Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
Mobiles Kartenterminal
(inkl. Mini-AK und Mini-PS)

Version:	2.14.0
Revision:	245771
Stand:	26.06.2020
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_MobKT

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	13.11.08		freigegeben Die vorliegende Version setzt auf dieser Version, die Historie wurde gekürzt und kann ggf. in Version 1.0.0 nachgelesen werden.	gematik
1.0.11	13.08.12		grundlegend überarbeitet für den Online-Rollout (Stufe 1), zusätzlich formale Überarbeitung	P77
1.0.12	21.08.12		zur Abstimmung freigegeben	PL P77
2.0.0	15.10.12		Einarbeitung Gesellschafterkommentare	P77
2.1.0	12.11.12		Einarbeitung Kommentare aus der übergreifenden Konsistenzprüfung	P77
2.2.0	29.05.13		Einarbeitung Gesellschafterkommentare, Bieterfragen und interner Kommentare	P 77
2.3.0	06.06.13		freigegeben	gematik
2.4.0	15.08.13		Einarbeitung lt. Änderungsliste vom 08.08.13	P 77
2.5.0	21.02.14		Losübergreifende Synchronisation	P77

2.6.0	17.06.14		Streichung der Maßangaben in [TIP1-A_3702], konfigurierbares Druckmodul [TIP-A_4415], Anpassung Begriff „Verbindung" [TIP-A_3754], Ergänzung Ausnahmeregelung für TOE Reset Pin [TIP1-A_3766] gemäß P11-Änderungsliste	P77
2.7.0	26.08.14		Anpassungen zu Cross-CV-Zertifikaten in #5.2.2.5, #7.4.3 und #10.1.7 gemäß P12-Änderungsliste (C_4560)	gematik
2.8.0	24.08.16		Anpassungen zum Online-Produktivbetrieb (Stufe 1)	gematik
2.9.0	28.10.16		Anpassungen gemäß Änderungsliste (Ergänzung TIP1-A_6706)	gematik
2.10.0	21.04.17	11.1.4 3.3.4	Anpassungen gemäß Änderungsliste	gematik
2.10.1	18.05.17		Redaktionelle Anpassungen (Lesbarkeit Abb)	gematik
2.11.0	14.05.18		Anpassungen gemäß Änderungsliste P 15.2 und P 15.4	gematik
2.11.1	05.06.18		Aktualisierung Angaben Deckblatt	gematik
2.12.0	15.05.19		Einarbeitung P18.1	gematik
2.13.0	02.10.19		Einarbeitung P20.1 (Unterstützung für G1+ eGK angepasst)	gematik
2.14.0	26.06.20		Anpassungen lt. Änderungsliste P21.3	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes 9

1.1 Zielsetzung 9

1.2 Zielgruppe 9

1.3 Geltungsbereich 9

1.4 Abgrenzung des Dokumentes 9

1.5 Methodik 10

1.5.1 Designansatz 10

1.5.2 Diagramme 10

1.5.3 Anforderungen 10

1.5.4 Rolle Administrator 11

1.5.5 Hinweis auf offene Punkte 11

2 Systemüberblick 12

2.1 Grundlagen 12

2.1.1 Einsatz des Mobilen Kartenterminals 12

2.1.2 Sicherheit 13

2.1.2.1 Nachgewiesene Sicherheit 13

2.2 Zulassungsverfahren, Zertifikat 13

2.3 Komponentenmodell 14

2.3.1 Kartenterminal-Modul 15

2.3.2 Mini-Anwendungskonnektor 16

2.3.3 Mini-Primärsystem 16

2.3.4 Management-Modul 16

2.3.5 Systemuhr 16

2.3.6 Erweitertes Display 16

2.3.7 Drucker 17

2.3.8 Ansteuerung externer Komponenten 17

2.3.9 Technische Ausprägungen 17

2.3.9.1 Einboxlösung 17

2.3.9.2 Mehrkomponenten-Lösung 17

2.4 Einbettung in das Anwendungsumfeld 17

2.5 Standards und Normen 18

3 Allgemeine Anforderungen 19

3.1 Logische und Funktionale Trennung 19

3.2 Integration in die Telematikinfrastruktur 19

3.3 Physikalische Anforderungen 20

3.3.1 EMV-Prüfung 20

3.3.2 Vibrationstest 20

3.3.3 Klima 20

3.3.4 Stromversorgung 21

3.3.5 Transportierbarkeit 22

3.3.6 Schnittstelle zum Primärsystem 22

3.3.7 Gehäuse 22
3.3.7.1 Versiegelung 22
3.3.7.2 Prüfzeichen 22
3.4 Betriebsanforderungen 24
3.4.1 Wartbarkeit 24
3.4.2 Anzeige des Betriebszustandes 24
3.4.3 Betriebssicherheit 24
3.4.4 Zuverlässigkeit 24
3.4.5 Fehlertoleranz 25
3.4.6 Auslieferungszustand 25
3.4.7 Werksreset 25
3.4.8 Firmware Update 27
3.4.8.1 Konzept der Firmware-Gruppen 28
3.4.9 Produkttypversion und Selbstauskunft 28
3.4.10 Kompatibilität zukünftiger Kartenversionen 28
3.5 Sicherheitstechnische Anforderungen 29
3.5.1 Schutz der KVK 29
3.5.2 Schutz der eGK 29
3.5.3 Vertraulichkeit 30
3.5.4 Lebensdauer sensibler Daten 30
3.5.5 Protokollierung des Zugriffs 30
3.5.6 Anschluss weiterer Komponenten 31
4 Anforderungen an das Kartenterminal-Modul 32
4.1 Display und PIN Pad 32
4.2 PIN-Eingabe und PIN-Änderung 32
4.3 Zugriffsanzeige 34
4.4 Performanz 35
4.5 Kartenorientierte Anforderungen 35
4.5.1 Stromversorgung der Chipkarten 35
4.5.2 Anzahl Kontaktiereinheiten 36
4.5.3 Ausprägung Kontaktiereinheiten 36
4.5.3.1 ID-1-Kartenkontaktierungen 37
4.5.3.2 ID-000 Kartenkontaktierungen 38
4.5.4 Chipkartenprotokolle 38
5 Anforderungen an den Mini-Anwendungskonnektor 40
5.1 Basismechanismen 40
5.1.1 Zufallszahlen und Schlüssel 40
5.2 Basisdienste 40
5.2.1 Kartenterminaldienst 40
5.2.2 Kartendienst 41
5.2.2.1 Identifikation des Kartentyps und der Version 41
5.2.2.2 Zugriff auf Dateien der Karte 43
5.2.2.3 PIN-Verifikation und PIN-Management 43
5.2.2.4 Ereignisse 43
5.2.2.5 Card-to-Card-Authentisierung und sichere Kanäle 44
5.2.2.6 Datenzugriffsaudit 44
5.2.3 Verschlüsselungsdienst 45

5.2.4 Zertifikatsdienst 45
5.3 Fachanwendung VSDM 46
5.3.1 Übergreifende Anforderungen 46
5.3.2 VSD von eGK im mobilen Einsatzszenario lesen 50
5.3.2.1 Technische Nutzbarkeit und Offline-Gültigkeit der eGK prüfen 51
5.3.2.2 Echtheit der beteiligten Karten prüfen 52
5.3.2.3 VSD Status Container Lesen 52
5.3.2.4 PD und VD von eGK lesen 53
5.3.2.5 GVD von eGK lesen 54
5.3.2.6 Protokolleintrag auf eGK schreiben 54
5.3.2.7 PD, VD, GVD und StatusVD im Zwischenspeicher ablegen 55
5.3.3 Versichertendaten von KVK im mobilen Einsatzszenario lesen 55
5.3.3.1 Versichertendaten von KVK lesen 56
5.3.3.2 Versichertendaten prüfen 56
5.3.3.3 Versichertendaten im Zwischenspeicher ablegen 57

6 Anforderungen an das Mini-Primärsystem 58
6.1 Abbildung fachlicher Anwendungsfälle auf technische Use Cases 58
6.2 Benutzerführung 59
6.2.1 Allgemeine Anforderungen 59
6.2.2 Fachliche Aufrufe 60
6.2.3 Warnmeldungen 60
6.2.4 Fehlermeldungen 60
6.3 Zwischenspeicher 61
6.3.1 Zugriffsschutz Zwischenspeicher 62
6.4 Zwischenspeichern von Daten 63
6.5 Übertragen von Daten 63
6.5.1 Sonderfall Dockingstation 65
6.6 Gezieltes Löschen von zwischengespeicherten Daten 65
6.7 PIN-Verwaltung 66
6.7.1 PIN ändern 66
6.7.2 PIN entsperren 66
6.8 Daten drucken 66

7 Anforderungen an das Management-Modul 68
7.1 Allgemeine Anforderungen 68
7.2 Kennwörter zur Sicherung der Managementschnittstelle 69
7.3 Durchführen und Anzeigen Ergebnis-Selbsttest 71
7.4 Konfigurationsbereiche 71
7.4.1 Konfiguration des Kartenterminal-Moduls 71
7.4.2 Konfiguration des Mini-PS 71
7.4.3 Konfiguration des Mini-AK 72
7.4.4 Konfiguration der Fachanwendungen 72
7.4.4.1 Fachmodul VSDM 72
7.4.5 Konfiguration der Systemuhr 72
7.4.6 Konfiguration der optionalen Druckerschnittstelle 73

7.4.7 Konfiguration des automatischen Rücksetzens des Sicherheitszustand bei Benutzerinaktivität 74

8 Anforderungen an das erweiterte Display 75

8.1 Kommunikation mit dem erweiterten Display 75

8.2 Nutzbarkeit für das Kartenterminal-Modul 76

9 Anforderungen an die Systemuhr 77

10 Technische Use Cases 78

10.1 Technische Use Cases des Mini-AK 78
10.1.1 TUC_MOKT_200 sendAPDU 78
10.1.2 TUC_MOKT_202 readFile 81
10.1.3 TUC_MOKT_209 readRecord 84
10.1.4 TUC_MOKT_214 appendRecord 87
10.1.5 TUC_MOKT_220 fulfillAccessConditions 90
10.1.6 TUC_MOKT_250 selectCardFile 94
10.1.7 TUC_MOKT_405 authenticateCardToCard 97
10.1.8 TUC_MOKT_406 writeEGKAudit 104
10.1.9 TUC_MOKT_407 selectKeyForAsymmetricExternalAuthentication 106
10.1.10 TUC_MOKT_412 verifyPIN 112
10.1.11 TUC_MOKT_417 readFromEGK 118
10.1.12 TUC_MOKT_418 checkEGK 122
10.1.13 TUC_MOKT_419 changePIN 124
10.1.14 TUC_MOKT_420 showEGKAccessInKTDisplay 128
10.1.15 TUC_MOKT_421 unblockPIN 129
10.1.16 TUC_MOKT_438 checkEGKAuthCertificate 133
10.1.17 TUC_MOKT_470 encryptData 136
10.1.18 TUC_MOKT_471 decryptData 140

10.2 Technische Use Cases des Mini-PS 145
10.2.1 TUC_MOKT_010 writeToInternalStorage 145
10.2.2 TUC_MOKT_011 readFromInternalStorage 147

