gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation der Testlaborkarte COS / Objektsysteme

Version:	1.5.0
Revision:	\main\rel_ors1\17
Stand:	29.08.2014
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemSpec_TLK_COS_G2]

Dokumentinformationen

Änderungen zur Version1.4.0

Einarbeitung der Fehlerkorrekturen zu Iteration 4:

Kapitel 2.2.5: Klarstellung zum Inhalt von EF.ATR

Kapitel 3.2 Knoten <cos_performancetest> aufgenommen

Kapitel 3.2.3: Klarstellungen zu Kartentyp-Objektsystemen in der TLK-Template-Datei

Kapitel 4.3: Ergänzt um einen Hinweis zu den Lade-Images (d3.-Files)

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.1	18.01.13		Ersterstellung	TST/KS, Karten
0.1.0	30.01.13		Berücksichtigung der Review-Kommentare	TST/KS, Karten
1.0.0_RC	31.01.13		zur Freigabe empfohlen	gematik
1.0.1	15.08.13		Anpassungen an die neue gemSpec_COS Version und weitere neue Erkenntnisse	TST/DP Karten
1.0.2	02.10.13		Einarbeitung weiterer Kommentare	TST/DP Karten
1.1.0	23.10.13		freigegeben	gematik
	09.12.13		Integration der TLK Objektsysteme für die Kartenprodukttypen	TST/DP Karten
	16.12.13		Berücksichtigung der Review-Kommentare	TST/DP Karten
1.2.0_RC	18.12.13		zur Freigabe empfohlen	gematik
	10.02.14		Klarstellungen, neues Image zum Test PACE-PCD	TST/DP Karten
1.3.0	21.02.14		freigegeben	gematik
1.3.1	23.04.14		Einarbeitung Fehlerkorrektur und neuer Anforderungen	TST/DP Karten
1.4.0	06.06.14		freigegeben	gematik
1.4.1	22.08.14		Klarstellungen, Hinweise und Ergänzungen (Cache-Image)	TST/DP Karten
1.5.0	29.08.14		freigegeben	gematik

Inhaltsverzeichnis

Dokumentinformationen **2**

Inhaltsverzeichnis **3**

1 Einordnung des Dokuments **5**

1.1 Zielsetzung **5**
1.1.1 Card Operating System (COS) 5
1.1.2 Kartentyp-Objektsysteme 5
1.1.3 Unterstützung durch die gematik 6

1.2 Zielgruppe **6**

1.3 Geltungsbereich **6**

1.4 Abgrenzungen **6**

1.5 Methodik **7**

2 Grundlegende Anforderungen **8**

2.1 Äußere Gestaltung der Testlaborkarte **8**

2.2 Attribute des Objektsystems **9**
2.2.1 Zugriffsregeln für besondere Kommandos 9
2.2.2 Answer To Reset 10
2.2.3 ICCSN 10
2.2.4 PublicKeyList 11
2.2.5 EF.ATR Inhalt (body) 11

2.3 Optionen **11**
2.3.1 COS-Optionen 11
2.3.2 Kartentyp-Objektsystem-Optionen 12

3 Testlabordateien **13**

3.1 Objektsysteme der Testlaborkarte **13**

3.2 Template-Datei **14**
3.2.1 Template <card_capabilities> 15
3.2.2 Template <cos_unterbrechungstest>, <load_application>, <cos_performancetest>, <cos_test> 16
3.2.3 Template <kartentyp_objektsysteme> 17

4 Initialisierungsdateien **18**

4.1 Übersicht der Image-Files (d3-Files) **18**
4.1.1 COS-Image-Files (d3-Files) 18
4.1.2 Kartentyp-Objektsystem Image-Files (d3-Files) 19

4.2 d3-File Name **20**

4.3 Aufbau und Struktur eines Image-Files **20**

Anhang A **22**

A1 – Abkürzungen **22**

A2 - Glossar **23**

A3 - Abbildungsverzeichnis **23**

A4 - Tabellenverzeichnis **23**

A5 - Referenzierte Dokumente **23**

A5.1 – Dokumente der gematik 23

A5.2 – Weitere Dokumente 25

1 Einordnung des Dokuments

1.1 Zielsetzung

Dieses Dokument enthält Informationen für Hersteller, die ihr Betriebssystem bzw. ihr Kartentyp-Objektsystem dem funktionalen Eignungs- bzw. Zulassungstest durch die gematik unterziehen lassen möchten, hinsichtlich:

- der Objektsysteme der Testlaborkarten, die dem Hersteller in Form von XML-Dateien von der gematik zur Verfügung gestellt werden,
- der Image-Files, ladefähige d3-Files, die der Hersteller, auf der Basis der XML-Dateien (COS), bzw. der Kartentyp-Objektsysteme (eGK, HBA, SMC-B, gSMC-K und gSMC-KT) zu erstellen hat,
- sowie zur äußeren Gestaltung der Testlaborkarten.

1.1.1 Card Operating System (COS)

Gemäß dem Zulassungsverfahren für Kartenbetriebssysteme [gemZul_ProdCOS] hat die gematik die funktionale Eignung der Betriebssysteme (Card Operating System, kurz COS) für Chipkarten in der TI des deutschen Gesundheitswesens sicherzustellen.

Als funktional geeignet wird ein Betriebssystem dann angesehen, wenn sich das COS entsprechend der funktional ausgerichteten Betriebssystem-Spezifikation [gemSpec_COS] verhält.

Die Prüfung des Betriebssystems, die ausgerichtet ist an der Betriebssystem-Spezifikation, ist nur in Verbindung mit mehreren speziellen Objektsystemen, den Testlaborkarten-Objektsystemen inklusive Attributen und Inhalten möglich.

1.1.2 Kartentyp-Objektsysteme

Gemäß den Zulassungsverfahren für die Kartentyp-Objektsysteme (siehe Kapitel A5.1 [gemZul_Prodxxx]), hat die gematik die funktionale Eignung der Anwendungen des jeweiligen Kartentyp-Objektsystems der Chipkarten in der TI des deutschen Gesundheitswesens sicherzustellen.

