ja	siehe Kat. 320	siehe Kat. 320
323	042	virtuell	VSDD	ja	siehe Kat. 320	siehe Kat. 320
324	042	virtuell	VSDD	ja	siehe Kat. 320	siehe Kat. 320

Kat.	Kat. alt	Ausprägung	Update-flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
325	042	virtuell	VSDD	ja	siehe Kat. 320	siehe Kat. 320
330	092	virtuell	CMS+ VSDD	ja	Sperren der Gesundheitsanwendungen und Umzug in eine andere Stadt	wie Kategorien 331 + Änderung der Adresse und zurück Alternative, fall <u>falls</u> UFS beim <u>SperrenDeaktivieren</u> der eGK das Updateflag für VSDD nicht ausliefert: - ungerader Tag: <u>SperrenDeaktivieren</u> der Gesundheitsanwendung - gerader Tag: <u>EntsperrenAktivieren</u> der Gesundheitsanwendung + Änderung der Adresse
331	093	virtuell	CMS	ja	Sperren der Gesundheitsanwendungen	DISABLEDEACTIVATE DF.HCA (an einem ungeraden Tag) und zurück (an einem geraden Tag)
332	094	virtuell	CMS	ja	siehe Kat. 331	siehe Kat. 331
333						Diese Kategorie ist absichtlich unbelegt. Die bisherige Definition wurde durch Kategorie 337 ersetzt.
334	096	virtuell	CMS	ja	siehe Kat. 331	siehe Kat. 331
335	097	virtuell	CMS	ja	siehe Kat. 331	siehe Kat. 331
336	098	virtuell	CMS	ja	siehe Kat. 331	siehe Kat. 331

Kat. .	Kat. alt	Ausprägung	Update -flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
337	095	virtuell	CMS	ja	siehe Kat. 331	siehe Kat. 331 Dieser Eintrag ersetzt die vormalige Kategorie 333
340	101	virtuell	CMS	ja	Entsperren der Gesundheitsanwendung en	ENABLE DF.HCA und zurück, Flip-Flop-Rythmus entgegengesetzt zu Kategorien 331-336
341	102	virtuell	CMS	ja	siehe Kat. 340	siehe Kat. 340
342	103	virtuell	CMS	ja	siehe Kat. 340	siehe Kat. 340
343	104	virtuell	CMS	ja	siehe Kat. 340	siehe Kat. 340
344	105	virtuell	CMS	ja	siehe Kat. 340	siehe Kat. 340
345	106	virtuell	CMS	ja	siehe Kat. 340	siehe Kat. 340
350		virtuell	VSDD	nein	siehe Kat. 200	Optionale Testkarten - OneTimeCard (OTC), wird bei den FDB benötigt, bei denen ein SOAP-Fehler mit Code 12105 zu einer Deaktivierung der eGK im Backend der Fachdienste führt, so dass im weiteren Testverlauf die eGK im Flip-Flop- Verfahren nicht mehr nutzbar ist. einmaliges Update
351		virtuell	VSDD	nein	siehe Kat. 200	
352		virtuell	VSDD	nein	siehe Kat. 200	
353		virtuell	VSDD	nein	siehe Kat. 200	

Kat. .	Kat. alt	Ausprägung	Update -flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
354		virtuell	VSDD	nein	siehe Kat. 200	
355		virtuell	VSDD	nein	siehe Kat. 200	
356		virtuell	VSDD	nein	siehe Kat. 200	
357		virtuell	VSDD	nein	siehe Kat. 200	
358		virtuell	VSDD	nein	siehe Kat. 200	
359		virtuell	VSDD	nein	siehe Kat. 200	
360		virtuell	VSDD	nein	siehe Kat. 200	
361		virtuell	VSDD	nein	siehe Kat. 200	
362		virtuell	VSDD	nein	siehe Kat. 200	
363		virtuell	VSDD	nein	siehe Kat. 200	
364		virtuell	VSDD	nein	siehe Kat. 200	
365		virtuell	VSDD	nein	siehe Kat. 200	
367		virtuell	VSDD	nein	siehe Kat. 200	
368		virtuell	VSDD	nein	siehe Kat. 200	
369		virtuell	VSDD	nein	siehe Kat. 200	

Kat. .	Kat. alt	Ausprägung	Update -flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
370		virtuell	CMS	nein	siehe Kat. 331	Optionale Testkarten - OneTimeCard (OTC), wird bei den FDB benötigt, bei denen ein SOAP-Fehler mit Code 12105 zu einer Deaktivierung der eGK im Backend der Fachdienste führt, so dass im weiteren Testverlauf die eGK im Flip-Flop- Verfahren nicht mehr nutzbar ist. einmaliges Update
371		virtuell	CMS	nein	siehe Kat. 331	
372		virtuell	CMS	nein	siehe Kat. 331	
373		virtuell	CMS	nein	siehe Kat. 331	
374		virtuell	CMS	nein	siehe Kat. 331	
375		virtuell	CMS	nein	siehe Kat. 331	
376		virtuell	CMS	nein	siehe Kat. 331	
377		virtuell	CMS	nein	siehe Kat. 331	
378		virtuell	CMS	nein	siehe Kat. 331	
379		virtuell	CMS	nein	siehe Kat. 331	
380		virtuell	CMS	nein	siehe Kat. 331	
381		virtuell	CMS	nein	siehe Kat. 331	
382		virtuell	CMS	nein	siehe Kat. 331	
383		virtuell	CMS	nein	siehe Kat. 331	