11 Beschreibung der Host-Schnittstelle zur Übertragung zwischen Mobilem Kartenterminal und Primärsystem 151

11.1 Kommandobeschreibung 152
11.1.1 RESET CT 152
11.1.2 REQUEST ICC 153
11.1.3 EJECT ICC 154
11.1.4 SELECT FILE 154
11.1.5 READ BINARY 156
11.1.5.1 READ BINARY KVK 156
11.1.5.2 READ BINARY eGK 157
11.1.6 ERASE BINARY 159
11.1.7 GET STATUS 160

11.2 Kommandosequenz des externen Primärsystems 163
11.2.1 Vorbereitung 163
11.2.2 Lesen der KVK (bei REQUEST ICC: SW1SW2=9000) 164
11.2.3 Lesen der VSD der eGK (bei REQUEST ICC: SW1SW2=9001) 164

11.3 Erweiterungen der Datentypen bei der Übertragung 165

12 Anhang A 167
12.1 Abkürzungen 167
12.2 Glossar 168
12.3 Abbildungsverzeichnis 168
12.4 Tabellenverzeichnis 169
12.5 Referenzierte Dokumente 171
12.5.1 Dokumente der gematik 171
12.5.2 Weitere Dokumente 173
12.6 Nutzung von Kartenelementen (COS und Objektsysteme) 175
13 Anhang B – Prüfvorgaben KVK 178
13.1 Aufbau der KVK 178
13.2 Prüfvorgaben der KVK 179

1 Einordnung des Dokumentes

1.1 Zielsetzung

Dieses Dokument spezifiziert das Mobile Kartenterminal inklusive der Schnittstelle zum Primärsystem zur Übertragung zwischengespeicherter Daten. In diesem Dokument wird die Einboxlösung, bei der die drei Komponenten Mini-AK, Mini-PS und Kartenterminal-Modul zusammen in einem Gerät umgesetzt sind, spezifiziert. Das Gesamtsystem ist konzipiert für den Einsatz außerhalb der Arztpraxis, z. B. bei Hausbesuchen, um abrechnungsrelevante Versichertenstammdaten (VSD) von einer Krankenversicherungskarte (KVK) oder einer elektronischen Gesundheitskarte (eGK) zu lesen und diese für Abrechnungszwecke an das Primärsystem (PS) des Leistungserbringers zu übertragen.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller von Mobilen Kartenterminals sowie Hersteller und Anbieter von Primärsystemen.

Es enthält zudem Informationen für die Leistungserbringer.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des Deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung im Zulassungsverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

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 Abgrenzung des Dokumentes

In diesem Dokument werden spezifische Anforderungen an Mobile Kartenterminals erhoben. Anforderungen, die neben dem mobilen Kartenterminal auch durch andere Produkttypen umgesetzt werden müssen, werden in übergreifenden Spezifikationen spezifiziert.

Festlegungen, welche im Schutzprofil (Protection Profile) des Mobilen Kartenterminals gemäß Common Criteria getroffen werden, werden hier nur angeführt, soweit es für das Verständnis erforderlich ist.

1.5 Methodik

1.5.1 Designansatz

Dieses Dokument spezifiziert die Komponente als Black Box, d. h. es beschreibt normativ die Außenschnittstellen (System- und Benutzerschnittstellen) und das äußere Verhalten der Komponente. Die innere Struktur wird durch dieses Dokument nicht geregelt. Um die komplexen Verhaltensmuster an den äußeren Schnittstellen besser beschreiben zu können, verwendet dieses Dokument eine modellhafte Beschreibung des inneren Verhaltens so weit, wie es für die verständliche Festlegung des Außenverhaltens erforderlich bzw. hilfreich ist.

Die Modellierung des inneren Verhaltens und der inneren Struktur dient auch als Hinweis auf Aspekte, deren Berücksichtigung bei der Sicherheitsevaluierung notwendig oder ratsam ist, um die Sicherheitsziele der Schutzprofile zu erfüllen. Die innere Struktur der realen Komponente bleibt jedoch vollständig eine herstellerseitige Definition, deren Schutzprofilkonformität allein der Hersteller im Rahmen seiner Komponentenevaluierung nachzuweisen hat (siehe auch Kapitel 2.1.2.1 Nachgewiesene Sicherheit).

1.5.2 Diagramme

Die Darstellung der Spezifikationen von Komponenten erfolgt auf der Grundlage einer durchgängigen Use-Case-Modellierung als

- technische Use Cases (eingebundene Grafik sowie tabellarische Darstellung mit Vor- und Nachbedingungen),
- Sequenz- und Aktivitätsdiagramme,
- Klassendiagramme sowie
- XML-Strukturen und Schnittstellenbeschreibungen.

1.5.3 Anforderungen

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

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

1.5.4 Rolle Administrator

In dieser Spezifikation wird der Begriff „Administrator" verwendet. Hierunter ist keine Berufsbezeichnung zu verstehen, sondern die Rolle Administrator, welche zur Verwaltung der Komponente besondere Rechte und Aufgaben hat. Darüber, welche Person diese Rolle ausfüllt, werden keine Vorgaben gemacht.

1.5.5 Hinweis auf offene Punkte

Auf offene Punkte wird durch einen Text in nachfolgendem Format hingewiesen:

Beispiel Formatierung offener Punkte

2 Systemüberblick

2.1 Grundlagen

2.1.1 Einsatz des Mobilen Kartenterminals

Das Mobile Kartenterminal kommt hauptsächlich außerhalb der Arztpraxis, z. B. bei Hausbesuchen oder Behandlungen in Heimen und bei Notdiensten zum Einsatz. Es soll dem Leistungserbringer ermöglichen, außerhalb seiner Praxis die Versichertenstammdaten seiner Patienten zu Abrechnungszwecken zu erfassen sowie anzuzeigen.

Um Zugriff auf die geschützten Daten (geschützte VSD) einer eGK zu erlangen, muss diese mittels eines HBAs oder einer SMC-B (im Folgenden als „berechtigte Karten" bezeichnet) freigeschaltet werden. Für den Zugriff auf die Daten einer KVK bzw. auf die ungeschützten VSD der eGK ist keine Freischaltung erforderlich. Während der Datenerfassung wird der Erfassungszeitpunkt protokolliert. Ein zwischengespeicherter Datensatz besteht aus den gelesenen VSD, dem zugehörigen Erfassungszeitpunkt sowie der Zulassungsnummer des Mobilen Kartenterminals. Auf Benutzerwunsch können VSD einer gesteckten Karte sowie zwischengespeicherte VSD am Mini-PS zur Anzeige gebracht werden. Schreibender Zugriff auf gesteckte Karten ist nur zum Zwecke der Protokollierung auf den Logging-Container der eGK zulässig. Weitere schreibende Zugriffe sind nicht erlaubt. Da die zwischengespeicherten Daten einen hohen Schutzbedarf besitzen und zu Abrechnungszwecken genutzt werden, müssen sie vor Zugriff durch Unbefugte, Manipulation und Missbrauch geschützt werden.

Um die zwischengespeicherten Daten für die Abrechnung mit den Krankenkassen zu nutzen, kann der Arzt sie auf sein Primärsystem (Praxisverwaltungssystem (PVS) bzw. Krankenhausinformationssystem (KIS)) übertragen (im Folgenden wird für beide nur noch der Begriff Primärsystem verwendet). Die Übertragung erfolgt über die so genannte Host-Schnittstelle, welche das CT-API-Protokoll [CT-API] zur Übertragung nutzt. Zwischengespeicherte Daten können auch ohne vorherige Übertragung an das Primärsystem gelöscht werden. Optional können die zwischengespeicherten VSD auch über einen integrierten oder extern angeschlossenen Drucker ausgedruckt werden.

Hersteller seien darauf hingewiesen, dass die mobilen Komponenten auch in Einsatzumgebungen verwendet werden können, die einem erhöhten Übertragungsrisiko für Infektionen, z. B. durch häufigen Hand- und Hautkontakt, ausgesetzt sind. Die regelmäßige Desinfektion der eingesetzten Geräte beim Leistungserbringer, dazu gehören auch die mobilen Komponenten, ist eine Maßnahme zur Verminderung des Übertragungsrisikos und zur Einhaltung entsprechender Vorgaben, z. B. denen des Arbeitsschutzgesetzes. Weiterführende Informationen sind unter anderem den folgenden Dokumenten zu entnehmen:

- Anforderungen an die Hygiene bei der Reinigung und Desinfektion von Flächen des Robert-Koch-Institutes [RKI],
- Technischen Regeln für Biologische Arbeitsstoffe im Gesundheitswesen und in der Wohlfahrtspflege [TRBA 250]
- Hygieneleitfaden des Deutschen Arbeitskreises für Hygiene in der Zahnmedizin [DAHZ].

2.1.2 Sicherheit

Um Zugriff auf die geschützten Daten einer eGK zu erlangen, ist eine Freischaltung der eGK mittels einer berechtigten Karte erforderlich. Die Freischaltung erfolgt im Hintergrund mittels Card-to-Card-Authentisierung (C2C) zwischen berechtigter Karte und eGK. Die Ablaufsteuerung der C2C-Authentisierung übernimmt der Mini-AK.

Damit die berechtigte Karte eine eGK freischalten kann, muss die berechtigte Karte mittels PIN-Eingabe freigeschaltet werden. Hierfür muss das Mobile Kartenterminal über ein Display und ein PIN Pad verfügen. Die PIN-Eingabe muss direkt am Mobilen Kartenterminal erfolgen.

Das Mobile Kartenterminal stellt sicher, dass ein Abhören, Zwischenspeichern oder Manipulieren der PIN nicht möglich ist. Die PIN wird ausschließlich an die berechtigte Karte gesendet und verlässt das Mobile Kartenterminal nicht über andere Schnittstellen. Der Benutzer muss überprüfen können, ob die eingesetzten Komponenten Mobiles Kartenterminal, Mini-AK und Mini-PS, zugelassen, vertrauenswürdig, authentisch und integer sind. Manipulationen an den Komponenten müssen mit hoher Wahrscheinlichkeit vom Benutzer erkennbar sein. Die Dauer der Freischaltung einer berechtigten Karte ist zeitlich begrenzt. VSD werden für die Zwischenspeicherung mit einer berechtigten Karte verschlüsselt. Das Mobile Kartenterminal stellt sicher, dass vertrauliche Daten (personenbezogene Daten, medizinische Daten etc.) nicht unberechtigt ausgelesen oder verändert werden können.

2.1.2.1 Nachgewiesene Sicherheit

Die Sicherheit von dezentralen Komponenten der Telematikinfrastruktur wird durch CC-Evaluierung und Zertifizierung nachgewiesen. Für die Evaluierung des Mobilen Kartenterminals sind die im Schutzprofil (Protection Profile) [BSI-CC-PP-0052] definierten Sicherheitsziele maßgeblich. Alle Sicherheitsziele werden dort definiert, die umgesetzten Maßnahmen einer Herstellerlösung müssen mindestens diese Ziele nachweislich erfüllen.

Da die Schutzprofile mit der angeschlossenen Sicherheitsevaluierung den Kern der Sicherheitsumsetzung bilden, werden im Rahmen dieser Spezifikation Anforderungen an die Sicherheit nur so weit erfasst, wie sie Auswirkungen auf andere funktionale oder nichtfunktionale Anforderungen haben oder wie eine Umsetzung einer reinen Sicherheitsanforderung Belange der Interoperabilität berührt. Spezifikation und Schutzprofil bilden hier eine Einheit der Anforderungen an ein Mobiles Kartenterminal.