Als funktional geeignet wird ein Kartentyp-Objektsystem dann angesehen, wenn das Kartentyp-Objektsystem entsprechend der jeweils relevanten Spezifikation (siehe Kapitel A5.1 [gemSpec_xxx_ObjSys]) realisiert wurde.

1.1.3 Unterstützung durch die gematik

Die gematik unterstützt Hersteller/Antragssteller (im Sinne von [gemZul_ProdCOS] bzw. [gemZul_Prodxxx]), im weiteren Verlauf des Dokuments Hersteller genannt, nach der Antragstellung auf Zulassung eines COS bzw. eines Kartentyp-Objektsystems für G2-Karten mit weitreichenden Vorgaben zur Erstellung der benötigten ladefähigen Image-Files, die die Objektsysteme für die Testlaborkarte widerspiegeln.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller, die ihr Chipkarten-Betriebssystem (COS) bzw. ihr Kartentyp-Objektsystem der Generation 2 für die TI des deutschen Gesundheitswesens einem funktionalem Eignungstest unterziehen lassen möchten.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zu den Objektsystemen, die für den funktionalen Eignungstest des COS bzw. der Kartentyp-Objektsysteme benötigt werden. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekanntgegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation 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 Spezifikation 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 Abgrenzungen

Dieses Dokument legt den Fokus auf die Unterstützung des COS-Herstellers bzw. des Kartentyp-Objektsystem-Herstellers durch die gematik. Der Hersteller wird in die Lage versetzt seiner Mitwirkungspflicht im Rahmen des funktionalen Eignungstests optimal nachkommen zu können.

Nicht Gegenstand dieses Dokumentes sind die Basiskommandos, die Grundfunktionen des Betriebssystems sowie die grundlegenden Sicherheitsfunktionen und -algorithmen für Karten des Gesundheitswesens. Diese werden in der Spezifikation des Card Operating System (COS) [gemSpec_COS] detailliert beschrieben.

Nicht Gegenstand dieses Dokumentes sind die Anwendungen, Objekte und Zugriffsregeln des jeweiligen Kartentyp-Objektsystems. Diese können der jeweiligen Kartentyp-Objektsystem-Spezifikation ([gemSpec_xxx_ObjSys]) entnommen werden.

Nicht Gegenstand dieses Dokumentes sind Optik, Struktur und Inhalt der Testkarten, diese sind Inhalt der Spezifikation Testkarten [gemSpec_TK].

Nicht Gegenstand dieses Dokumentes ist die Personalisierungsvalidierung. Diese wird in eigenständigen Dokumenten spezifiziert.

1.5 Methodik

1.5.1 Verwendung von Referenzen und Abkürzungen

Referenzen auf weitere Dokumente und Standards sind in [eckige Klammern] gesetzt und werden im Anhang aufgelöst. Abkürzungen werden bei ihrer ersten Verwendung in (Klammern) gesetzt und im Abkürzungsverzeichnis aufgelöst.

1.5.2 Verwendung von Schlüsselworten

Anforderungen als Ausdruck normativer Festlegungen werden durch die in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN, entsprechend [RFC2119], gekennzeichnet.

Abwandlungen von „MUSS“ zu „MÜSSEN“ etc. sind der Grammatik geschuldet. Da im Beispielsatz „*Eine leere Liste DARF NICHT ein Element besitzen*.“ die Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „*Eine leere Liste DARF KEIN Element besitzen*.“ verwendet.

2 Grundlegende Anforderungen

Grundlegende Anforderungen, an die Zulassung des Kartenbetriebsystems, können u. a. dem Dokument Zulassungsverfahren COS [gemZul_ProdCOS] entnommen werden.

2.1 Äußere Gestaltung der Testlaborkarte

Auf die Oberfläche der Testlaborkarte MÜSSEN

- der Schriftzug „Testlaborkarte G2“,
- der Name des Herstellers oder Antragsstellers,
- das Produktkürzel des Kartenbetriebsystems,
- die Produktversion des Kartenbetriebsystems,
- das Erstellungsdatum und
- der von der gematik vergebene Zulassungsschlüssel (COS Zulassung)

aufgedruckt werden.

Die Beschriftung SOLL

- der folgenden Abbildung 1,
- der Schriftart Verdana True Type und
- dem Schriftgrad 10 pt entsprechen.

Wegen der geringen Ansprüche an das Layout der Testlaborkarte wird auf eine Bemaßung verzichtet.

Der Produktname MUSS vom Hersteller bestimmt werden.

Die Produktversion MUSS vom Hersteller bestimmt werden und MUSS den Vorgaben des Dokuments [gemSpec_OM] entsprechen.

Der Hersteller MUSS bei zu unterschiedlichen Zeitpunkten eingereichten Testlaborkarten gleicher Version ein unterscheidbares Erstellungsdatum aufbringen.

Den Zulassungsschlüssel erhält der Hersteller nach Eingang des Zulassungsantrags von der Zulassungsstelle der gematik. Sie erlaubt die eindeutige Zuordnung der Karte zu einem funktionalen Zulassungsprozess.

Wird die „Unterstützung der USB-Schnittstelle“ (Opt-1) im Antrag auf funktionale Zulassung gewählt, dann muss der Hersteller 5 Adapter inklusive USB Device Descriptor zur Verfügung stellen. Nach dem funktionalen Eignungstest werden die Gegenstände aus Revisionsgründen bei der gematik archiviert. Weitere Informationen zur Archivierung sind dem Dokument [gemZul_ProdCOS] zu entnehmen.

Optional KANN zusätzlich das Logo des Herstellers aufgebracht werden.

Die Gestaltung der Kartenrückseite KANN der Hersteller bestimmen.

Die im Zuge der für den funktionalen Eignungstest eines COS vom Hersteller zur Verfügung gestellten Testlaborkarten verbleiben bei der gematik. Ein Teil der Testlaborkarten wird archiviert. Die restlichen Testlaborkarten werden im Rahmen eventuell nachfolgender Eignungstests kartentypspezifischer Objektsysteme (z. B. eGK) verwendet.