Kat.	Kat. alt	Ausprägung	Update-flags für	Flip / Flop	Beschreibung des Testdatensatzes	Details und Hinweise
384		virtuell	CMS	nein	siehe Kat. 331	
385		virtuell	CMS	nein	siehe Kat. 331	
386		virtuell	CMS	nein	siehe Kat. 331	
387		virtuell	CMS	nein	siehe Kat. 331	
388		virtuell	CMS	nein	siehe Kat. 331	
389		virtuell	CMS	nein	siehe Kat. 331	

Für Festlegungen zum Flip/Flop-Verfahren siehe [gemKPT_Test].

8.48.3 Testkategorien RU / Testportal

~~Für den produktübergreifenden Test in der RU über das Solange die gematik im Testportal sind durch die eine fachliche Testsuite zur Durchführung als EvT der FDB VSDM bereitstellt, benötigen die Fachdienstbetreiber virtuelle Testkarten nach Definition in bereitzustellen.~~

~~A_20635—Testkategorien RU—virtuelle Testkarten~~

~~Jeder Fachdienstbetreiber MUSS in der Umgebung RU mindestens einen Testkartensatz gemäß TAB_TK_FD_010 in der Ausprägung „virtuell“, Diese virtuellen Testkarten werden in diesem Sinne als eGK-Testkarten FD für die Nutzung durch das Testportal der gematik bereitstellen. [≤=]~~

~~andere durch die FDB VSDM bereitgestellt.~~

Die virtuellen Testkartensätze gemäß TAB_TK_FD_010 der TU können für die Bereitstellung in der RU nachgenutzt werden.

Die Bereitstellung von mehr als einem Testkartensatz bzw. Testkartenteilsätzen ist zulässig und besonders für OTC-Karten sinnvoll.

8.5 Bereitstellung von Testkarten nach der Zulassung

~~In 8.1 Testkategorien RU, 8.2 Testkategorien TU und 8.3 Testkategorien RU / Testportal ist die Bereitstellung von Testkartensätzen für die Zulassung eines Fachdienstes geregelt. Für den Nachweis des korrekten Betriebs des Fachdienstes kann es aufgrund von Änderungen der Mandanten oder des Personalisierers und weiterer Kriterien im Betrieb des Fachdienstes notwendig sein, erneut Testkartensätze bereitzustellen.~~

~~A_20515—Bereitstellung von Testkarten im Betrieb~~

~~Der Fachdienstbetreiber VSDM MUSS der gematik Testkartensätze gemäß TAB_TK_FD_009 und TAB_TK_FD_010 bereitstellen, sobald mindestens ein Kriterium aus~~

~~TAB_TK_FD_012 zutrifft. Dabei MÜSSEN die jeweiligen „Bedingungen zur Lieferung der Testkarten“ aus TAB_TK_FD_012 eingehalten werden.~~

~~Der Fachdienstbetreiber MUSS die Lieferung der Testkarten selbstständig ohne Aufforderung der gematik veranlassen (soweit nicht anders lautend unter „Bedingungen zur Lieferung der Testkarten“ festgelegt).~~

~~Tabelle 9: TAB_TK_FD_012 Kriterien zur Neulieferung von Testkarten~~

Kriterium zur Neulieferung von Testkarten	Bedingungen zur Lieferung der Testkarten
Bereitgestellte Testkarten werden aufgrund der Laufzeit der Zertifikate ungültig, Karten dieser Produkttypversion werden aber weiterhin noch mindestens 12 Monate produktiv im Feld betrieben.	Die Lieferung der Testkarten an die gematik erfolgt bis spätestens 3 Monate vor dem Ende der Gültigkeit der betroffenen Testkarten.
Bereitgestellte Testkarten sind defekt oder nicht mehr nutzbar, Karten dieser Produkttypversion werden aber weiterhin produktiv im Feld betrieben.	Die Lieferung der Ersatzkarten erfolgt zeitnah in Abstimmung mit der gematik nach Identifikation betroffener Karten.
Die Produkttypversion der Produktivkarten wird gewechselt (beispielweise durch Änderung der Generation der Karten)	Die Lieferung der Testkarten erfolgt so früh wie möglich.
Der Personalisierer der Produktivkarten wechselt.	Die Lieferung der Testkarten an die gematik erfolgt bis spätestens 3 Monate vor dem Ende der Gültigkeit der Testkarten des ehemaligen Personalisierers.
Der Fachdienstbetreiber gibt Produktivkarten für zusätzliche, neue Mandanten (Kassen) heraus. Dieses kann auch durch den Wechsel des Fachdienstbetreibers durch eine Kasse ohne Datenmigration der Bestandsdaten verursacht sein.	Die Lieferung der Testkarten erfolgt so früh wie möglich, idealerweise vor der Herausgabe von Produktivkarten durch den Fachdienstbetreiber für den zusätzlichen, neuen Mandanten.
Der Fachdienstbetreiber einer Kasse wechselt, der Datenbestand wird migriert. Der Personalisierer wechselt.	Siehe "Der Personalisierer der Produktivkarten wechselt".
Der Fachdienstbetreiber einer Kasse wechselt, der Datenbestand wird migriert. Ein Wechsel des Personalisierers findet nicht statt	Keine Neulieferung erforderlich.