2.2 Zulassungsverfahren, Zertifikat

Für die Zulassung des Mobilen Kartenterminals sind sicherheitstechnische und funktionale Prüfungen erforderlich. Das Zulassungsverfahren unterliegt den Vorgaben und der Aufsicht der gematik. Die Erteilung einer Zulassung erfolgt durch die gematik oder von ihr bevollmächtigte Dritte.

Eine durch die gematik akkreditierte Prüfstelle konzentriert Herstellererklärungen, Nachweise und Teilzertifikate, bewertet die Eignung, erstellt einen zusammenfassenden Bericht und reicht diesen an die Zulassungsstelle weiter, welche die Vollständigkeit und die Korrektheit überprüft. Die normativen Vorgaben zur Zulassung sind im Dokument „Zulassung von dezentralen IT-Komponenten in der Telematikinfrastruktur (Mobile Kartenterminals)“ [gemZul_MobKT] beschrieben.

Im Zuge der funktionalen Zulassung wird lediglich die korrekte Funktionalität an den Geräteschnittstellen getestet (Black-Box-Test). Die Sicherheitsevaluierung bezieht sich jedoch auch auf die internen herstellerspezifischen Umsetzungen.

2.3 Komponentenmodell

Diese Spezifikation beschreibt das Mobile Kartenterminal als Einboxlösung, d. h. eine Lösung, die in einem einzigen, geschlossenen Gehäuse zusammengefasst ist.

Um das Gerät verständlicher in die Telematikinfrastruktur einordnen zu können, wird zur Beschreibung eine Modularisierung gemäß einer stationären Ausstattung eines Leistungserbringers gewählt: Konnektor, Kartenterminal und Primärsystem. Diese Modularisierung ist ein architektonischer Ansatz zur Beschreibung des Außenverhaltens des Geräts, basierend auf bekannten Strukturen. Eine reale, direkte Umsetzung in diese Module ist für das Mobile Kartenterminal als Einboxlösung nicht erforderlich.

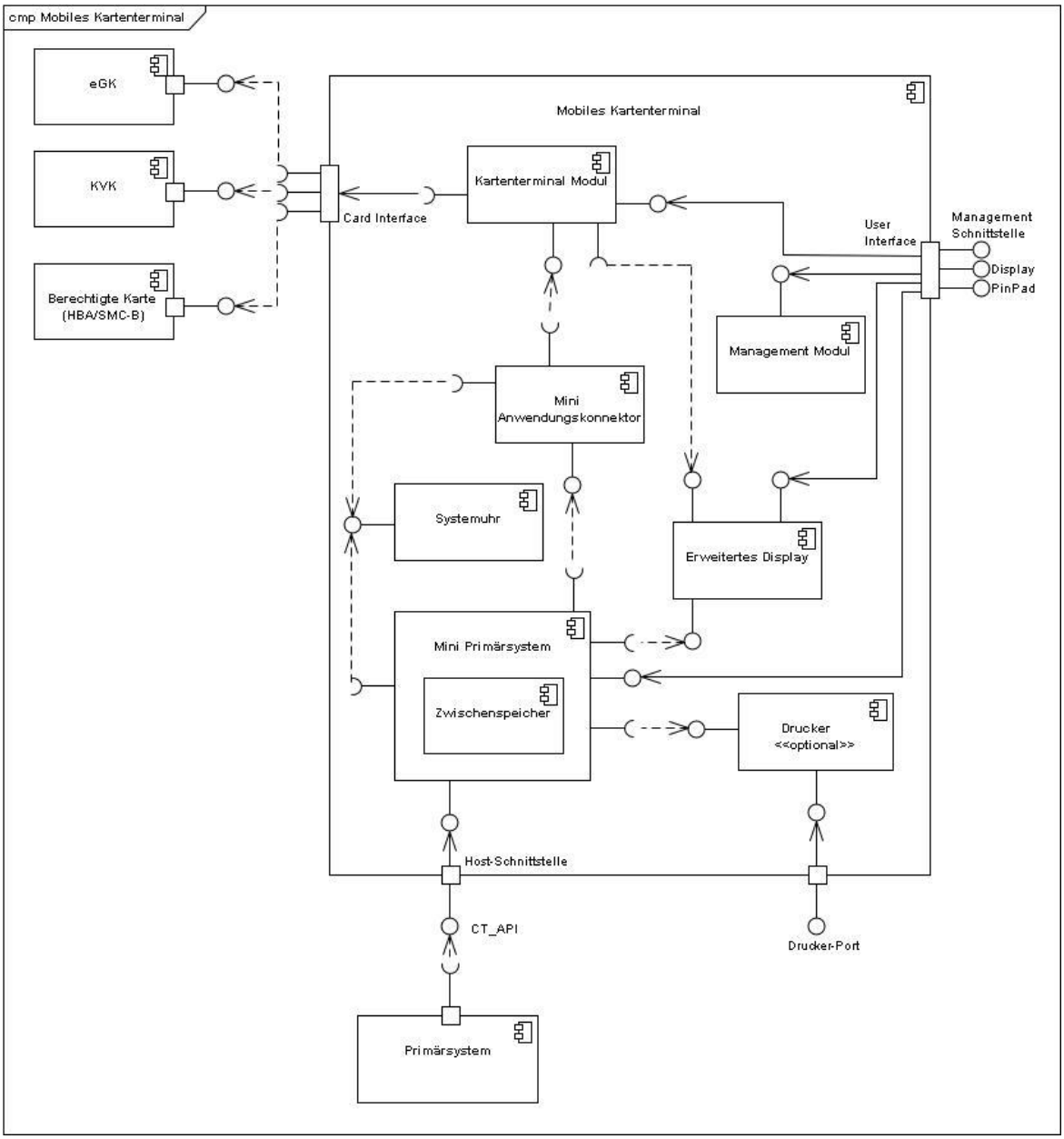


Abbildung 1: Komponentenmodell (logische Sicht)

Im Folgenden werden die Module des Mobilen Kartenterminals im Überblick beschrieben. Details zu den einzelnen Punkten sind dem normativen Teil zu entnehmen.

2.3.1 Kartenterminal-Modul

Das Kartenterminal-Modul bildet die logische Einheit, die für die physikalische Interaktion mit den Karten sowie die Nutzerinteraktion bei Kartenoperationen (Beispiel PIN-Eingabe) zuständig ist. Gemäß dem hier vorgestellten Komponentenmodell entspricht dieses Modul dem eHealth-Kartenterminal.

2.3.2 Mini-Anwendungskonnektor

Der Mini-AK ist eine Minimalversion des Anwendungskonnektors, dessen Funktionalität auf das für das mobile Szenario Notwendige beschränkt ist. Zu seinen Aufgaben zählen:

- die Durchsetzung der Abläufe entsprechend der Spezifikation,
- die C2C-Authentisierung,
- die Karten- und Kartenterminalverwaltung,
- die Display-Ansteuerung des Kartenterminal-Moduls,
- das Melden von Events (z. B. Karte gesteckt) an das Mini-PS,
- das Melden von Fehlern,
- die Ver- und Entschlüsselung,
- die Dekomprimierung von Daten.

Es ist zu beachten, dass die im Mini-AK durchgeführte X.509-Zertifikatsprüfung aufgrund der eingeschränkten Fähigkeiten des Mobilen Kartenterminals stark von der Prüfung in anderen Telematikinfrastruktur-Komponenten abweicht. Die Zertifikatsprüfung umfasst ausschließlich die Gültigkeits- und Rollenprüfung. Eine mathematische Prüfung bzw. eine Prüfung bzgl. des Vertrauensraums findet nicht statt.

2.3.3 Mini-Primärsystem

Das Mini-PS ist eine Minimalversion eines Primärsystems. Aus logischer Sicht liest das Mini-PS analog zum stationären Primärsystem (PS) Daten aus. Daher ist das Mini-PS aus logischer Sicht auch der Speicherort der zwischenzuspeichernden Daten und somit für den Schutz und die Übertragung der Daten an das Primärsystem zuständig. Neben dem Zwischenspeichern und Übertragen von Daten ist die Hauptaufgabe des Mini-PS die Benutzerinteraktion. Ereignisse werden an das Mini-PS gemeldet, welches in weiterer Folge den Anwender über das Ereignis informiert. Es bietet eine Benutzerschnittstelle zur Interaktion. Abläufe wie z. B. „VSD lesen" werden über das Mini-PS gestartet.

2.3.4 Management-Modul

Um das Mobile Kartenterminal konfigurieren zu können, ist ein Management-Modul erforderlich. Über dieses können alle Aspekte, auf die ein Administrator oder ein normaler Anwender Einfluss nehmen können muss, erreicht werden. Beispiele hierfür sind das Einspielen einer neuen Firmware und das Einstellen der Systemzeit.

2.3.5 Systemuhr

Das Mobile Kartenterminal muss für die Protokollierung von Zugriffen über eine eigene Systemuhr verfügen.

2.3.6 Erweitertes Display

Im Gegensatz zu einem stationären eHealth-Kartenterminal, welches ein Display vorrangig zur Benutzerführung während der PIN-Eingabe benötigt, müssen an dem Mobilen Kartenterminal umfangreichere Daten angezeigt werden können. Es wird daher

ein entsprechend dimensioniertes Grafikdisplay benötigt, für welches zur Abgrenzung der Begriff des „erweiterten Displays" eingeführt wird.

2.3.7 Drucker

Um VSD einer Karte oder zwischengespeicherte VSD auszudrucken, wird ein Drucker benötigt. Dieser ist in allen Fällen optional.

2.3.8 Ansteuerung externer Komponenten

Die technische Ausprägung der Schnittstelle, über die eine externe Komponente an das Mobile Kartenterminal angebunden wird, ist herstellerspezifisch. Geräte verschiedener Hersteller müssen nicht interoperabel sein. Unter externen Komponenten sind Peripheriegeräte des Mobilen Kartenterminals zu verstehen, wie z. B. ein Drucker oder gegebenenfalls das externe erweiterte Display.

2.3.9 Technische Ausprägungen

2.3.9.1 Einboxlösung

Diese Spezifikation definiert ausschließlich die Anforderungen an eine Einboxlösung, in der die in den Kapiteln 2.3.1 bis 2.3.3 (Mini-AK, Kartenterminal-Modul und Mini-PS) beschriebenen Module eine physikalische Einheit bilden (d. h. sie sind von einem gemeinsamen Gehäuse umgeben).

2.3.9.2 Mehrkomponenten-Lösung

Bei einer Mehrkomponentenlösung bilden die Komponenten keine physikalische Einheit, sondern sind auf getrennten Geräten umgesetzt. Dies bedeutet, dass die Komponenten über externe Schnittstellen miteinander verbunden werden müssen.