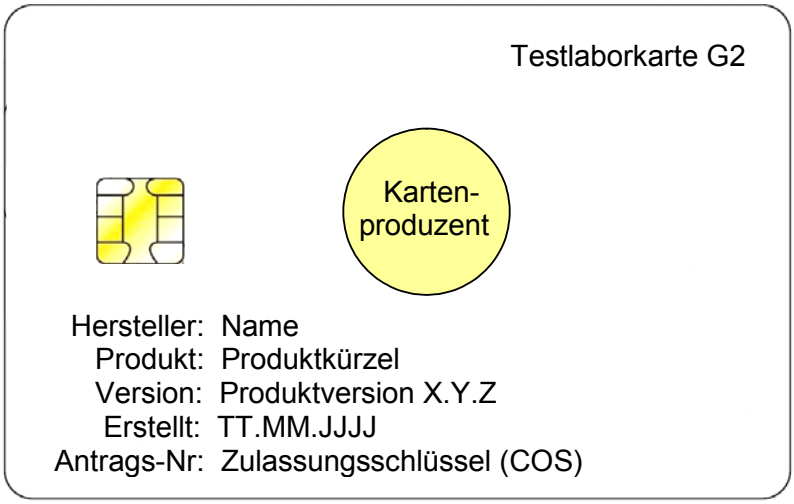

Abbildung 1: Layout der Testlaborkarte der Generation 2

Hinweis: Im Antrag auf Zulassung eines Kartentyp-Objektsystems ist als Referenz der Zulassungsschlüssel eines bereits zugelassenen Kartenbetriebssystems (COS) anzugeben.

2.2 Attribute des Objektsystems

Das Objektsystem mit seinen Attributen MUSS grundsätzlich den Vorgaben aus [gemTLK_COS-Dat] bzw. [gemSpec_xxx_ObjSys] entsprechen. Die folgenden Unterkapitel enthalten weitergehende Vorgaben.

2.2.1 Zugriffsregeln für besondere Kommandos

Für Kommandos, für die eine Zugriffsregelauswertung gemäß [gemSpec_COS] optional ist, werden nicht in den Image-Files, sondern nachfolgend festgelegt:

- Für die kontaktbehaftete Schnittstelle MUSS die Zugriffsbedingung für die Kommandos GET CHALLENGE, LIST PUBLIC KEY, MANAGE SECURITY ENVIRONMENT und SELECT stets ALWAYS sein.

- Falls ein Kartentyp die Option_kontaktlose_Schnittstelle unterstützt, dann MUSS die Zugriffsbedingung für die Kommandos GET CHALLENGE, LIST PUBLIC KEY, MANAGE SECURITY ENVIRONMENT und SELECT stets ALWAYS sein.

- Falls ein Kartenherausgeber die Nutzung einer im COS vorhandenen kontaktlosen Schnittstelle unterbinden will, dann MUSS die Zugriffsbedingung für die Kommandos GET CHALLENGE, LIST PUBLIC KEY, MANAGE SECURITY ENVIRONMENT und SELECT für die kontaktlose Schnittstelle herstellerspezifisch stets entweder ALWAYS oder NEVER sein.

2.2.2 Answer To Reset

Die Attribut *answerToReset* (coldAnswerToReset und warmAnswerToReset) MUSS die in Tab_TLK_ObjSys_001 dargestellten Werte besitzen.

Tabelle 1: Tab_TLK_ObjSys_001 – ATR-Codierung

Zeichen	Wert	Bedeutung
TS	´3B´	Initial Character (direct convention)
T0	´9x´	Format Character (TA1/TD1 indication, x = no. of HB)
TA1	´xx´	Interface Character (FI/DI, erlaubte Werte: siehe [gemSpec_COS])
TD1	´81´	Interface Character, (T=1, TD2 indication)
TD2	´B1´	Interface Character, (T=1, TA3/TB3/TD3 indication)
TA3	´FE´	Interface Character (IFSC coding)
TB3	´45´	Interface Character, (BWI/CWI coding)
TD3	´1F´	Interface Character, (T=15, TA4 indication)
TA4	´xx´	Interface Character (XI/UI coding)
Ti	HB	Historical Bytes (HB, imax. = 15)
TCK	XOR	Check Character (exclusive OR)

Der ATR SOLL ein TC1 Byte mit dem Wert ´FF´ enthalten. In diesem Fall MUSS T0 auf den Wert ´Dx´ gesetzt werden.

Das Attribut *answerToReset* SOLL keine Historical Bytes enthalten.

Falls *answerToReset* Historical Bytes enthält, dann MÜSSEN

- diese gemäß [ISO7816-4] kodiert sein,

- die dort getroffenen Angaben konsistent zu den Angaben im EF.ATR sein.

2.2.3 ICCSN

Die ICCSN8 MUSS identisch zu den letzten acht Oktetten im *body* von EF_GDO sein.

Die ICCSN MUSS über alle Testlaborkarten und in allen Image-Files (siehe Kapitel 3) einer Lieferung denselben Wert besitzen.

2.2.4 PublicKeyList

Für die funktionale Prüfung des COS werden öffentliche Schlüssel vorgegeben, die der Liste *applicationPublicKeyList* ([gemSpec_COS]#N019.900.d) zuzuführen sind. Die relevanten Schlüssel sind dem jeweiligen Image-File [gemTLK_COS-Dat], identifizierbar über <attribute id="applicationPublicKeyList">.

Hinweis: Aus Kompatibilitätsgründen besitzt das Attribut zurzeit die Kennung <..id="persistentPublicKeyList">.

Weitere Tests im Rahmen der funktionalen Prüfung des COS betreffen die Listenelemente in *persistentCache*. Die Spezifikation [gemSpec_COS] fordert gemäß der Anforderung N019.900.e.2 das die Objektsystem-Spezifikation eine Begrenzung der Listenelemente vorschreiben soll.