Kriterium zur Neulieferung von Testkarten	Bedingungen zur Lieferung der Testkarten
Zwei oder mehrere Kassen fusionieren unter Beibehaltung der bisherigen Provider IDs	Siehe "Der Fachdienstbetreiber gibt Produktivkarten für zusätzliche, neue Mandanten (Kassen) heraus" bzw. "Der Personalisierer der Produktivkarten wechselt".
Zwei oder mehrere Kassen fusionieren, es entsteht eine neue Provider ID.	Die Lieferung der Testkarten erfolgt so früh wie möglich, idealerweise vor der Herausgabe von Produktivkarten durch den Fachdienstbetreiber für die fusionierte Kasse.

9 {<=>}

10 Anhang D – Zuordnung KVNR-Nummernkreise für eGK-Testkarten FD für andere

Hinweis:

Die Kombination von Werten der Oberkennung und Ausdifferenzierung Kostenträger, Kategorie der Testkarte und laufender Nummer der Testkarte soll keine Ziffernfolgen mit mehr als drei gleichen, aufeinanderfolgenden Ziffern erzeugen. Aus diesem Grund wird auf die Vergabe von zwei gleichen Ziffern für die Ausdifferenzierung verzichtet.

Tabelle 8: TAB_TK_FD_011 Zuordnung der KVNR-Nummernkreise

Kategorie	Oberkennung	Nr	Kostenträger	zugewiesener Nummernkreis
AOK	A,1	01	AOK - Die Gesundheitskasse für Niedersachsen	Ax101xxxxP
AOK	A,1	02	AOK - Die Gesundheitskasse in Hessen	Ax102xxxxP
AOK	A,1	05	AOK Baden-Württemberg	Ax105xxxxP
AOK	A,1	06	AOK Bayern	Ax106xxxxP
AOK	A,1	09	AOK Bremen/Bremerhaven	Ax109xxxxP
AOK	A,1	21	AOK PLUS - Die Gesundheitskasse für Sachsen und Thüringen	Ax121xxxxP
AOK	A,1	12	AOK Rheinland/Hamburg	Ax112xxxxP
AOK	A,1	13	AOK Sachsen-Anhalt	Ax113xxxxP
AOK	A,1	14	AOK NordWest	Ax114xxxxP
AOK	A,1	16	AOK Rheinland-Pfalz/Saarland	Ax116xxxxP
AOK	A,1	17	AOK Nordost	Ax117xxxxP
BARMER	B,1	01	BARMER GEK	Bx101xxxxP
BKK	C,1	01	atlas BKK ahlmann	Cx101xxxxP

Kategorie	Ober- kennung	Nr	Kostenträger	zugewiesener Nummernkreis
BKK	C,1	02	Audi Betriebskrankenkasse	Cx102xxxxP
BKK	C,1	03	BAHN-BKK	Cx103xxxxP
BKK	C,1	04	Bertelsmann BKK	Cx104xxxxP
BKK	C,1	05	Betriebskrankenkasse - Würth	Cx105xxxxP
BKK	C,1	06	Betriebskrankenkasse Achenbach Buschhütten	Cx106xxxxP
BKK	C,1	07	Betriebskrankenkasse Basell Polyolefine GmbH	Cx107xxxxP
BKK	C,1	08	Betriebskrankenkasse Braun Gillette	Cx108xxxxP
BKK	C,1	09	Betriebskrankenkasse der BMW AG	Cx109xxxxP
BKK	C,1	10	Betriebskrankenkasse der BPW	Cx110xxxxP
BKK	C,1	12	Betriebskrankenkasse der G. M. PFAFF AG	Cx112xxxxP
BKK	C,1	13	Betriebskrankenkasse der Grillo- Werke AG	Cx113xxxxP
BKK	C,1	14	Betriebskrankenkasse der MTU	Cx114xxxxP
BKK	C,1	15	Betriebskrankenkasse der SIEMAG	Cx115xxxxP
BKK	C,1	16	Betriebskrankenkasse der VICTORIA und D.A.S.(Fusion mit BIG direkt gesund)	Cx116xxxxP
BKK	C,1	17	Betriebskrankenkasse Ernst & Young	Cx117xxxxP
BKK	C,1	18	Betriebskrankenkasse Freudenberg	Cx118xxxxP
BKK	C,1	19	Betriebskrankenkasse Groz-Beckert	Cx119xxxxP
BKK	C,1	20	Betriebskrankenkasse HEIMBACH GmbH & Co.	Cx120xxxxP