2.4 Einbettung in das Anwendungsumfeld

Es ergeben sich folgende Schnittstellen des Mobilen Kartenterminals mit seinem Umfeld:

- Kartenschnittstellen in Form von ID-1-Kontaktiereinheiten, die sich zur Aufnahme von KVKs, eGKs und HBAs eignen. Um den HBA und die Karte des Versicherten (KVK oder eGK) gleichzeitig stecken zu können, verfügt das Mobile Kartenterminal über mindestens 2 ID-1-Kontaktiereinheiten. Das Kartenterminal soll auch Plugin-Karten im ID-000-Format aufnehmen. Plugin-Karten können auch mittels Adapter in einen ID-1-Slot eingebracht werden.
- Das Userinterface bildet eine weitere Schnittstelle. Es ist hauptsächlich auf den Leistungserbringer ausgerichtet, da der Versicherte, abgesehen vom Stecken und Ziehen seiner eGK, nicht in Anwendungsfälle des Mobilen Kartenterminals involviert ist. Das Userinterface bietet die Möglichkeit, Vorgänge zu starten und zu steuern, sich über Fehlerzustände und Ereignisse zu informieren sowie Konfigurationseinstellungen vorzunehmen. PINs werden direkt am PIN Pad des Mobilen Kartenterminals eingegeben.
- Die Host-Schnittstelle dient zur Übertragung der im Mini-PS zwischengespeicherten Daten an das stationäre Primärsystem, wobei die

zwischengespeicherten Daten unverändert an das stationäre PS übertragen werden. Es kommt das CT-API-Protokoll [CT-API] zum Einsatz sowie das in Kapitel 11 beschriebene Übertragungsprotokoll an der Host-Schnittstelle zur Übertragung zwischen Mobilem Kartenterminal und Primärsystem. Eine Übertragung der Daten ist erst nach erfolgreicher Authentifizierung des Arztes möglich. Daten dürfen auch mittelbar über eine Dockingstation an das PS übertragen werden. Die Anforderungen an die Host-Schnittstelle müssen in diesem Fall von der Dockingstation umgesetzt werden.

2.5 Standards und Normen

Die Spezifikation basiert auf der Normenreihe ISO/IEC 7816 für die Chipkartenansteuerung und Chipkartenkommunikation [ISO7816-2], [ISO7816-3] sowie [ISO7816-10], [ISO7816-12].

3 Allgemeine Anforderungen

Dieses Kapitel definiert Anforderungen, die für das Mobile Kartenterminal als Ganzes sowie für alle in dieser Spezifikation spezifizierten Module (Kartenterminal-Modul, Mini-Anwendungskonnektor, Mini-Primärsystem etc.) verbindlich sind. Dies umfasst sowohl die funktionalen und nicht-funktionalen Anforderungen als auch die Sicherheitsanforderungen.

TIP1-A_3738 - Definition Einboxlösung
Der Hersteller des Mobilen Kartenterminals MUSS bei einer Einboxlösung des Mobilen Kartenterminals das Kartenterminal-Modul, den Mini-AK und das Mini-PS innerhalb desselben Gehäuses realisieren, um diese als physikalische Einheit abzubilden.
[<=]

Das erweiterte Display kann extern realisiert werden.

Dies bedeutet auch, dass Anforderungen, die an mehrere Komponenten gestellt werden, im Rahmen einer Einboxlösung einmalig umgesetzt werden können, wobei diese einmalige Umsetzung durch alle Komponenten genutzt werden kann (z. B. Systemuhr, Managementschnittstelle, Firmware Update, Fehleranzeige, Stromquelle, Prüfzeichen, ...).

3.1 Logische und Funktionale Trennung

Damit es nach einer erfolgreichen Evaluierung eines Mobilen Kartenterminals auch weiterhin möglich bleibt, Software oder Daten, die keinen direkten Einfluss auf Sicherheitsfunktionen des Evaluierungsgegenstands (EVG) aufweisen, ohne eine Re-Evaluierung definiert auszutauschen, hinzuzufügen oder zu erweitern, ist eine Separation der Komponenten des EVG anzuraten.

Implementiert der Hersteller keine bzw. nicht ausreichende Separationsmechanismen, so ist bei bestimmten Update-Arten von einer aufwändigen Re-Evaluierung des entsprechenden EVGs auszugehen. Die Separation dient also der Trennung zwischen ausführbarem Code des EVG, welcher Sicherheitsfunktionen umsetzt, und zusätzlichem ausführbarem Code auf dem Mobilen Kartenterminal, welcher keine Sicherheitsfunktionen umsetzt.

Die Wahl der Separationsmechanismen steht dem Hersteller frei und muss in den Sicherheitsvorgaben für den EVG beschrieben und als solcher evaluiert werden. Aus diesen Sicherheitsvorgaben ergibt sich auch, welche Update-Arten bei welchen Separationsmechanismen eine Re-Evaluierung des EVG erfordern und wie aufwändig diese Re-Evaluierung ausfällt.

Die funktionale und logische Trennung bezieht sich daher nicht auf die physische Ausprägung (d. h. sie schließt keine gemeinsame Nutzung von Hardwarekomponenten, Klassen oder Bibliotheken aus).

3.2 Integration in die Telematikinfrastruktur

Es ist keine Online-Anbindung bzw. keine Anbindung an einen stationären Konnektor vorgesehen.

3.3 Physikalische Anforderungen

3.3.1 EMV-Prüfung

Seit 01.01.1996 ist die EU-Richtlinie EMV (89/336/EWG) auf elektrische und elektronische Produkte anzuwenden, welche durch die Richtlinie (2004/108/EG) ersetzt wurde.

TIP1-A_5014 - EMV-Prüfung
Das mobile Kartenterminal MUSS die Anforderungen der gültigen EU-Richtlinie über die elektromagnetische Verträglichkeit erfüllen.
[<=]

In Deutschland ist die EU-Richtlinie EMV umgesetzt durch das EMVG (Gesetz über die elektromagnetische Verträglichkeit von Geräten). Die CE-Kennzeichnung erfordert die Einhaltung des EMVG.

Der Nachweis der Einhaltung der Schutzanforderung erfordert die Prüfung durch ein akkreditiertes Prüflabor. Die Ergebnisse sind durch geeignete Prüfprotokolle nachzuweisen.

3.3.2 Vibrationstest

TIP1-A_4947 - Vibrationstests I
Jede physische Komponente des Mobilen Kartenterminals MUSS den folgenden Normen entsprechen:

- Schwingen DIN EN 60068 T2-6/6.90
- Vibration DIN EN 60068 T2-27/8.29
- Dauerschock DIN EN 60068 T2-29/8.29

[<=]

TIP1-A_5373 - Vibrationstests II, Falltest
Jede physische Komponente des Mobilen Kartenterminals SOLL der folgenden Norm entsprechen:

- Falltest DIN EN 60068-2-32

[<=]

Nur bei Geräten, die auf Basis eines migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 zugelassen werden, kann auf eine Umsetzung verzichtet werden.

3.3.3 Klima

TIP1-A_3805 - Umweltanforderungen für den Einsatz in mobilen Szenarien bei Lagerung
Jede physische Komponente des Mobilen Kartenterminals DARF durch eine Lagertemperatur von -20°C bis 60°C und einer relativen Luftfeuchtigkeit von 5% bis 95% NICHT defekt werden.
[<=]

TIP1-A_3712 - Umweltanforderungen für den Einsatz in mobilen Szenarien
Das Mobile Kartenterminal MUSS mindestens im Bereich der Raumtemperatur von 0°C bis 40°C funktionieren.
[<=]

Geprüft wird nach der Normenreihe DIN IEC 68.

3.3.4 Stromversorgung

TIP1-A_3802 - Mobile Szenarien: Interne Stromquelle
Das Mobile Kartenterminal MUSS über eine interne Stromquelle verfügen, die austauschbar oder wiederaufladbar sein MUSS.
[<=]

Das Mobile Kartenterminal kann zusätzlich den Betrieb über eine externe Stromquelle unterstützen.

TIP1-A_7033 - Austauschbare Pufferbatterien
Verbaut der Hersteller des mobilen Kartenterminals nicht wiederaufladebare Batterien im Mobilen Kartenterminal, so SOLL das Mobile Kartenterminal deren Austauschbarkeit durch den Benutzer ermöglichen.
Hierzu zählen auch interne Stromquellen wie Pufferbatterien gemäß [TIP1-A_4412] oder [TIP1-A_3709].
[<=]

Nur bei Geräten, die auf Basis eines migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 zugelassen werden, kann auf eine Umsetzung verzichtet werden.

TIP1-A_7034 - Stromloser Zustand – Verlust der Uhrzeit und Übertragung von Daten
Hat das Mobile Kartenterminal durch einen stromlosen Zustand beim Wechsel der Pufferbatterie gemäß [TIP1-A_7033] die eingestellte Uhrzeit verloren und sind im Zwischenspeicher des Mobilen Kartenterminals VSD gemäß [VSDM-A_2876] gespeichert, MUSS das mobile Kartenterminal ausschließlich die Übertragung der VSD über die Hostschnittstelle oder das Löschen der im Zwischenspeicher gespeicherten VSD erlauben. Unabhängig davon MUSS das Mobile Kartenterminal einen Werksreset ermöglichen. Das mobile Kartenterminal MUSS den Benutzer auf diesen Umstand hinweisen.
[<=]

TIP1-A_7035 - Stromloser Zustand – Einstellen der Uhrzeit
Hat das mobile Kartenterminal durch einen stromlosen Zustand beim Wechsel der Pufferbatterie gemäß [TIP1-A_7033] die eingestellte Uhrzeit verloren und sind im Zwischenspeicher des Mobilen Kartenterminals keine VSD gespeichert, MUSS das Mobile Kartenterminal das Lesen von Daten einer eGK verhindern bis die Uhrzeit durch den Administrator eingestellt wurde. Das mobile Kartenterminal MUSS den Benutzer auf diesen Umstand hinweisen.
[<=]

TIP1-A_3847 - Mobile Szenarien: Betriebsdauer mittels interner Stromquelle
Das Mobile Kartenterminal SOLL mit seiner internen Stromquelle den Betrieb mindestens 6h aufrecht erhalten können.
[<=]

TIP1-A_3803 - Mindestdauer der Standbyzeit für Mobile Kartenterminals
Das Mobile Kartenterminal SOLL eine Standbyzeit von mindestens 300h sicherstellen.
[<=]

3.3.5 Transportierbarkeit

TIP1-A_3713 - Transportierbarkeit für den Einsatz in mobilen Szenarien
Das Mobile Kartenterminal MUSS in jeder Ausprägung weniger als 0,7 Kilo wiegen und ein Volumen kleiner als 1 dm^3 aufweisen.
[<=]

3.3.6 Schnittstelle zum Primärsystem

TIP1-A_3689 - Lokaler Anschluss zur Übertragung an das HOST-System
Das Mobile Kartenterminal MUSS über mindestens einen lokalen Anschluss zur Übertragung der zwischengespeicherten Daten an das Primärsystem verfügen.
[<=]

TIP1-A_3690 - mobile Szenarien: Datenübertragung an das Primärsystem mittels Dockingstation
Die Dockingstation des Mobilen Kartenterminals MUSS, wenn das Mobile Kartenterminal diese zur Übertragung der zwischengespeicherten Daten benötigt, über einen lokalen Anschluss an das Primärsystem verfügen.
[<=]

3.3.7 Gehäuse

3.3.7.1 Versiegelung

Aufgrund des hohen Schutzbedarfs der verarbeiteten Daten und der hohen Anforderungen an die zuverlässige Durchführung der Abläufe müssen entsprechend wirkungsvolle Mechanismen zum Schutz der Integrität des Mobilen Kartenterminals angewendet werden. Die entsprechenden Anforderungen an das Gehäuse und dessen Versiegelung sind dem PP [BSI-CC-PP-0052] zu entnehmen.