Die Anzahl der Listenelemente hängt u. a. von der Anzahl logischer Kanäle ab die das COS gemäß „Antrag auf Zulassung … COS G2" unterstützen soll. Die entsprechende Formel lautet „(Basiskanal + Anzahl logischer Kanäle) * 2 + 1 + ReserveElemente".

Die Anzahl der Reserveelemente kann den jeweiligen Image-Files [gemTLK_COS-Dat], <attribute id="reservedPersistentCacheSlots"> entnommen werden.

2.2.5 EF.ATR Inhalt (body)

Der Inhalt des Attributes „body" im EF.ATR muss in allen Initialisierungsdateien (d3-Files) gemäß [gemSpec_Karten_Fach_TIP] umgesetzt werden.

2.3 Optionen

Die COS-Spezifikation wie auch die Kartentyp-Objektsystem-Spezifikationen kennen Optionen. Es handelt sich dabei um über die Basisfunktionalität hinausgehende Funktionen die der Hersteller realisieren kann.

2.3.1 COS-Optionen

Die COS-Spezifikation [gemSpec_COS] kennt fünf Funktionspakete, die das Betriebssystem erweitern und ein Hersteller optional realisieren kann. Es handelt sich um die:

- Option USB-Schnittstelle (Opt-1),
- Option kontaktlose Schnittstelle (Opt-2),
- Option (mehrere) logische Kanäle (Opt-3),
- Option Kryptobox (Opt-4),

- Option PACE PCD (Opt-5).

Die Optionen „kontaktlose Schnittstelle“, „Kryptobox“ und „PACE PCD“ benötigen spezielle Objektsysteme in der Testlaborkarte.

Wünscht ein Hersteller eine um Optionen ergänzte Zulassung und handelt es sich um eine der zuvor genannten drei Optionen, dann erhält er von der gematik, auf die jeweilige Option bezogen, ergänzende Image-Files zur Erstellung der Objektsysteme.

2.3.2 Kartentyp-Objektsystem-Optionen

Die Kartentyp-Objektsystem-Optionen können der jeweiligen Objektsystem-Spezifikation [gemSpec_xxx_ObjSys] entnommen werden.

Die Auswirkungen der Optionen auf das Objektsystem des jeweiligen Kartentyps sind ebenfalls in der Objektsystem-Spezifikation beschrieben und müssen, bei gewollter Realisierung, auch bei der Erstellung des Objektsystems für die Testlaborkarte Berücksichtigung finden.

3 Testlabordateien

Die gematik stellt Herstellern Dateien zur Verfügung, die die Basis für den Mitwirkungsprozess des Herstellers darstellen. Es handelt sich um

- COS
  mehrere Dateien (XML-Format) die jeweils ein Objektsystem beinhalten, als Vorlage für die Erstellung der für den funktionalen Eignungstest notwendigen, ladefähigen Image-Files (d3-Files),

- Kartentyp-Objektsysteme
  die für den funktionalen Eignungstest zu erstellenden notwendigen, ladefähigen Image-Files (d3-Files) MÜSSEN auf den jeweiligen Kartentyp-Objektsystem-Spezifikationen [gemSpec_xxx_ObjSys] basieren,

- eine Template-Datei (XML-Format), in die herstellerspezifische Informationen einzutragen sind.

Zur Durchführung der umfangreichen funktionalen Tests macht die gematik Vorgaben hinsichtlich Struktur, Attribute und Inhalt der Testlaborkarten-Objektsysteme. In einem dem funktionalen Eignungstest vorgeschalteten Eingangstest wird die Einhaltung der Vorgaben geprüft.

Die Objektsystemdateien wie auch die Template-Datei können Werte, die als [herstellerspezifisch] gekennzeichnet sind, enthalten. Diese Platzhalter MÜSSEN in den zu erstellenden ladefähigen Image-Files bzw. in der Template-Datei mit Werten des Herstellers gefüllt werden.

Die Namen der ladefähigen Image-File-Dateien (d3-Files) MÜSSEN denen in der Tabelle 3 (COS) bzw. der Tabelle 4 (Kartentyp-Objektsystem) entsprechen.

Die Bestandteile <zls> und <datum> im Dateinamen der Template-Datei MÜSSEN vom Hersteller entsprechend der Tabelle 5 modifiziert werden.

3.1 Objektsysteme der Testlaborkarte

Die Objektsystemdateien, zusammengefasst unter [gemTLK_COS-Dat] bzw. [gemSpec_xxx_ObjSys], enthalten Objektsysteme und Inhalte, die auf die erstellten Testsuiten der Testplattform abgestimmt sind.

Diese Vorgaben der gematik stellen für den Hersteller die Grundlage zur Erstellung der Image-Files (d3 Files), siehe Kapitel 4, dar.

Für jedes Objekt- bzw. Prüfgebiet existiert je eine Objektsystemdatei mit exakten Vorgaben zur Erstellung des ladefähigen Image-Files.

Für als „herstellerspezifisch“ deklarierte Variablen sind keine direkten Vorgaben seitens der gematik gegeben. Es können sich jedoch an anderer Stelle spezifizierte Werte auf herstellerspezifische Variablen auswirken. Unter Berücksichtigung dieses Effekts MUSS der Hersteller diese Werte festlegen.

Die Objektsystemdateien, zusammengefasst unter [gemTLK_COS-Dat] werden von der gematik nicht zurück erwartet.

3.2 Template-Datei

Die Datei [gemTLK_COS-Tpl] enthält von der gematik zur Verfügung gestellte Rahmeninformationen, die vom Hersteller zu ergänzen, zu modifizieren oder zu selektieren sind.

Die Datei ist in fünf Hauptknoten unterteilt:

- Knoten <card_capabilities>
  Karten- und herstellerspezifische Eigenschaften z. B. die Bezeichnung der Image-Files (d3-Files), Angaben zum EF_ATR.

- Knoten <cos_unterbrechungstest>
  Benötigte APDU-Sequenzen zum Anlegen unterschiedlicher Objekte, die für den Test des Roll-Verhaltens (siehe [gemSpec_COS]) benötigt werden.