Kategorie	Ober- kennung	Nr	Kostenträger	zugewiesener Nummernkreis
BKK	C,1	21	Betriebskrankenkasse Herford Minden Ravensberg	Cx121xxxxP
BKK	C,1	22	Betriebskrankenkasse KBA	Cx122xxxxP
BKK	C,1	23	BKK Wirtschaft & Finanzen	Cx123xxxxP
BKK	C,1	24	Betriebskrankenkasse KRONES	Cx124xxxxP
BKK	C,1	25	Betriebskrankenkasse LINDE	Cx125xxxxP
BKK	C,1	26	Betriebskrankenkasse MAHLE	Cx126xxxxP
BKK	C,1	27	Betriebskrankenkasse Maschinenfabrik und Eisengießerei Meuselwitz	Cx127xxxxP
BKK	C,1	28	Betriebskrankenkasse Mobil Oil	Cx128xxxxP
BKK	C,1	30	Betriebskrankenkasse PricewaterhouseCoopers	Cx130xxxxP
BKK	C,1	31	Betriebskrankenkasse RIEKER . RICOSTA . WEISSER	Cx131xxxxP
BKK	C,1	32	Betriebskrankenkasse RWE	Cx132xxxxP
BKK	C,1	33	Betriebskrankenkasse S - H	Cx133xxxxP
BKK	C,1	34	Betriebskrankenkasse Schwarzwald- Baar-Heuberg	Cx134xxxxP
BKK	C,1	35	Betriebskrankenkasse Verkehrsbau Union	Cx135xxxxP
BKK	C,1	36	BKK R + V	Cx136xxxxP
BKK	C,1	37	BKK Pro Vita (vorher:BKK A.T.U)	Cx137xxxxP
BKK	C,1	38	BKK advita	Cx138xxxxP
BKK	C,1	39	BKK Aesculap	Cx139xxxxP

Kategorie	Ober- kennung	Nr	Kostenträger	zugewiesener Nummernkreis
BKK	C,1	40	BKK Akzo Nobel - Bayern -	Cx140xxxxP
BKK	C,1	41	actimonda BKK	Cx141xxxxP
BKK	C,1	42	BKK B. Braun Melsungen AG	Cx142xxxxP
BKK	C,1	43	BKK Beiersdorf AG	Cx143xxxxP
BKK	C,1	44	BKK BJB GmbH & Co. KG (Fusion mit BKK Gildemeister Seidensticker)	Cx144xxxxP
BKK	C,1	45	BKK DEMAG KRAUSS-MAFFEI	Cx145xxxxP
BKK	C,1	48	Thüringer Betriebskrankenkasse	Cx148xxxxP
BKK	C,1	49	BKK Diakonie	Cx149xxxxP
BKK	C,1	50	BKK Dürkopp Adler	Cx150xxxxP
BKK	C,1	51	BKK Essanelle (Fusion mit Deutsche BKK)	Cx151xxxxP
BKK	C,1	52	BKK EUREGIO	Cx152xxxxP
BKK	C,1	53	BKK EWE	Cx153xxxxP
BKK	C,1	54	BKK exklusiv	Cx154xxxxP
BKK	C,1	55	BKK Faber-Castell & Partner	Cx155xxxxP
BKK	C,1	56	BKK firmus	Cx156xxxxP
BKK	C,1	58	BKK GILDEMEISTER SEIDENSTICKER	Cx158xxxxP
BKK	C,1	59	BKK HENSCHEL Plus	Cx159xxxxP
BKK	C,1	60	BKK Herkules	Cx160xxxxP
BKK	C,1	61	BKK family	Cx161xxxxP
BKK	C,1	62	BKK Karl Mayer	Cx162xxxxP

Kategorie	Ober- kennung	Nr	Kostenträger	zugewiesener Nummernkreis
BKK	C,1	63	BKK Kassana (Fusion mit BKK VerbundPlus)	Cx163xxxxP
BKK	C,1	64	BKK MEDICUS (Fusion mit BKK VBU)	Cx164xxxxP
BKK	C,1	65	BKK Melitta Plus	Cx165xxxxP
BKK	C,1	66	BKK Merck	Cx166xxxxP
BKK	C,1	67	BKK Miele	Cx167xxxxP
BKK	C,1	68	BKK Pfalz	Cx168xxxxP
BKK	C,1	69	BKK Publik	Cx169xxxxP
BKK	C,1	70	BKK Salzgitter	Cx170xxxxP
BKK	C,1	71	BKK Scheufelen	Cx171xxxxP
BKK	C,1	72	BKK Stadt Augsburg	Cx172xxxxP
BKK	C,1	73	BKK Technoform	Cx173xxxxP
BKK	C,1	74	BKK TUI	Cx174xxxxP
BKK	C,1	75	BKK VDN Vereinigte Deutsche Nickel- Werke AG	Cx175xxxxP
BKK	C,1	76	BKK VerbundPlus	Cx176xxxxP
BKK	C,1	77	BKK Vital	Cx177xxxxP
BKK	C,1	78	BKK vor Ort	Cx178xxxxP
BKK	C,1	79	BKK Voralb	Cx179xxxxP
BKK	C,1	80	BKK Werra-Meissner	Cx180xxxxP
BKK	C,1	81	BKK ZF & Partner	Cx181xxxxP
BKK	C,1	82	BKK24	Cx182xxxxP