3.3.7.2 Prüfzeichen

Die Berechtigung zur Nutzung des Prüfzeichens durch den Hersteller erfolgt mit der Zulassung der Geräte durch die gematik. Im Rahmen des Zulassungsverfahrens werden dem Hersteller alle Versionen des gematik-Prüfzeichens als Bilddateien in geeigneter Auflösung zur Verfügung gestellt.

Das Prüfzeichen bietet einen Wiedererkennungswert für zugelassene Mobile Kartenterminals, es sind keine Sicherheitsfunktionen damit verbunden.

TIP1-A_4406 - Spezifizierung gematik-Prüfzeichen
Das Mobile Kartenterminal MUSS auf dem Gehäuse über ein gematik-Prüfzeichen verfügen, welches nicht unbeschadet ablösbar sein darf.
[<=]

TIP1-A_4407 - Anbringung gematik-Prüfzeichen
Der Hersteller des Mobilen Kartenterminals MUSS das gematik-Prüfzeichen an einer während der PIN-Eingabe für den Benutzer gut sichtbaren Stelle am mobilen Kartenterminal aufbringen.
[<=]

TIP1-A_4408-01 - Optische Gestaltung des Prüfzeichens
Der Hersteller des mobilen eHealth-Kartenterminals MUSS eine der abgebildeten Varianten als Prüfzeichen verwenden und sicherstellen, dass die optische Gestaltung des Prüfzeichens den folgenden Vorgaben entspricht:

- Die Mindesthöhe des Prüfzeichens (exklusiv Schutzbereich) beträgt 10 mm.
- Das Seitenverhältnis des Prüfzeichens ist Breite/Höhe = 2,7/1.
- Die Farbgebung des Prüfzeichens ist einfarbig auf transparentem oder kontrastfarbigem Grund.
- Der einfarbige Schriftzug muss in einer der folgenden Farben ausgeführt sein:
  - schwarz (RGB: 0, 0, 0)
  - dunkelblau (RGB: 0, 14, 82)
  - weiß (RGB: 255, 255, 255)
- Der Hintergrund muss transparent oder mit einer Kontrastfarbe versehen sein:
  - weiß (RGB: 255, 255, 255) für schwarzen und blauen Schriftzug
  - schwarz (RGB: 0, 0, 0) für weißen Schriftzug
  - dunkelblau (RGB; 0, 14, 82) für weißen Schriftzug
- An allen vier Seiten des Prüfzeichens ist ein Schutzbereich vorzusehen. Dieser Bereich ist grundsätzlich frei zu halten von Objekten oder Beschriftungen.
- Der Schutzbereich wird durch die Größe des Prüfzeichens definiert und entspricht umlaufend der Höhe des Buchstaben "Z" im Schriftzug "Zugelassen".
- Das Prüfzeichen muss bei vorgesehener Verwendung des mobilen Kartenterminals durch einen Benutzer waagerecht orientiert sein.



zulässige Varianten des Prüfzeichens und Darstellung des Schutzbereichs

[<=]

3.4 Betriebsanforderungen

3.4.1 Wartbarkeit

Das Mobile Kartenterminal wird in der Regel in einem Umfeld mit geringer Betriebsführungsintensität betrieben. Es ist daher wartungsarm auszulegen. Das Mobile Kartenterminal hat einen, bis auf das Einspielen von Firmware Updates sowie ein eventuelles Nachladen oder Austauschen der internen Stromquelle, wartungsfreien Betrieb zu erlauben.

3.4.2 Anzeige des Betriebszustandes

TIP1-A_3696 - Mobile Szenarien, Betriebsbereitschaft: Anzeige der Betriebsbereitschaft im Rahmen der Benutzerführung
Das Mobile Kartenterminal MUSS seine Betriebsbereitschaft anzeigen.
[<=]

Eine Anzeige des Standby-Modus ist nicht erforderlich.

TIP1-A_4260 - Mobile Szenarien: Anzeige der Fehlerzustände
Das Mobile Kartenterminal MUSS Fehlerzustände, die im Rahmen der Betriebsbereitschaft auftreten, anzeigen.
[<=]

3.4.3 Betriebssicherheit

Das Mobile Kartenterminal darf nur in den Verkehr gebracht werden, wenn Sicherheit und Gesundheit von Anwendern nicht gefährdet werden. Dazu muss der Anwender der Produkte über alle Sicherheitsinformationen zum Produkt informiert werden. Auch muss der Hersteller den Lebenszyklus seines Produktes beobachten und bei bekannt gewordenen Mängeln die zuständige Behörde informieren und gegebenenfalls einen Rückruf einleiten. Das Mobile Kartenterminal muss den Anforderungen aus dem Produktsicherheitsgesetz (PRODSG) [PRODSG] entsprechen. Darüber hinaus kann die Betriebssicherheit des Mobilen Kartenterminals durch ein Prüfzeichen (z. B. VDE, GS) nachgewiesen werden.

3.4.4 Zuverlässigkeit

Zuverlässigkeitsaspekte sind Differenzierungsmerkmale verschiedener Produkte und Hersteller. Durch die hohe Anzahl von Steckzyklen und die häufige Nutzung unterliegen die Mobilen Kartenterminals im Gesundheitssystem anderen Beanspruchungen als Consumer-Geräte. Dies ist zu berücksichtigen.

TIP1-A_3800 - Mobile Szenarien: Haltbarkeit der Geräte
Das Mobile Kartenterminal MUSS bei 24/7-Betrieb eine Mean Time Between Failures (MTBF) von mindestens 3 Jahren bzw. 100.000 Steckzyklen gewährleisten.
[<=]

TIP1-A_3801 - Mobile Szenarien: Zuverlässigkeitsprognose der Geräte
Der Hersteller des Mobilen Kartenterminals MUSS eine nachvollziehbare Zuverlässigkeitsprognose für das Mobile Kartenterminal mit Darstellung der zugrunde gelegten Ausfallraten und Stückzahlen der Bauelemente und der anderen

zuverlässigkeitsrelevanten Elemente (Lötstellen, Leiterbahnen, etc.) bereitstellen. Hat der Hersteller in dieser Zuverlässigkeitsprognose Schätzungen verwendet, MUSS er diese erläutern.
[<=]

3.4.5 Fehlertoleranz

TIP1-A_4275 - Überbrücken von Fehlerzuständen bei der Kartenkommunikation
Das Mobile Kartenterminal MUSS transiente bzw. überbrückbare Fehlerzustände bei der Kartenkommunikation erkennen und automatisch bereinigen.
[<=]

Insbesondere, aber nicht ausschließlich, bezieht sich dies auf die Resynchronisation der Kartenkommunikation.

TIP1-A_3698 - Anzeige von Bedienfehlern und ungültigen Eingaben am Mobilen KT
Das Mobile Kartenterminal MUSS Bedienfehler und ungültige Eingaben anzeigen oder ignorieren.
[<=]

TIP1-A_3711 - Blockieren von ungültigen und fehlerhaften Kommandos
Das Mobile Kartenterminal MUSS fehlerhafte oder ungültige Kommandos erkennen und abweisen.
[<=]

3.4.6 Auslieferungszustand

TIP1-A_3766 - mobKT Werkszustand - Kennwörter
Das Mobile Kartenterminal MUSS im Auslieferungszustand leere/ungesetzte Kennwörter besitzen. Wird zur Umsetzung des weiteren Werksreset-Mechanismus gemäß [TIP1-A_5427] die im Protection Profile [BSI-CC-PP-0052] beschriebene und im Auslieferungszustand bereits gesetzte TOE Reset PIN implementiert, bleibt diese hiervon unberührt.
[<=]

TIP1-A_3767 - mobKT Werkszustand - erlaubte Funktion
Das Mobile Kartenterminal MUSS im Auslieferungszustand sicherstellen, dass ohne vorheriges Setzen des Administratorenpasswortes keine weitere Funktion angeboten wird.
[<=]

TIP1-A_3870 - mobKT im Werkszustand erlaubte Funktion
Das Mobile Kartenterminal MUSS sicherstellen, dass es im Auslieferungszustand, also wenn das Administratorenpasswort noch nicht gesetzt ist, nicht möglich ist, Daten einer eGK einzulesen und zu speichern.
[<=]

3.4.7 Werksreset

TIP1-A_4954 - Möglichkeit zum Werksreset
Das Mobile Kartenterminal MUSS über eine Möglichkeit zum Werksreset verfügen.
[<=]

TIP1-A_3761 - Definition Werksreset
Das Mobile Kartenterminal MUSS bei einem Werksreset die Konfigurationen wieder in den Auslieferungszustand setzen, nicht jedoch die Firmware und die Firmware-Gruppe.
[<=]

TIP1-A_4955 - Werksreset Administrator
Das Mobile Kartenterminal MUSS die Möglichkeit zum Werksreset gemäß [TIP1-A_4954] ausschließlich dem Administrator zur Verfügung stellen.
[<=]

TIP1-A_5427 - Weiterer Mechanismus für Werksreset
Der Hersteller des Mobilen Kartenterminals MUSS für den Werksreset neben [TIP1-A_4955] einen weiteren Mechanismus zur Durchführung anbieten, welcher die Arbeitsabläufe beim Leistungserbringer nur minimal unterbricht.
[<=]

TIP1-A_5428 - Authentisierung für weiteren Werksreset Mechanismus
Das Mobile Kartenterminal MUSS sicherstellen, dass der Mechanismus gemäß [TIP1-A_5427] ausschließlich nach Authentisierung durch eine Kombination aus Username und Passwort oder einen mindestens gleich starken Mechanismus ausgeführt werden kann.
[<=]

TIP1-A_5429 - Dokumentation Werksreset Mechanismus
Der Hersteller des Mobilen Kartenterminals MUSS die Umsetzung von [TIP1-A_5427] in der Benutzerdokumentation beschreiben und die aus Sicht des Anwenders notwendigen Schritte verständlich darstellen.
[<=]

TIP1-A_5430 - Ausführung eines Werksreset ohne Authentisierung
Der Hersteller des Mobilen Kartenterminals KANN einen zusätzlichen Werksreset-Mechanismus ohne vorherige Authentisierung implementieren (d.h. der Werksreset ist von jeder Person ausführbar).
[<=]

TIP1-A_5431 - Aktivierung/Deaktivierung des Werksreset ohne Authentisierung
Falls der zusätzliche Werksreset-Mechanismus ohne Authentisierung gemäß [TIP1-A_5430] implementiert wird, MUSS das Mobile Kartenterminal ausschließlich dem Administrator die Aktivierung und Deaktivierung dieses Mechanismus ermöglichen.
[<=]

TIP1-A_5432 - Standardeinstellung Werksreset ohne Authentisierung
Falls der zusätzliche Werksreset-Mechanismus ohne Authentisierung gemäß [TIP1-A_5430] implementiert wird, MUSS das Mobile Kartenterminal diesen Mechanismus als Standardeinstellung deaktivieren.
[<=]

Wenn der Werksreset-Mechanismus ohne vorherige Authentisierung implementiert und aktiviert ist, kann der Anwender im Einzelfall wählen, welchen der Werksreset-Mechanismen (authorisiert oder unauthorisiert) er ausführen möchte.