- Knoten <cos_performancetest>
  Benötigte APDU-Sequenzen zum Anlegen der Anwendung DF_LCS, die für den Leistungstest benötigt werden. Die Anwendung DF_LCS kann [gemSpec_COS] entnommen werden.

- Knoten <load_application>
  Benötigte APDU-Sequenzen zum Anlegen unterschiedlicher Objekte per LOAD APPLICATION sind hier zu hinterlegen.

- Knoten <cos_test>
  Die hier einzutragenden APDU-Sequenzen werden u. a. für Tests mit Files übergroßer Länge verwendet.

- Knoten <kartentyp_objektsysteme>
  Der funktionale Eignungstest der Kartentyp-Objektsysteme erfordert abgestimmte Werte für einige Objekte/Attribute, die in die ladefähigen Image-Files einfließen müssen.
  a. Die gematik gibt Werte vor, die vom Hersteller übernommen werden müssen.
  b. Herstellerspezifische Werte sind an den vorgegebenen Stellen vom Hersteller der Objektsysteme einzutragen.

In den nachfolgenden Tabellen werden nur die Elemente/Attribute beschrieben, die vom Hersteller in der Template-Datei zu modifizieren oder zu ergänzen sind.

Die Template-Datei, mit den modifizierten Einträgen, MUSS an die gematik zurück gesandt werden.

3.2.1 Template <card_capabilities>

Die Angaben in diesem Knoten sind mit größter Sorgfalt zu erstellen, da z. B. der Test aufgrund nicht gefundener Image-Files nicht durchgeführt oder auf eine falsche Ausprägung hin getestet werden könnte. Dies führt zu Fehlern und kann zu einer negativen Beurteilung der funktionalen Eignung führen.

In der folgenden Tabelle sind die Hauptelemente und ihre Funktionen erklärt. Die Tabelle dient als Orientierungshilfe. Weitere Hinweise zu den Elementen finden sich in [gemTLK_COS-Tpl].

Tabelle 2: Tab_TLK_ObjSys_002 – Template <card_capabilities>

Element / Attribut	Attribut	Wert
<Image-Files_COS> Name der für den Zulassungstest notwendigen d3-Files. Nur relevant für den funktionalen Eignungstest des Kartenbetriebssystems.	<COS_accessSe> bis <COS_performC>	TLK_<zls>_<objekt- bzw. pruefgebiet>_<datum>.d3 (siehe Tabelle 3)
	<COS_kontaktlos128> bis <COS_kontaktlos256> Nur wenn Opt-2 kontaktlose Schnittstelle unterstützt wird.	TLK_<zls>_<objekt- bzw. pruefgebiet>_<datum>.d3 (siehe Tabelle 3)
	<COS_kryptobox> und <COS_searchKrypto box> Nur wenn Opt-4 Kryptobox unterstützt wird.	TLK_<zls>_<objekt- bzw. pruefgebiet>_<datum>.d3 (siehe Tabelle 3)
	<COS_pace_pcd> Nur wenn Opt-5 PACE-PCD unterstützt wird.	TLK_<zls>_<objekt- bzw. pruefgebiet>_<datum>.d3 (siehe Tabelle 3
<Image-Files_CardObjSys> Nur relevant für den funktionalen Eignungstest des jeweiligen Kartentyp-Objektsystems.		TLK_<zls>_<kartentyp>_<datum >.d3 (siehe [gemTLK_COS-Tpl]
<preissuing_data> Über diesen Eintrag ist eindeutig die Karte identifizierbar. Es handelt sich um das Pre-Issuing Data Object im ATR / Historical Bytes und den Daten des TAG '66'/'46' des EF.ATR. Die hier einzutragenden Werte sind hexadezimal zu kodieren.	<icm>	Angabe der IC-Herstellerkennung
	<ict>	Angabe des IC-Typ
	<osv>	Angabe zur Operation System Version
	<dd>	Discretionary Data
	<iccm>	Kartenherstellerkennung
<buffer_size>	<req_apdu_ohne_sm>	maximale Länge einer ungesicherten Kommando-APDU

Element / Attribut	Attribut	Wert
Die Angaben zu den max. APDU-Längen müssen mit denen im EF.ATR TAG 'E0' identisch sein. Die Längen sind hexadezimal zu kodieren	<resp_apdu_ohne_sm>	maximale Länge einer ungesicherten Antwort-APDU
	<req_apdu_mit_sm>	maximale Länge einer Kommando-APDU mit Secure Messaging
	<resp_apdu_mit_sm>	maximale Länge einer Antwort-APDU mit Secure Messaging

Hinweis: Es werden nur die Image-Files (d3-Files) des Produkttyps (COS, Kartentyp-Objektsystem) benötigt, für die ein Antrag auf Zulassung gestellt wurde.

3.2.2 Template <cos_unterbrechungstest>, <load_application>, <cos_performancetest>, <cos_test>

Dieses Kapitel ist nur für den funktionalen Eignungstest eines COS relevant.

Die diesem Knoten zugeordneten Objekte, Elementary Files unterschiedlicher Ausprägung und kompletter Applikation, dienen der Prüfung:

- des Roll-Verhaltens im Falle eines Spannungsabfalls,
- des Kommandos LOAD APPLICATION [gemSpec_COS],
- des Kommandos LOAD APPLICATION im Rahmen des Leistungstests,
- der geforderten Funktionalität „Defragmentierung“ [gemSpec_COS] und
- der Use Cases (Kartentyp-Objektsystem).

Der erste Teil dieses Knotens enthält transparente und strukturierte Elementary Files unterschiedlicher Ausprägung.

Zu jedem dieser EFs MUSS eine APDU oder eine APDU-Sequenz angelegt werden. Diese muss an vorgegebener Stelle auf das Kommando LOAD APPLICATION abgestimmt werden. Zu codieren sind die Nettodaten (ohne Berücksichtigung eines möglichen, vom Basiskanal abweichenden Kanals und ohne Berücksichtigung eines möglichen Secure-Messaging).