Kategorie	Ober- kennung	Nr	Kostenträger	zugewiesener Nummernkreis
BKK	C,1	83	Bosch BKK	Cx183xxxxP
BKK	C,1	84	Brandenburgische BKK	C0184xxxxP
BKK	C,1	85	Daimler BKK	Cx185xxxxP
BKK	C,1	86	DIE BERGISCHE KRANKENKASSE	Cx186xxxxP
BKK	C,1	87	Debeka Betriebskrankenkasse	Cx187xxxxP
BKK	C,1	88	Deutsche BKK	Cx188xxxxP
BKK	C,1	89	Die Continentale BKK	Cx189xxxxP
BKK	C,1	91	energie-BKK	Cx191xxxxP
BKK	C,1	92	E.ON Betriebskrankenkasse	Cx192xxxxP
BKK	C,1	93	ESSO BKK (Fusion mit Novitas BKK)	Cx193xxxxP
BKK	C,1	94	Gemeinsame Betriebskrankenkasse der Gesellschaften der "textilgruppe hof"	Cx194xxxxP
BKK	C,1	95	Gemeinsame Betriebskrankenkasse der Wieland-Werke AG	Cx195xxxxP
BKK	C,1	96	Metzinger BKK	Cx196xxxxP
BKK	C,1	97	HEAG BKK	Cx197xxxxP
BKK	C,1	98	Heimat Krankenkasse	Cx198xxxxP
BKK	C,1	99	HypoVereinsbank BKK (Fusion mit BKK Mobil Oil)	Cx199xxxxP
BKK	C,2	02	mhplus Betriebskrankenkasse	Cx202xxxxP
BKK	C,2	03	NOVITAS BKK	Cx203xxxxP
BKK	C,2	04	pronova BKK	Cx204xxxxP

Kategorie	Ober- kennung	Nr	Kostenträger	zugewiesener Nummernkreis
BKK	C,2	06	Salus BKK	Cx206xxxxP
BKK	C,2	07	SBK Siemens Betriebskrankenkasse	C0207xxxxP
BKK	C,2	08	Schwenninger BKK	Cx208xxxxP
BKK	C,2	09	SECURVITA BKK	Cx209xxxxP
BKK	C,2	10	Shell BKK / LIFE (Fusion mit DAK Gesundheit)	Cx210xxxxP
BKK	C,2	12	Südzucker-Betriebskrankenkasse	Cx212xxxxP
BKK	C,2	13	Vaillant BKK	C0213xxxxP
BKK	C,2	14	Vereinigte BKK	Cx214xxxxP
BKK	C,2	15	WMF Betriebskrankenkasse	Cx215xxxxP
BKK	C,2	16	SKD BKK	Cx211xxxxP
BKK	C,2	21	Betriebskrankenkasse der Deutsche Bank AG	Cx221xxxxP
BSRV	U,1	01 - 99	Bitmarck Service	Ux101xxxxP - Ux199xxxxP
DAK	D,1	01	D A K - Gesundheit	Dx101xxxxP
IKK	I,1	01	IKK Brandenburg und Berlin	Ix101xxxxP
IKK	I,1	02	IKK classic	Ix102xxxxP
IKK	I,1	03	IKK gesund plus	Ix103xxxxP
IKK	I,1	04	IKK Nord	Ix104xxxxP
IKK	I,1	05	IKK Südwest	Ix105xxxxP
KKH	K,1	01	Kaufmännische Krankenkasse - KKH	Kx101xxxxP
LANDW	L,1	09	Sozialversicherung für Landwirtschaft, Forsten und Gartenbau (SVLFG)	Lx109xxxxP

Kategorie	Ober- kennung	Nr	Kostenträger	zugewiesener Nummernkreis
SONST	P,1	01	Hanseatische Krankenkasse	Px101xxxxP
SONST	Q,1	01	hkk Erste Gesundheit	Qx101xxxxP
SONST	R,1	01	Knappschaft	Rx101xxxxP
SONST	S0,	01	BIG direkt gesund	Sx101xxxxP
TK	T,1	01	Techniker Krankenkasse	Tx101xxxxP

11 Anhang E - Bereitstellung von eGK-Testkarten FD für die gematik

11.1 Testdatenmanagement und Erkennbarkeit des Testdatentyps

Die eGK-Testkarten FD für die gematik benötigen für die Testdurchführung eine Bereitstellung von wechselnden Versichertenstammdaten bzw. einen Statuswechsel des Kartencontainers DF.HCA (ENABLED <-> DISABLED) im Flip-Flop-Verfahren (siehe [gemKPT_Test#Flip/Flop-Verfahren]).

Um leicht zu erkennen, welche wechselnden Testdaten mit der entsprechenden Karte verknüpft sind, werden Festlegungen zu der Art der wechselnden Daten und deren Erkennbarkeit getroffen.

A 24052 - Flip/Flop-Daten zu eGK-Testkarten FD für die gematik und deren Erkennbarkeit

Der Fachdienstbetreiber VSDM MUSS wechselnde Testdaten nach TAB TK FD 017 und gemäß [gemKPT_Test#Flip/Flop-Verfahren] für die entsprechend benannte Testumgebung bereitstellen. Der FDB VSDM MUSS dafür jeder eGK-Testkarte FD für die gematik den in TAB TK FD 017 für einen Testdatentyp definierten String als Vornamen des Testversicherten festlegen.