TIP1-A_3869 - Werksreset nicht dauerhaft unausführbar
Das Mobile Kartenterminal DARF durch einen Werksreset bei sachgemäßer Handhabung und ohne technisches Versagen NICHT einen Zustand annehmen, der einen erneuten Werksreset unausführbar macht. Der Auslieferungszustand für das Administratorenpasswort gemäß [TIP1-A_3767] bleibt hiervon unberührt.
[<=]

Die Umsetzung des Werksreset-Mechanismus ist herstellerspezifisch.

TIP1-A_3748 - mobile Szenarien: Löschen des Zwischenspeichers bei Rücksetzen auf Werkseinstellungen
Das Mobile Kartenterminal MUSS sicherstellen, dass beim Rücksetzen des Mobilen Kartenterminals in den Auslieferungszustand alle Daten im Zwischenspeicher gelöscht werden.
[<=]

3.4.8 Firmware Update

TIP1-A_3743 - Sicherer Firmware-Update-Mechanismus
Das Mobile Kartenterminal MUSS über eine gesicherte Update-Möglichkeit seiner Firmware verfügen.
[<=]

TIP1-A_3744 - Erkennung von Übertragungsfehlern während des Firmware Updates
Das Mobile Kartenterminal MUSS beim Firmware Update selbständig Übertragungsfehler und nicht authentische Übertragungen erkennen.
[<=]

TIP1-A_3839 - Manipulationsgeschützte Speicherung des Sicherheitsattributes für die Sicherung des FW- Updates
Das Mobile Kartenterminal MUSS das zur Erkennung von Übertragungsfehlern und nicht authentischen Übertragungen notwendige Sicherheitsattribut für Firmware Updates in einem manipulationsgeschützten Bereich des Gerätes ablegen.
[<=]

Das Verwaltungsverfahren muss mindestens den Anforderungen entsprechen, die in der Sicherheitsevaluierung und dem zugehörigen Protection Profile sowie den Sicherheitszielen zu Grunde gelegt werden.

TIP1-A_3747 - Mobile Szenarien, Firmware Update: Zulässige Verfahren zur Sicherung des FW-Updates
Das Mobile Kartenterminal MUSS sicherstellen, dass die Aktualisierung der Firmware mittels asymmetrischer kryptographischer Verfahren geschützt wird.
[<=]

Festlegungen zu zulässigen kryptographischen Verfahren werden in [gemSpec_Krypt] getroffen. Konkret wird nur eine Sicherung der Authentizität und Integrität gewährleistet werden. Dies ist durch eine Signatur durch den Hersteller zu gewährleisten. Die Signatur durch den Hersteller dient dazu sicherzustellen, dass bei der Übermittlung und den anschließenden Prüf- und Verarbeitungsschritten innerhalb der prüfenden und zulassenden Stelle keine beabsichtigten oder unbeabsichtigten Verfälschungen der Firmware („Bitdreher") auftreten können. Das Format der Firmware (d. h. des Binärfiles) bleibt herstellerspezifisch.

TIP1-A_3746 - Mobile Szenarien, Firmware Update: Verantwortlichkeit der Prüfung der neuen Firmware
Das Mobile Kartenterminal MUSS sicherstellen, dass die aktive Firmware, die auch die öffentlichen Schlüssel für die Signaturprüfung enthalten MUSS, die einzuspielende Firmware-Version prüft.
[<=]

Ein Wechsel des Schlüsselmaterials ist damit über die Einbeziehung einer neuen Schlüsselgeneration in die Firmware möglich. Auch ist es zulässig (und sogar empfohlen), dass eine Firmware nur die öffentlichen Schlüssel einer übergeordneten CA enthält und

das konkrete Zertifikat zur Signatur in das bzw. an das Signaturenvelope ein- bzw. angefügt wird.

TIP1-A_3699 - Versionierung der Firmware
Das Mobile Kartenterminal MUSS für jede Firmware-Version des Mobilen Kartenterminals über eine Versionsnummer verfügen.
[<=]

Die Art der Versionierung ist unter der Einhaltung der Vorgaben aus [gemSpec_OM] herstellerspezifisch.

TIP1-A_3700 - Sicherstellung von Authentizität und Integrität eines FW-Updates
Das Mobile Kartenterminal MUSS vor Austausch der Firmware-Version die Authentizität und Integrität des Updatepakets prüfen.
[<=]

TIP1-A_3701 - Übernahme als aktive Firmware
Das Mobile Kartenterminal MUSS sicherstellen, dass die neue Firmware korrekt und vollständig in den Speicher übernommen wurde, bevor die Kennzeichnung als aktive Firmware von der bisherigen auf die neue übernommen wird.
[<=]

3.4.8.1 Konzept der Firmware-Gruppen

Das Konzept der Firmwaregruppen wird in [gemSpec_OM] beschrieben. Über die dortigen Anforderungen hinaus gilt:

TIP1-A_3825 - Ausführen eines zulässigen Downgrades
Der Hersteller des Mobilen Kartenterminals MUSS dafür sorgen, dass der Administrator vor dem Ausführen eines zulässigen Downgrades auf die möglichen Konsequenzen hingewiesen wird - z.B. im Rahmen der Benutzerdokumentation - und die Möglichkeit erhält, den Downgrade-Prozess noch abzubrechen.
[<=]

3.4.9 Produkttypversion und Selbstauskunft

Die Anforderungen bezüglich der Produkttypversion und Selbstauskunft sind in [gemSpec_OM] festgelegt. Hierüber hinaus gilt:

TIP1-A_4273 - Selbstauskunft: Produkt-Versionsstand
Das Mobile Kartenterminal MUSS die Rückgabe der Selbstauskunft über die Administrationsschnittstelle mittels Benutzerschnittstelle ermöglichen.
[<=]

TIP1-A_4274 - Selbstauskunft: Firmware-Gruppen-Version
Das Mobile Kartenterminal MUSS im Zuge der Selbstauskunft die aktuell installierte Firmware-Gruppen-Version darstellen.
[<=]

3.4.10 Kompatibilität zukünftiger Kartenversionen

Im Hinblick auf die Spezifikation zukünftiger Kartenversionen der durch das Mobile Kartenterminal verarbeiteten Kartentypen eGK, HBA und SMC-B ist die gematik auf Informationen der Hersteller angewiesen, ob über die spezifizierten Zugriffe (Verwendung von Kartenkommandos bzw. Zugriffe auf Kartenobjekte) hinaus herstellerspezifisch weitere sicherheitsrelevante Zugriffe erfolgen. Die gematik wird diese Information

zukünftig im Rahmen von Impact-Analysen bei anstehenden Änderungen an den relevanten Kartenspezifikationen nutzen.

TIP1-A_6485 - Mobiles KT: Kompatibilität zukünftiger Kartenversionen
Der Hersteller des Mobilen Kartenterminals MUSS im Rahmen der Zulassung erklären, ob sein Mobiles Kartenterminal über die in Anhang A6 aufgeführten Kartenzugriffe hinaus weitere sicherheitsrelevante Kartenzugriffe vornimmt. Der Hersteller MUSS diese weiteren herstellerspezifischen sicherheitsrelevanten Zugriffe unter Verwendung der in Anhang A6 vorhandenen Tabellenform darstellen.
[<=]

Der Hersteller des mobilen Kartenterminals kann die Informationen über Kartenzugriffe, welche Sicherheitsleistungen im Sinne des [BSI-CC-PP-0052] erbringen, im Rahmen einer Re-Evaluierung bzw. Re-Zertifizierung seines Produktes ebenfalls nutzen. Die für die Sicherheitsleistung des Mobilen Kartenterminals relevanten Zugriffe sind in der Tabelle im Anhang A6 gelistet.

3.5 Sicherheitstechnische Anforderungen

3.5.1 Schutz der KVK

TIP1-A_4973 - Schreibschutz KVK
Das Mobile Kartenterminal DARF NICHT schreibend auf die KVK zugreifen.
[<=]

3.5.2 Schutz der eGK

TIP1-A_3717 - Freischaltung der eGK mittels PIN
Das Mobile Kartenterminal DARF die Freischaltung einer eGK mittels PIN-Eingabe NICHT ermöglichen.
[<=]

TIP1-A_3754 - Schutz vor Kartenzugriff bei Anschluss an das Primärsystem
Das Mobile Kartenterminal MUSS sicherstellen, dass, wenn es unmittelbar oder mittelbar (z. B. über das Mini-PS und den Mini-AK) mit dem stationären Primärsystem verbunden ist, Kartenzugriffe auf gesteckte eGKs oder KVKs nicht möglich sind. Maßgeblich ist hier die physikalische Verbindung (Kabel gesteckt) zwischen dem Mobilen Kartenterminal und einem Hostsystem (einem beliebigen Computer).
[<=]

Wenn das Mobile Kartenterminal bei Auslegung mit USB-Schnittstelle eindeutig erkennen kann, dass es nur zum Laden an einem USB-Ladegerät (nicht Hostsystem) angeschlossen wird, so ist dies zulässig und verletzt die Anforderung [TIP1-A_3754] nicht.

Wenn das Mobile Kartenterminal - beispielsweise bei Verwendung einer seriellen Schnittstelle - die physikalische Verbindung zwischen Mobilem Kartenterminal und Hostsystem nicht erkennen kann, so lässt sich die Anforderung [TIP1-A_3754] wie folgt erfüllen:
Im Mobilen Kartenterminal wird die Schnittstelle zum Hostsystem derart gestaltet, dass sie durch den Nutzer softwaretechnisch per Schalter aktivierbar und deaktivierbar ist. Wenn die Schnittstelle aktiviert ist, darf das Mobile Kartenterminal einen Zugriff auf gesteckte eGKs oder KVKs nicht ermöglichen. Ist die Schnittstelle zum Hostsystem deaktiviert, darf das Mobile Kartenterminal einen Zugriff über die Schnittstelle vom Hostsystem aus nicht ermöglichen.

3.5.3 Vertraulichkeit

Das mobile Kartenterminal vermittelt Daten mit medizinischen und personenbezogenen Inhalten. Diese haben einen hohen oder sehr hohen Schutzbedarf und es muss daher sichergestellt werden, dass sie nur im Rahmen der explizit vorgesehenen und beschriebenen Verfahren preisgegeben werden. Die Maßnahmen zum Schutz von diesen Informationsobjekten mit hohem und sehr hohem Schutzbedarf (z. B. PINs, Schlüssel, medizinische Daten) drücken sich im PP des Mobilen Kartenterminals in organisatorischen Anforderungen der Einsatzumgebungen und sicherheitstechnischen Maßnahmen des Mobilen Kartenterminals aus.

3.5.4 Lebensdauer sensibler Daten

TIP1-A_3852 - Lebensdauer sensibler, medizinischer Daten
Das Mobile Kartenterminal MUSS nach Abschluss jedes Prozessschrittes, bei dem sensible Daten wie VSD oder PINs verarbeitet werden, diese sensiblen Daten aus seinem Arbeitsspeicher unwiderruflich entfernen.
[<=]

3.5.5 Protokollierung des Zugriffs

Nach Vorgabe des [SGB V §291a] sind Protokollierungen des Zugriffs auf Daten durchzuführen.