Dabei sind ggf. einige Value-Felder der TLV-DOs für die Attribute “applicationIdentifier“, "fileIdentifier", "shortFileIdentifier", "numberOfOctet", "positionLogicalEndOfFile", "maximumNumberOfRecords" und "maximumRecordLength" durch Platzhalter [AID: x..x], [FID: x...x], [SFID: xx], [SIZE: x..x], [LEOF: x..x]“ ", "[MAXREC: xx]", "[RECLEN: xx]" zu ersetzen. Die Darstellung erfolgt Hexadezimal.

Weitergehende Informationen können den Objektsystemdateien [gemTLK_COS-Tpl] entnommen werden.

Unterstützt das COS die Option „kontaktlose Schnittstelle“ MUSS die APDU-Sequenz, wenn vorgegeben, neben den Attributen accessRules für den kontaktbehafteten Zugriff

(Kennung: CB) auch die accessRules für den kontaktlosen Zugriff (Kennung: CL) enthalten.

3.2.3 Template <kartentyp_objektsysteme>

Dieses Kapitel ist nur für den funktionalen Eignungstest eines Kartentyp-Objektsystems relevant.

Für jeden Kartentyp ist mindestens ein Sub-Knoten vorhanden. Unterschiedliche Ausprägungen einer Karte, beispielsweise bei der SMC-B, können zu mehreren Sub-Knoten führen.

Für einen optimalen Ablauf des funktionalen Eignungstests eines Objektsystems sind Attributwerte zwischen der gematik und dem jeweiligen Hersteller einer eGK oder anderen Kartentypen abzustimmen.

Unter jedem Sub-Knoten (Kartentyp-Knoten) sind nur die Objekt Attribute aufgelistet, die

- der Identifikation des Objekts dienen,
- die herstellerspezifisch zu ergänzen sind.

Der Einfachheit halber gibt die gematik nicht verbindliche Werte vor. Diese können für die Erstellung eines ladefähigen Images (d3-File) genutzt werden. Sollten für das d3-File abweichende Werte verwendet werden, müssen diese in dieser Template-Datei an entsprechender Stelle eingetragen werden.

4 Initialisierungsdateien

Für die Durchführung der Tests ist es zwingend notwendig, dass die Testlaborkarten re-initialisiert werden können, da einige Testscripte die Kartenstruktur bzw. Dateninhalte z. B. im Fehlerfall irreversibel ändert. In einem solchen Fall muss das Testsystem in die Lage versetzt werden, die Testlaborkarte wieder in ihren Ursprungszustand bringen zu können.

Die Durchführung einer Reinitialisierung erfolgt durch Ausführung einer vom Hersteller bereitzustellenden Liste von APDUs, die in einer Textdatei (mit der Endung .d3), den Image-Files, abgelegt werden müssen. Nach der Ausführung dieser Kommandosequenz muss sich das Objektsystem wieder im Ausgangszustand befinden.

Sollten vom Hersteller Kommandos für die Reinitialisierung benutzt werden, die Rechte einfordern, die in den zur Verfügung gestellten Objektsystemen für das COS [gemTLK_COS-Dat] bzw. den Kartentyp Objektsystemspezifikationen [gemSpec_xxx_ObjSys] nicht enthalten sind, so muss der Hersteller die d3-Files um diese zusätzlich benötigten Rechte für den funktionalen Eignungstest des COS und der Kartentyp Objektsysteme, typischer Weise im MF, ergänzen.

4.1 Übersicht der Image-Files (d3-Files)

Die d3-Files enthalten je ein Image, das vor den Tests abhängig vom Prüfgebiet in die Testlaborkarte übertragen werden muss. Diese d3-Files MÜSSEN und können nur vom Hersteller erstellt werden. Nachfolgend eine Übersicht der d3-Files inklusive der Datenvorlage für diese Dateien.

4.1.1 COS-Image-Files (d3-Files)

Die nachfolgenden d3-Files werden für den funktionalen Eignungstest des Kartenbetriebssystems benötigt.

Tabelle 3: Tab_TLK_ObjSys_003 – Übersicht der d3-Files (COS)

Prüfgebiet	d3-File Name* / Datenbasis
Zugriffskontrolle und Security Environment	TLK_<zls>_access_se_<datum>.d3 Vorlage: TLK_COS_image_access_se.xml
Statische Secure Messaging	TLK_<zls>_staticSM_<datum>.d3 Vorlage: TLK_COS_image_staticSM.xml
Applikationen / DFs	TLK_<zls>_folder_<datum>.d3 Vorlage: TLK_COS_image_folder.xml
Transparente Daten Elemente	TLK_<zls>_binary_files_<datum>.d3 Vorlage: TLK_COS_image_binary_files.xml
Strukturierte	TLK_<zls>_record_filesLF_<datum>.d3

Prüfgebiet	d3-File Name* / Datenbasis
Daten Elemente, fixe Länge	Vorlage: TLK_COS_image_record_filesLF.xml
Strukturierte Daten Elemente, varibale Länge	TLK_<zls>_record_filesLV_<datum>.d3 Vorlage: TLK_COS_image_record_filesLV.xml
Strukturierte Daten Elemente, zyklisch	TLK_<zls>_record_filesZ_<datum>.d3 Vorlage: TLK_COS_image_record_filesZ.xml
Passwörter	TLK_<zls>_passwords_<datum>.d3 Vorlage: TLK_COS_image_passwords.xml
Universal einsetzbar	TLK_<zls>_universal_<datum>.d3 Vorlage: TLK_COS_image_universal.xml
RSA-Schlüssel	TLK_<zls>_keys_rsa_<datum>.d3 Vorlage: TLK_COS_image_keys_rsa.xml
ELC-Schlüssel	TLK_<zls>_keys_elc_<datum>.d3 Vorlage: TLK_COS_image_keys_elc.xml
Objektsuche	TLK_<zls>_search_obj_<datum>.d3 Vorlage: TLK_COS_image_search_obj.xml
Transaktionsschutz und Checksumme	TLK_<zls>_roll_function_<datum>.d3 Vorlage: TLK_COS_image_roll_function.xml
Importierte, öffentliche Schlüssel	TLK_<zls>_cache_<datum>.d3 Vorlage: TLK_COS_image_cache.xml
Perfomance des COS Teil A	TLK_<zls>_performA_<datum>.d3 Vorlage: TLK_COS_image_performA.xml
Perfomance des COS Teil B	TLK_<zls>_performB_<datum>.d3 Vorlage: TLK_COS_image_performB.xml
Perfomance des COS Teil C	TLK_<zls>_performC_<datum>.d3 Vorlage: TLK_COS_image_performC.xml
Option kontaktlose Schnittstelle CAN128	TLK_<zls>_kontaktlos128_<datum>.d3 Vorlage: TLK_COS_image_kontaktlos128.xml
Option kontaktlose Schnittstelle CAN192	TLK_<zls>_kontaktlos192_<datum>.d3 Vorlage: TLK_COS_image_kontaktlos192.xml
Option kontaktlose Schnittstelle CAN256	TLK_<zls>_kontaktlos256_<datum>.d3 Vorlage: TLK_COS_image_kontaktlos256.xml
Option Kryptobox	TLK_<zls>_kryptobox_<datum>.d3 Vorlage: TLK_COS_image_kryptobox.xml
Option Kryptobox Objektsuche	TLK_<zls>_search_kryptobox_<datum>.d3 Vorlage: TLK_COS_image_search_kryptobox.xml
Option PACE-PCD	TLK_<zls>_pace_pcd_<datum>.d3 Vorlage: TLK_COS_image_pace_pcd.xml