**Tabelle 9 TAB TK FD 017 Definition von Testdatentypen und Zuordnung des Vornamens
des Testversicherten**

<u>Testdatentyp</u>	<u>Testumgebung</u>	<u>Vorname des Testversicherten</u>	<u>Details zu den Testdaten</u>
<u>VSD-Update</u>	<u>RU</u>	<u>"Rvsd"</u>	<u>VSD-Update mit Umzug in einen anderen KV-Bezirk + Zuordnung besondere Personengruppe</u>
<u>CMS-Update mit eGK-Sperrung bzw. eGK-Entsperrung</u>	<u>RU</u>	<u>"Rcms"</u>	<u>eGK-Sperrung: der Status des Containers DF.HCA wird deaktiviert (DEACTIVATE Kommando)</u> <u>eGK-Entsperrung: der Status des Containers DF.HCA wird aktiviert (ACTIVATE Kommando)</u>
<u>VSD-Update</u>	<u>TU</u>	<u>"Tvsd"</u>	<u>VSD-Update mit Umzug in einen anderen KV-Bezirk + Zuordnung besondere Personengruppe</u>
<u>CMS-Update mit eGK-Sperrung an einem ungeraden Tag</u>	<u>TU</u>	<u>"Tcmsu"</u>	<u>eGK-Sperrung an einem ungeraden Tag: der Status des Containers DF.HCA wird deaktiviert (DEACTIVATE Kommando)</u> <u>eGK-Entsperrung an einem geraden Tag: der Status des Containers DF.HCA wird aktiviert (ACTIVATE Kommando)</u>
<u>CMS-Update mit eGK-Sperrung an einem geraden Tag</u>	<u>TU</u>	<u>"Tcmsg"</u>	<u>eGK-Sperrung an einem geraden Tag: der Status des Containers DF.HCA wird deaktiviert (DEACTIVATE Kommando)</u> <u>eGK-Entsperrung an einem ungeraden Tag: der Status des Containers DF.HCA wird aktiviert (ACTIVATE Kommando)</u>

<u>Testdatentyp</u>	<u>Testumgebung</u>	<u>Vorname des Testversicherten</u>	<u>Details zu den Testdaten</u>
<u>Kombination VSD-Update mit CMS-Update</u>	<u>TU</u>	<u>"Tcmsvsd"</u>	<u>Es wird eine Kombination von CMS-Update und VSD-Update bereitgestellt.</u> <u>Ob zusammen mit dem Sperren der eGK auch ein VSD-Update bereitgestellt wird SOLL entsprechend dem produktiven Verhalten der jeweiligen FD VSDM erfolgen.</u>

[<=]

11.2 Bereitstellung von Testkarten für die gematik

Die Anzahl von zu liefernden eGK-Testkarten für die gematik für die RU und TU pro Testdatentyp werden wie folgt definiert:

A 24053 - Bereitstellung Testkartensatz RU durch Fachdienstbetreiber VSDM

Jeder Fachdienstbetreiber VSDM MUSS der gematik im Rahmen der Zulassungstests der Fachdienste VSDM einen Testkartensatz bestehend aus:

- 150 Testkarten mit CMS-Update ("Rcms") und
- 150 Testkarten VSD-Update ("Rvsd")

gemäß TAB TK FD 017 für die RU liefern. [<=]

A 24054 - Bereitstellung Testkartensatz TU durch Fachdienstbetreiber VSDM

Jeder Fachdienstbetreiber VSDM MUSS der gematik im Rahmen der Zulassungstests der Fachdienste VSDM jeweils einen Testkartensatz bestehend aus

- 30 Testkarten mit VSD-Update ("Tvsd")
- 10 Testkarten mit CMS-Update für ungerade Tage ("Tcmsu")
- 10 Testkarten mit CMS-Update für gerade Tage ("Tcmsg")
- 2 Testkarten mit Kombination CMS-Update und VSD-Update ("Tcmsvsd")

gemäß TAB TK FD 017 für die TU liefern.

Bei mandantenfähigen Fachdiensten MUSS der Fachdienstbetreiber zusätzlich einen zweiten Testkartensatz gemäß zuvor genannter Vorgaben für einen zusätzlichen Mandaten liefern. [<=]

11.3 Erneute Bereitstellung von Testkarten für die gematik

Es gibt verschiedene Bedingungen, unter denen eine erneute Bereitstellung von eGK-Testkarten FD für die gematik notwendig wird. Dies dient dem Erhalt der durchgehenden Testbarkeit. Sowohl für den eigenen Bestätigungstest der FD VSDM als auch der Testbarkeit für andere Anwendungen oder für Dritte in der RU.

A 20515-01 - Erneute Bereitstellung von eGK-Testkarten FD für die gematik

Der Fachdienstbetreiber VSDM MUSS der gematik die in Kapitel 10.2 definierten Testkartensätze erneut bereitstellen, sobald mindestens ein Kriterium aus TAB TK FD 012 zutrifft. Dabei MÜSSEN die jeweiligen „Bedingungen zur Lieferung der Testkarten“ aus TAB TK FD 012 eingehalten werden.
Der Fachdienstbetreiber MUSS die Lieferung der Testkarten selbstständig ohne Aufforderung der gematik veranlassen, soweit nicht anders lautend unter „Bedingungen zur Lieferung der Testkarten“ festgelegt.