Der Mini-AK muss für bestimmte Aktionen Protokolleinträge auf die eGK schreiben. Das Format der Protokolleinträge ist in Kapitel 10.1.8 beschrieben.

TIP1-A_4948 - Ausprägung des Zugriffsprotokolls
Der Hersteller des Mobilen Kartenterminals MUSS es ermöglichen, dass bei Zugriffen von Personen nach Absatz 4 Satz 1 Nr. 1 [SGB V §291a] Buchstabe d und e sowie Nummer 2 Buchstabe d und e, die über keinen elektronischen Heilberufsausweis oder entsprechenden Berufsausweis verfügen, nachweisbar in elektronischer Form außerhalb des Mobilen Kartenterminals protokolliert werden kann, wer auf die Daten zugegriffen hat und von welcher Person, die über einen elektronischen Heilberufsausweis oder entsprechenden Berufsausweis verfügt, die zugreifende Person autorisiert wurde.
[<=]

Beim in der obigen Anforderung genannten Personenkreis handelt es sich um Personen, die nicht über einen eigenen elektronischen Heilberufsausweis verfügen. In diesem Fall ist als berechtigte Karte eine Institutionskarte SMC-B im mobilen Kartenterminal vorhanden. Auf einer verarbeiteten eGK wird in einem solchen Fall protokolliert, mit welcher SMC-B zugegriffen wurde, nicht aber, welche Person zugegriffen hat. Diese Information muss außerhalb der verarbeiteten eGK und letztendlich außerhalb des mobilen Kartenterminals protokolliert werden, damit dieses Protokoll nicht bei Verlust des Geräts ebenfalls verloren geht.

Der Hersteller kann hier unterstützend eine technische Lösung implementieren. Es kann aber auch durch organisatorische Maßnahmen beim Leistungserbringer sichergestellt werden, dass zu jedem Zeitpunkt in elektronischer Form nachvollziehbar ist, welche Person auf die Daten zugegriffen hat und durch wen sie autorisiert wurde. Der Hersteller muss in der Dokumentation entsprechende Möglichkeiten beschreiben.

TIP1-A_4949 - Beschreibung des Verfahrens für das Zugriffsprotokoll
Der Hersteller des Mobilen Kartenterminals MUSS das Verfahren gemäß [TIP1-A_4948] in der Benutzerdokumentation beschreiben.
[<=]

3.5.6 Anschluss weiterer Komponenten

TIP1-A_4405 - Sicherheit bei Anschluss externer Komponenten
Der Hersteller des Mobilen Kartenterminals MUSS sicherstellen, dass eventuell angeschlossene externe Komponenten die Sicherheit des Mobilen Kartenterminals nicht nachteilig beeinflussen.
[<=]

4 Anforderungen an das Kartenterminal-Modul

Dieses Kapitel beschreibt die zu erfüllenden funktionalen und nicht-funktionalen Anforderungen an das Kartenterminal-Modul.

4.1 Display und PIN Pad

TIP1-A_3715 - Display zur Anzeige am Mobilen KT
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS über ein Display verfügen.
[<=]

TIP1-A_3867 - Mobile Szenarien: Am Display darstellbare Zeichen
Das Display des mobilen Kartenterminal MUSS mindestens zwei Zeilen á 16 Zeichen ISO646DE-Text darstellen können.
[<=]

Die Fähigkeit zur Anzeige von weiteren Sonderzeichen ist erlaubt.

TIP1-A_3716 - PIN Pad zur PIN-Eingabe am Mobilen KT
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS über ein PIN Pad oder eine vergleichbare Eingabeeinheit, welche sich zur Eingabe einer numerischen PIN und zur damit verbundenen Authentisierung eignet, verfügen.
[<=]

Weitere Sensoren/Eingabeeinheiten können im Kartenterminal-Modul vorgesehen sein.

Das Kartenterminal-Modul kann statt eines eigenen Displays auch das erweiterte Display nachnutzen. Siehe hierzu Kapitel 8.2 [TIP1-A_4425].

4.2 PIN-Eingabe und PIN-Änderung

Die Mechanismen zum Schutz der PIN ergeben sich aus den Festlegungen zum Angriffspotential sowie des EAL (Evaluation Assurance Level. In der Common Criteria definierte Vertrauenswürdigkeitsstufen, EAL 1-7), welche im zugehörigen Protection Profile getroffen werden.

TIP1-A_3861 - Mobiles KT: Vorgaben zum Kommando SICCT PERFORM VERIFICATION
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS für die PIN-Eingabe die Vorgaben zum Kommando SICCT PERFORM VERIFICATION (siehe [SICCT#5.19.1,5.19.2]) - außer für die Dauer der Wartezeiten bei der PIN-Eingabe - umsetzen.
[<=]

TIP1-A_3862 - Mobiles KT: Timeout bei der PIN-Eingabe (erstes Zeichen)
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS bei der PIN-Eingabe - abweichend von [SICCT#5.19.2] - standardmäßig 30 Sek. (statt 15 Sek. laut SICCT) auf die Eingabe des ersten Zeichens oder die Betätigung der Abbruchtaste warten.
[<=]

TIP1-A_3863 - Mobiles KT: Timeout bei der PIN-Eingabe (weitere Zeichen)
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS - abweichend von [SICCT#5.19.2] - standardmäßig 30 Sek. (statt 5 Sek. laut SICCT) auf die Eingabe des

jeweils nächsten Zeichens oder die Betätigung der Abbruch- bzw. Bestätigungstaste warten.
[<=]

TIP1-A_3864 - Mobiles KT: Vorgaben zum Kommando SICCT MODIFY VERIFICATION
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS für die PIN-Änderung die Vorgaben zum Kommando SICCT MODIFY VERIFICATION (siehe [SICCT#5.20.1,5.20.2]) - außer für die Wartezeiten bei der PIN-Änderung – umsetzen.
[<=]

TIP1-A_3865 - Mobiles KT: Timeout bei der PIN-Änderung (erstes Zeichen)
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS bei der PIN-Eingabe - abweichend von [SICCT#5.20.2] - standardmäßig 30 Sek. (statt 15 Sek. laut SICCT) auf die Eingabe des ersten Zeichens oder die Betätigung der Abbruchtaste warten.
[<=]

TIP1-A_3866 - Mobiles KT: Timeout bei der PIN-Änderung (weitere Zeichen)
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS - abweichend von [SICCT#5.20.2] - standardmäßig 30 Sek. (statt 5 Sek. laut SICCT) auf die Eingabe des jeweils nächsten PIN-Zeichens oder die Betätigung der Abbruch- bzw. Bestätigungstaste warten.
[<=]

TIP1-A_3806 - Bestätigung der PIN-Eingabe am Mobilen KT
Das Mobile Kartenterminal MUSS sicherstellen, dass, unabhängig davon ob es sich um eine Eingabe von einer PIN mit variabler oder fixer Länge handelt, die Eingabe der PIN durch Drücken einer „Enter"-Taste (dies legt nicht die Beschriftung dieser Taste, sondern lediglich ihre Funktion bei der PIN-Eingabe fest) bestätigt werden muss.
[<=]

TIP1-A_4976 - Enter-Taste bei bekannter PIN-Länge
Das Mobile Kartenterminal DARF bei bekannter PIN-Länge und falls diese unterschritten wird, die "Enter"-Taste NICHT akzeptieren.
[<=]

Siehe hierzu Abbildung 3 Pic_MOKT_0023 Verhalten bei PIN-Eingabe mit bekannter Länge.

TIP1-A_4958 - Abbruchtaste bei PIN-Eingabe
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS dem Benutzer die Möglichkeit bieten, die PIN-Eingabe jederzeit mittels Drücken einer "Abbruch"-Taste abbrechen zu können.
[<=]

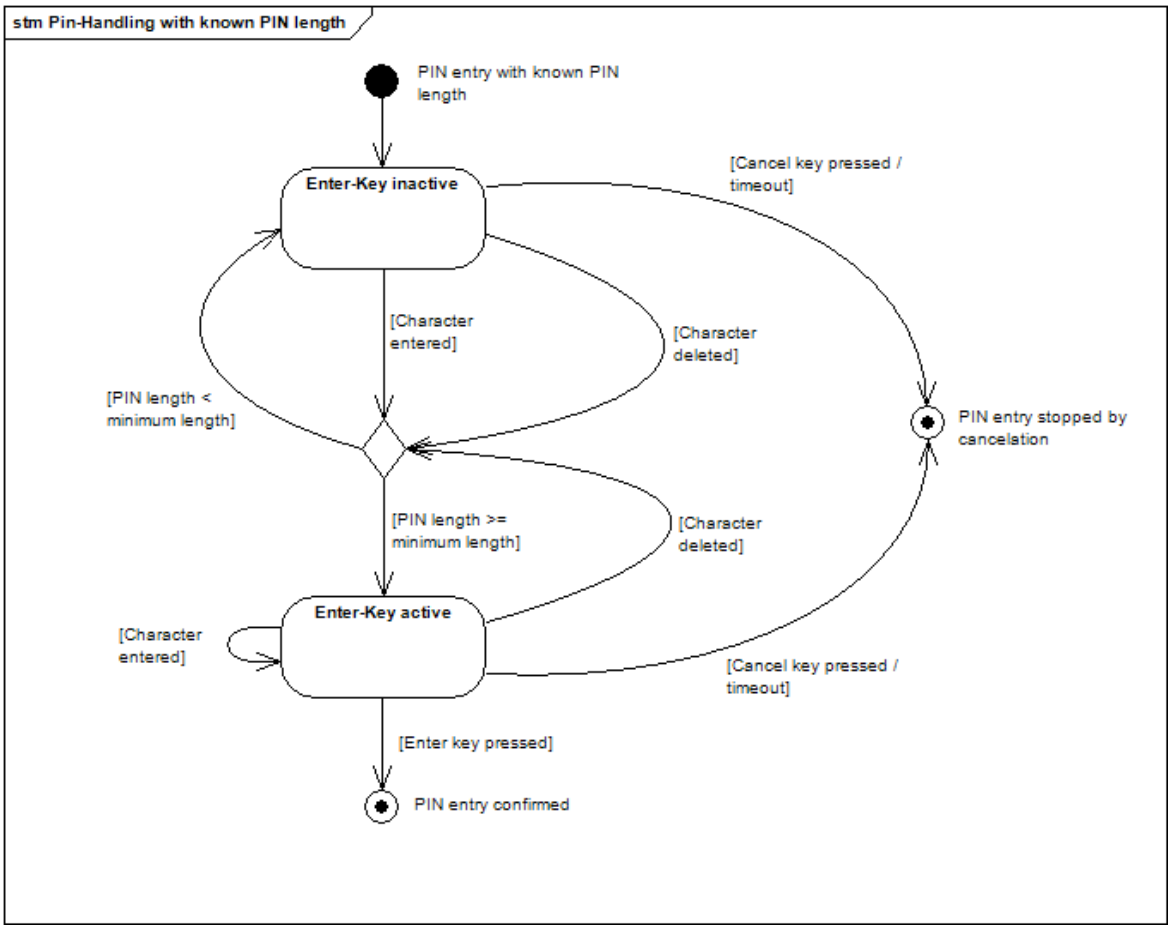


Abbildung 2: Pic_MOKT_0023 Verhalten bei PIN-Eingabe mit bekannter Länge

TIP1-A_4922 - Mobiles KT: sicherer Modus
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS sich im Betrieb immer im sicheren Modus befinden, der sicherstellt, dass eine PIN über keine andere Schnittstelle als die zu der Karte, die für die PIN-Eingabe vorgesehen ist, übertragen wird und nicht zwischengespeichert, dupliziert oder manipuliert werden kann.
[<=]

Eine Anzeige des sicheren Modus ist nicht erforderlich.