4.1.2 Kartentyp-Objektsystem Image-Files (d3-Files)

Die nachfolgenden d3-Files werden für den funktionalen Eignungstest des jeweiligen Kartentyp-Objektsystems benötigt.

Tabelle 4: Tab_TLK_ObjSys_004 – Übersicht der d3-Files (Kartentyp)

Prüfgebiet	d3-File Name* / Datenbasis
Objektsystem eGK	TLK_<zls>_eGK_G2_<datum>.d3 Vorlage: [gemSpec_eGK_ObjSys]
Objektsystem HBA	TLK_<zls>_HBA_G2_<datum>.d3 Vorlage: [gemSpec_HBA_ObjSys]
Objektsystem SMC-B	TLK_<zls>_SMC_B_G2_<datum>.d3 Vorlage: [gemSpec_SMC-B_ObjSys]
Objektsystem gSMC_K	TLK_<zls>_gSMC_K_G2_<datum>.d3 Vorlage: [gemSpec_gSMC-K_ObjSys]
Objektsystem gSMC-KT	TLK_<zls>_ gSMC_KT_G2_<datum>.d3 Vorlage: [gemSpec_gSMC-KT_ObjSys]

4.2 d3-File Name

Für die Platzhalter in den Dateinamen gelten die Werte in der nachfolgenden Tabelle.

Tabelle 5: Tab_TLK_ObjSys_005 – d3-File Name

<zls>	Zulassungsschlüssel [gemZul_ProdCOS] bzw. [gemZul_Prodxxx]-Kennung des „Antrags auf Zulassung … - …“ Vergeben durch die Zulassungsstelle der gematik Struktur: ZLS_<Produkttyp>_<herstellerkürzel>_<lfd. nr.>
<datum>	Erstelldatum des d3-Files (jjjjmmtt ohne Trennpunkte).

4.3 Aufbau und Struktur eines Image-Files

Image-Files beinhalten eine Auflistung von Chipkartenkommandos (APDUs), mit deren Hilfe Objektsystem und Inhalte in eine Testlaborkarte eingebracht werden können. Für das Einbringen dieser Informationen in eine Testlaborkarte können auch Chipkarten-kommandos benutzt werden, die nicht Bestandteil der Spezifikation [gemSpec_COS] sind.

Chipkartenkommandos müssen in dem d3-File dem folgenden Format entsprechend ge-speichert werden:

```
{
  (LOAD)
  {
    (APDU_0001) = 00 01 02 03;
    (APDU_0002) = 00 01 02 03 04 05;

    (APDU_nnnn) = 00 01 02 03;
  }
}
```

Diese APDU-Liste - durchnummeriert von 0001 bis nnnn (Hex-Werte) - wird durch die Testskripte sequenziell abgearbeitet und jede APDU an die Karte gesendet. Als SW1||SW2 erwartet die Testsuite ‚9000' zurück.

Ein erneutes Laden eines Images in die Testlaborkarte kann spezielle Kommandos (Sonderkommandos) erforderlich machen.

Die APDU-Liste KANN Sonderkommandos enthalten. Diesen APDUs sind folgende Präfixe voranzustellen, die durch die Testsuite ausgewertet werden:

00 00 00 00 xx

Für xx == 00 → die Testsuite initiiert ein COLD RESET der Karte.

Für xx == 01 → die Testsuite wertet den auf eine APDU returnierten Return-Code nicht aus.

Sollte es beispielsweise ein Sonderkommando DELETE MF geben, wäre es sinnvoll den Präfix 00 00 00 00 01 voranzustellen.

Weitere Präfixe können – falls nötig – in Absprache mit der gematik verwendet werden.

Hinweis: Die Reinitialisierung des Objektsystems kann zu unterschiedlichen Zeitpunkten eines Testfalls aufgerufen werden. Zu diesem Zeitpunkt kann der Zeiger auf ein Objekt im Objektsystem zeigen, das nicht gleich dem MF (Root) ist. Abhängig von den in der Initialisierungsdatei verwendeten Chipkartenkommandos kann es notwendig sein, die Initialisierungsdatei mit einem SELECT auf das MF (Root) zu beginnen.