Tabelle 10: TAB TK FD 012 Kriterien zur Neulieferung von eGK-Testkarten FD für die gematik

<u>Kriterium zur Neulieferung von Testkarten</u>	<u>Bedingungen zur Lieferung der Testkarten</u>
<u>Bereitgestellte Testkarten werden aufgrund der Laufzeit der Zertifikate ungültig, Karten dieser Produkttypversion werden aber weiterhin noch mindestens 12 Monate produktiv im Feld betrieben.</u>	<u>Die Lieferung der Testkarten an die gematik erfolgt bis spätestens 3 Monate vor dem Ende der Gültigkeit der betroffenen Testkarten.</u>
<u>Bereitgestellte Testkarten sind defekt oder nicht mehr nutzbar, Karten dieser Produkttypversion werden aber weiterhin produktiv im Feld betrieben.</u>	<u>Die Lieferung der Ersatzkarten erfolgt zeitnah in Abstimmung mit der gematik nach Identifikation betroffener Karten.</u>
<u>Die Produkttypversion der Produktivkarten wird gewechselt (beispielweise durch Änderung der Generation der Karten)</u>	<u>Die Lieferung der Testkarten in der neuen Produkttypversion erfolgt so früh wie möglich.</u>
<u>Eine Kasse, für die von einem FDB VSDM eGK-Testkarten für die gematik bereitgestellt wurden</u> <ul style="list-style-type: none"> <u>fusioniert mit einer anderen Kasse, wobei die eGK-Testkarten für die gematik ihre Nutzbarkeit verlieren (z. B. die Konfiguration zur Adressierung durch den Konnektor & Intermediär wird ungültig).</u> <u>Wechselt den Fachdienstbetreiber und der neue Fachdienstbetreiber kann oder will nicht die alten eGK-Testkarten für die gematik und die damit verknüpften Testdaten zur Nutzung bereitstellen.</u> 	<u>Die Lieferung der Testkarten erfolgt so früh wie möglich. Die Möglichkeit zur Durchführung von Tests mit dem betroffenen Fachdienstbetreiber muss sichergestellt bleiben.</u>

[<=]

Im Rahmen dieser erneuten Bereitstellung können Folgekarten erstellt werden, sofern die Bedingungen für die Bildung der KVNR die gleichen geblieben sind.

Hinweis: Es ist zulässig, aber nicht verpflichtend Folgekartennummern auf die Karten aufzudrucken.

12 Anhang F - Testvektoren

12.1 Testvektoren für Schlüsselableitung Variante 1: gematik

Dieser Abschnitt enthält Testvektoren für die Schlüsselableitung gemäß A 24099. Die Angaben sind informativ und ohne Gewähr.

ICCSN = 80276883110761400005

```
SK.CMS.AES128.ENC = 1596958d6848403879f49d4cc089edd7
SK.CMS.AES128.MAC = a161324de494507f603cf9e8b35ba92a
SK.VSD.AES128.ENC = 9c4c1d0b98f1779376ac9f3c5aca02ce
SK.VSD.AES128.MAC = 96fd00847b158c557662af0e324299fc
SK.CMS.AES256.ENC = 7772af336af2f5fd7e925afe86f6f53a847127af17576520158e8d5b29b88cf7
SK.CMS.AES256.MAC = ff84dadfee1e160bf9d6c3ae00967dda6ee534de9e5c5e7bfb279d9a130ebf6
SK.VSD.AES256.ENC = f4edba04e3253e6c008ddb72af08b4fef9be68f8512b03ffadcb9ace7563e0f0
SK.VSD.AES256.MAC = d9d921537b0c8507a8444e5e9e0ae694287343acb81304bc628ba6abb6a1a4e
```

ICCSN = 80276881031971421010

```
SK.CMS.AES128.ENC = d4dd0f4966ce13b1c8a91be4b17972f4
SK.CMS.AES128.MAC = 7c5dcbd4ed461c85ed4ac54b92c7f821
SK.VSD.AES128.ENC = 24a379c27c6a93a27d2095d2d8cfaf72
SK.VSD.AES128.MAC = fa4bcc22476ac5f287213fffc9a80ee5
SK.CMS.AES256.ENC = 59d0c921aeab21782587a68d90b355b71a9f651405b07878bb216aaf7ff5d580
SK.CMS.AES256.MAC = 175b09ee81b44315cf6b85eae14a94a8e22cc74ce06a251363150d8a0dd1efe7
SK.VSD.AES256.ENC = 8f533c6371dda6f957959b1b01dd8d549e5fe8c386722584fe800b57e6a208d3
SK.VSD.AES256.MAC = fb90558adc407b1fc545380b38d71023532cd520f518af186c59cbc9fd97e62f
```

ICCSN = 80276881190000003706

```
SK.CMS.AES128.ENC = 7ca08936b5e10527ed1a7aa49f931f02
SK.CMS.AES128.MAC = fd82005e7ebd041a24b285d295ee9f30
SK.VSD.AES128.ENC = bc87adf84bdbda62b18614bfe6fcb1c2
SK.VSD.AES128.MAC = e21cf109ae2f85fc2a465dab622a2ad5
SK.CMS.AES256.ENC = 96b1c02977e8bb949bdf5b9bb33633c63dc34e9735dcd1090b650c9d044a8468
SK.CMS.AES256.MAC = fcffa3067491771bb5b6b8bd7de090e4855e2cb2dccfc5020b519e1d79af02e3
SK.VSD.AES256.ENC = ac7128316159603bac3f999dc9d7b6dc51d3f035f6439dcb18db3f750ed702ca
SK.VSD.AES256.MAC = 404e0ca76dcfa92dabb563ea23f57eff5195872dd0f13385164c8113ad5b1906
```

ICCSN = 80276881190000003723

```
SK.CMS.AES128.ENC = 84f2c37eb9a894a7ee716971dc95511a
SK.CMS.AES128.MAC = 564d02f053d1a181862aaa614f51608e
SK.VSD.AES128.ENC = 10d2308e9dffa822402c48aa3a594083
SK.VSD.AES128.MAC = 00b4ebf8307dff695530d9f3dce10dbe
SK.CMS.AES256.ENC = 7872010703e6d523be2aa9cddb629685a266e1c54ec6dbb63bed4a3f97240065
SK.CMS.AES256.MAC = 8f82e9b4901c4a7b2d7c731459b6940c0f8e729420a5046479a726861ffe3cb5
SK.VSD.AES256.ENC = 778c16d9e74780829574cc016aaa24a82c87cae6c327be5b5211c07e2eae4acf
SK.VSD.AES256.MAC = b91f79fd0787c5457a4d5efd22e3df897d7a8d8b01d827d1a020927ab1898539
```

ICCSN = 80276881500000001416

```
SK.CMS.AES128.ENC = 5bedab2f527a2adb65ed458686554c36
SK.CMS.AES128.MAC = de996c091f5d6f25e9b76b411611d15a
SK.VSD.AES128.ENC = 0495f3524ae773910b71a16e99b3a04f
SK.VSD.AES128.MAC = d446f73fb3aad1b4cd885ac02c5f0eac
SK.CMS.AES256.ENC = e1f1a979c65a141c7cca549304272b99a2bd32a615c2a3c3a50c6430cad1829f
SK.CMS.AES256.MAC = 8cb848323d16293de405b8b4fc7d7e1353936ec5c782f6c2a876c65aae7c8575
SK.VSD.AES256.ENC = 4c3d3cf423506bd47aadbe000b513eb8e62da345a275cb54e251d036898ca54a
SK.VSD.AES256.MAC = ff21f6762314a62020f178b43906382fc817f05df4d03e30db1d946d556a1468
```

12.2 Testvektoren für Schlüsselableitung Variante 2: Atos

Dieser Abschnitt enthält Testvektoren für die Schlüsselableitung gemäß A 24100. Die Angaben sind informativ und ohne Gewähr.

ICCSN = 80276001040000000001

SK.CMS.AES128.ENC	=	83b71ca85a0f940fd154409ac67ae0db
SK.CMS.AES128.MAC	=	fa65036cc682e440903a9ba7f90e0f2c
SK.VSD.AES128.ENC	=	47e68b915481a7a6b772d58ab55cc48c
SK.VSD.AES128.MAC	=	f602f5c2f838b8230f0b623131b9a35b
SK.CMS.AES256.ENC	=	fa9e833e3584f7b2f27f08e2e9c4b72d4112b78a4236af799adf6a25584a1848
SK.CMS.AES256.MAC	=	ff9690c39521dd9bc7dd8d8b33b741a8888bde8fa8def8dca840079ff646aae8
SK.VSD.AES256.ENC	=	c82de2d3878f8257c452f0e355a1212e2d5a3f4f96cbc4503885d3cf593c9018
SK.VSD.AES256.MAC	=	1f3901dd3274fc85822853276d369ba408b5afee6fa2804fe42115ef0c314804

ICCSN = 80276881040000000001

SK.CMS.AES128.ENC	=	abbc22c5ffbf6c6eff5280e361f04787f
SK.CMS.AES128.MAC	=	e8383de2e13b258ae00e3dd3310193e3
SK.VSD.AES128.ENC	=	e5b29e78518a773500d8162df95d00cd
SK.VSD.AES128.MAC	=	0768809344eadfa795d40ad5f19578fe
SK.CMS.AES256.ENC	=	ade61aa4d28b52a68ff7436d15b1af8b53284653a2924c9ad48b8642f6c5e1c2
SK.CMS.AES256.MAC	=	40421e7e8735ae5e72923668901020dbee3632bfd228faf2594504145096e067
SK.VSD.AES256.ENC	=	bc98c4b7671a6a1c9aad10636b66257f6226e1f7a6bab9dcc772aa5edb039b12
SK.VSD.AES256.MAC	=	cefe1d240f29fda5b7036ff6dd70d0d8cab562ab8e9fa1e2e0927978d48713a3

12.3 Testvektoren für Schlüsselableitung Variante 3: G&D

Dieser Abschnitt enthält Testvektoren für die Schlüsselableitung gemäß A 24101. Die Angaben sind informativ und ohne Gewähr.

ICCSN = 80276881040000000001

SK.CMS.AES128.ENC	=	3da50518af5497266ebb27b5b787ee20
SK.CMS.AES128.MAC	=	cfbd857414520cfbf6afd61133cb6e2d
SK.VSD.AES128.ENC	=	3efb91375510c0b86026b742c8b5b7a8
SK.VSD.AES128.MAC	=	abf6746469ffb322b1b00d8c0afde0aa
SK.CMS.AES256.ENC	=	3da50518af5497266ebb27b5b787ee209b8c2408d729f76167d592fb8cb9be8b
SK.CMS.AES256.MAC	=	cfbd857414520cfbf6afd61133cb6e2df04a82de411d45597d32e33ab20d7111
SK.VSD.AES256.ENC	=	3efb91375510c0b86026b742c8b5b7a843c103a48f51519be86b71c99b6d832a
SK.VSD.AES256.MAC	=	abf6746469ffb322b1b00d8c0afde0aa4619842a38a2f8637df9a66927ad8b56