Anhang A

A1 – Abkürzungen

Kürzel	Erläuterung
ATR	Answer to Reset
AUT	Authentifizierung
BÄK	Bundesärztekammer
BCD	Binär kodierte Dezimalzahl
CAN	Card Access Number
COS	Card Operating System
CVC	Card Verifiable Certificate
DF	Dedicated File
EF	Elementary File
eGK	elektronische Gesundheitskarte
EHIC	Europäische Krankenversichertenkarte
ENC	Verschlüsselung (Encryption)
HBA	Heilberufsausweis (auch HPC)
HPC	Health Professional Card (auch HBA)
ICCSN	Integrated Circuit Card Serial Number
MF	Master File
OCSP	Online Certificate Status Protocol
PIN	Persönliche Identifikationsnummer
PuK	Public Key (öffentlicher Schlüssel)
PUK	Pin Unblocking Key
PrK	Private Key (privater Schlüssel)
QES	Qualifizierte Elektronische Signatur
SMC	Security Module Card
TLV	Tag Length Value
TLK	Testlaborkarte
XML	Universelle Datenbeschreibungssprache (Extensible Markup Language)
ZLS	Zulassungsschlüssel

A2 - Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 - Abbildungsverzeichnis

Abbildung 1: Layout der Testlaborkarte der Generation 2 9

A4 - Tabellenverzeichnis

Tabelle 1: Tab_TLK_ObjSys_001 – ATR-Codierung 10
Tabelle 2: Tab_TLK_ObjSys_002 – Template <card_capabilities> 15
Tabelle 3: Tab_TLK_ObjSys_003 – Übersicht der d3-Files (COS) 18
Tabelle 4: Tab_TLK_ObjSys_004 – Übersicht der d3-Files (Kartentyp) 20
Tabelle 5: Tab_TLK_ObjSys_005 – d3-File Name 20

A5 - Referenzierte Dokumente

A5.1 – Dokumente der gematik

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

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS) - Elektrische Schnittstelle
[gemSpec_eGK_ObjSys]	gematik: Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem
[gemSpec_gSMC-K_ObjSys]	gematik: Spezifikation der gSMC-K Objektsystem
[gemSpec_gSMC-KT_ObjSys]	gematik: Spezifikation der gSMC-KT Objektsystem
[gemSpec_HBA_ObjSys]	gematik: Spezifikation des elektronischen Heilberufsausweises HBA Objektsystem

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_SMC-B_ObjSys]	gematik: Spezifikation der Security Module Card SMC-B Objektsystem
[gemSpec_TK]	gematik: Spezifikation für Testkarten gematik (eGK, HBA, (g)SMC) der Generation 2
[gemSpec_xxx_ObjSys]	xxx = Synonym für eGK, HBA, SMC-B, gSMC-K, gSMC-KT
[gemSpec_Karten_Fach_TIP]	gematik: Befüllvorschriften für die Plattformanteile der Karten der TI
[gemTLK_COS-Dat]	Dateiname: TLK_COS_image_<objekt- bzw. prüfgebiet>.xml Sammelbegriff für die Objektsystemdateien, die dem Hersteller eines COS zur Verfügung gestellt werden. Auf der Basis dieser Dateien erstellt der Hersteller die ladefähigen Image-Files für die Testlaborkarte (siehe Kapitel 4.1). Objektsystemdateien: TLK_COS_image_access_se.xml TLK_COS_image_staticSM.xml TLK_COS_image_folder.xml TLK_COS_image_binary_files.xml TLK_COS_image_record_filesLF.xml TLK_COS_image_record_filesLV.xml TLK_COS_image_record_filesZ.xml TLK_COS_image_passwords.xml TLK_COS_image_universal.xml TLK_COS_image_keys_rsa.xml TLK_COS_image_keys_elc.xml TLK_COS_image_search_obj.xml TLK_COS_image_roll_function.xml TLK_COS_image_cache.xml TLK_COS_image_performA.xml TLK_COS_image_performB.xml TLK_COS_image_performC.xml TLK_COS_image_kontaktlos128 (nur Opt-2) TLK_COS_image_kontaktlos192 (nur Opt-2) TLK_COS_image_kontaktlos256 (nur Opt-2) TLK_COS_image_kryptobox.xml (nur Opt-4) TLK_COS_image_search_kryptobox.xml (nur Opt-4) TLK_COS_image_pace_pcd.xml (nur Opt-5) Die vom Hersteller erstellten, ladefähigen Image-Files sind maßgeblich für den funktionalen Eignungstest eines COS.
[gemTLK_COS-Tpl]	Dateiname: TLK_<zls>_Template_<datum>.xml Template-Datei (xml-Struktur), die Informationen für den Hersteller eines COS beinhaltet und ergänzt werden muss mit Informationen durch den Hersteller. Die vom Hersteller modifizierte Datei ist maßgeblich für den funktionalen Eignungstest eines COS bzw. der Kartentyp-Objektsysteme.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemZul_ProdCOS]	gematik: Verfahrensbeschreibung Zulassung Produkte der Telematikinfrastruktur hier: Card Operating System (COS)
[gemZul_ProdeGK]	gematik: Verfahrensbeschreibung Zulassung Produkte der Telematikinfrastruktur hier: elektronische Gesundheitskarte (eGK) G2
[gemZul_ProdHBA]	gematik: Verfahrensbeschreibung Zulassung Produkte der Telematikinfrastruktur hier: Heilberufsausweis (HBA) G2
[gemZul_ProdSMCB]	gematik: Verfahrensbeschreibung Zulassung Produkte der Telematikinfrastruktur hier: Sicherheitsmodulkarte Typ B (SMC-B) G2
[gemZul_ProdSMCK]	gematik: Verfahrensbeschreibung Zulassung Produkte der Telematikinfrastruktur hier: gerätespezifische Sicherheitsmodulkarte Typ K (gSMC-K) G2
[gemZul_ProdSMCKT]	gematik: Verfahrensbeschreibung Zulassung Produkte der Telematikinfrastruktur hier: gerätespezifische Sicherheitsmodulkarte Typ K (gSMC-KT) G2
[gemZul_Prodxxx]	xxx = Synonym für eGK, HBA, SMC-B, gSMC-K, gSMC-KT

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ISO7816-4]	ISO/IEC 7816-4: 2013 Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange
[RFC2119]	Network Working Group, Request for Comments: 2119, S. Bradner Harvard, University, March 1997, Category: Best Current Practice Key words for use in RFCs to Indicate Requirement Levels http://www.apps.ietf.org/rfc/rfc2119.html