TIP1-A_3875 - Freischaltung der berechtigten Karte mittels PIN
Das Mobile Kartenterminal MUSS es dem Leistungsbringer ermöglichen, den HBA und die SMC-B mittels PIN-Eingabe am Kartenterminal-Modul des Mobilen Kartenterminals freizuschalten.
[<=]

4.3 Zugriffsanzeige

TIP1-A_3799 - Signalisieren der Kartenzugriffe
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS bei Kartenzugriffen (Lesen, Schreiben, Operationszugriffe) den Umstand, dass auf eine Karte zugegriffen wird, für die gesamte Dauer des Zugriffs für den Benutzer gut sichtbar anzeigen, z.B. mittels einer

LED, die bei Kartenzugriffen blinkt.
[<=]

Es ist nicht erforderlich, Zugriffe für jede Karte separat anzuzeigen.

Das Kartenterminal-Modul kann hierzu auch das erweitere Display nachnutzen.

4.4 Performanz

TIP1-A_4423 - Übertragungsraten zu den Chipkarten
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS die Übertragungsraten zu den Chipkarten gemäß den technischen Spezifikationen ([KVK], [eGK], [HBA] und [SMC-B]), unterstützen.
[<=]

4.5 Kartenorientierte Anforderungen

Die Beschreibung der Kartenschnittstelle ist auf den Einsatz kontaktbehafteter Gesundheitskarten abgestimmt. Die Basis für alle Anforderungen ist die internationale Normenreihe ISO/IEC 7816. Die technischen Anforderungen an die Chipkartenschnittstelle sind in der SICCT-Spezifikation [SICCT] beschrieben.

TIP1-A_4946 - Umsetzung der Chipkartenschnittstelle entsprechend [KVK], [HBA], [SMC-B] und [eGK]
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS die Karten:KVK [KVK], HBA [HBA], SMC-B [SMC-B] und eGK [eGK] unterstützen.
[<=]

4.5.1 Stromversorgung der Chipkarten

Das Kartenterminal-Modul bedient in erster Linie ISO/IEC-kompatible Chipkarten und daher ist der Standard ISO/IEC 7816-3 [ISO7816-3] maßgeblich.

TIP1-A_4401 - Dauerhafte Stromversorgung der gesteckten Chipkarte(n)
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS während des Betriebs eine dauerhafte Stromversorgung der Chipkarte(n) mit dem Maximalstrom nach den derzeit gültigen internationalen Standards ([ISO7816-3]) gewährleisten.
[<=]

Dabei ist zu beachten, dass Chipkarten kurzzeitig auch einen höheren Stromverbrauch haben können.

TIP1-A_4411 - Kurzzeitig höherer Strombedarf von Chipkarten (Spike)
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS bei kurzzeitig höherem Stromverbrauch der Chipkarten (Spike gemäß [ISO7816-3]) die volle Funktionsfähigkeit des Kartenterminal-Moduls gewährleisten.
[<=]

TIP1-A_3765 - Mobiles KT: Karten-Versorgungsspannung
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS einer Karte die im Rahmen der ATR-Prozedur ausgehandelte Versorgungsspannung in folgender Reihenfolge (absteigend) anbieten:

1. 5V (verpflichtend)

2. 3V (verpflichtend)
3. 1,8V (optional).

[<=]

4.5.2 Anzahl Kontaktiereinheiten

TIP1-A_3718 - Mindestanzahl der Kontaktiereinheiten am mobilen Kartenterminal
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS über zwei Kontaktiereinheiten zur Aufnahme von Chipkarten im ID-1-Format verfügen.
[<=]

TIP1-A_3719 - Mindestanzahl gleichzeitig aufnehmbarer ID-1-Karten
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS zwei Karten im ID-1-Format gleichzeitig aufnehmen können.
[<=]

TIP1-A_3720 - Gleichzeitig aufnehmbare ID-1-Karte und Plug-In-Karte
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS eine Karte im ID-1-Format und eine Karte im ID-000-Format gleichzeitig aufnehmen können.
[<=]

Das Format der für die Aufnahmen von ID-000-Modulen bestimmten Kontaktiereinheiten ist herstellerspezifisch, da das ID-000-Modul auch mittels eines Adapters gesteckt werden kann.

TIP1-A_3721 - Anzahl Kontaktiereinheiten im Sinne der Zukunftssicherheit
Das Kartenterminal-Modul des Mobilen Kartenterminals SOLL - zusätzlich zu den beiden ID-1-Kontaktiereinheiten - über eine eigenständige Kontaktiereinheit zur Aufnahme von Karten im ID-000-Format verfügen.
[<=]

4.5.3 Ausprägung Kontaktiereinheiten

Die KVK, eGK und der HBA verlangen kontaktbehaftete Schnittstellen mit Kontaktiereinheiten der Größe ID-1 (mit dem Maßen 85,6mm x 54,0 mm).

TIP1-A_3702 - Format der Kontaktiereinheit zur Aufnahme von Karten im ID-1-Format
Die kontaktbehafteten Schnittstellen des Kartenterminal-Moduls des Mobilen Kartenterminals mit der Kontaktiereinheitengröße ID-1 MÜSSEN der Norm ISO/IEC 7810 [ISO7810] entsprechen.
[<=]

TIP1-A_3807 - Format der zu unterstützenden Plug-In-Karten
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS Secure Module Cards (SMC) als kontaktbehaftete Karte im Format ID-1 oder ID-000 (Plug-in-Karte) nach CEN ENV 1375-1 [CEN ENV] unterstützen.
[<=]

TIP1-A_4977 - Lage Kartenkontakte
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS die Lage und Zuordnung der Kontakte entsprechend der Norm ISO/IEC 7816-2 [ISO7816-2] umsetzen.
[<=]

Generell sind alle Kontaktierungstypen zulässig, sofern die generellen mechanischen Anforderungen der folgenden Abschnitte eingehalten werden.

TIP1-A_4978 - Unterstützung Kartenkontakte
Das Mobile Kartenterminal SOLL die Kartenkontakte C4, C6 und C8 NICHT unterstützen.
[<=]

TIP1-A_4979 - Elektrischer Anschluss Kartenkontakte
Das Mobile Kartenterminal SOLL die Kartenkontakte C4, C6 und C8 NICHT elektrisch anschließen.
[<=]

TIP1-A_4262 - Verwendung von Kontaktschonenden Kontaktiereinheiten
Die kontaktbehafteten Schnittstellen des Kartenterminal-Moduls des Mobilen Kartenterminals MÜSSEN kontaktschonend sein.
[<=]

TIP1-A_3763 - Landende Kontakte
Das Mobile Kartenterminal SOLL Kontaktiereinheiten mit landenden Kontakten als kontaktschonende Kontaktiereinheiten verwenden.
[<=]

TIP1-A_3812 - Kartenkontakte und Umschalten in andere Betriebsmodi
Das Mobile Kartenterminal MUSS sicherstellen, dass, wenn die Kartenkontakte C4, C6 und C8 für spezielle Betriebsmodi wie ISO7816-12 erforderlich sind, diese nicht vor dem Umschalten in einen solchen Modus aktiviert werden.
[<=]

TIP1-A_3813 - Kartenkontakte und Umschalten Betriebsmodi
Das Mobile Kartenterminal MUSS sicherstellen, dass, wenn die Kartenkontakte C4, C6 und C8 für spezielle Betriebsmodi wie ISO7816-12 erforderlich sind, diese initial, vor dem Umschalten in einen solchen Modus potentialfrei sind.
[<=]

TIP1-A_3804 - Umschalten aus einem speziellen Betriebsmodus
Das Mobile Kartenterminal MUSS sicherstellen, dass nach dem Umschalten des Mobilen Kartenterminals aus einem speziellen Modus in den Standardmodus die Kartenkontakte C4, C6 und C8 wieder deaktiviert werden.
[<=]

4.5.3.1 ID-1-Kartenkontaktierungen

TIP1-A_4402 - Vermeidung von Beschädigungen der Karte durch die Kontaktiereinheit
Das Mobile Kartenterminal MUSS sicherstellen, dass die Entnahme oder Einführung der Chipkarte in das Mobile Kartenterminal nicht zu einer Beschädigung der Bedruckung bzw. der Funktionalität der Karte durch die Kontaktiereinheit führt.
[<=]

TIP1-A_3703 - Zeitpunkt der Schaltung des „Card-In-Schalters"
Das Mobile Kartenterminal MUSS sicherstellen, dass der „Card-In"-Schalter des Mobilen Kartenterminals (d.h. der Schalter zur Kartenpräsenzerkennung) nicht vor Kontaktierung der Kontaktflächen und Erreichen des Kontakt-Enddrucks geschaltet wird.
[<=]

TIP1-A_3704 - Anpressdruck der Kontaktflächen
Das Mobile Kartenterminal MUSS sicherstellen, dass der Anpressdruck der Kontakte der Chipkartenkontaktiereinheit auf die Kontaktflächen zwischen 0.2N und 0.6N beträgt.
[<=]

Das Kartenterminal-Modul kann anzeigen, ob sich eine Chipkarte korrekt in der Kontaktiereinheit befindet und diese mit Strom versorgt ist.

4.5.3.2 ID-000 Kartenkontaktierungen

Nicht jeder Terminaltyp muss ID-000-Kontaktierungen besitzen.

Sofern ID-000-Kontaktierungen vorhanden sind gilt:

- Der Zugriff auf die Plug-In-Karte(n) kann möglich sein. Der Zugang zur Plug-In-Karte muss jedoch zum Zwecke des Diebstahlschutzes beschränkt sein
- Eine Versiegelung des Zugangs kann erforderlich werden, wenn die Gehäuseöffnungen Zugang zu sicherheitsrelevanten Teilen des Kartenterminalinneren bieten, oder als Maßnahme zum Schutz gegen das Abgreifen oder Manipulieren der Kontaktiereinheit.
- Es ist kein Card-In-Kontakt erforderlich.

TIP1-A_4413 - Beschränkung des Zugangs zu Plug-In-Karten
Das Kartenterminal-Modul des mobilen Kartenterminals SOLL, sofern es über native ID-000-Kontaktiereinheiten verfügt, den Zugang zur Plug-In-Karte zum Zwecke des Diebstahlschutzes beschränken.
[<=]

Nur bei Geräten, die auf Basis eines migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 zugelassen werden, kann auf eine Umsetzung verzichtet werden.

4.5.4 Chipkartenprotokolle

TIP1-A_3705 - Umsetzung der Kartenkommunikation
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS die Kartenkommunikation und das Reset-Verhalten gemäß den Spezifikationen der KVK [KVK], des HBA [HBA], der SMC-B [SMC-B] und der eGK [eGK] umsetzen.
[<=]

Das Kartenterminal-Modul muss nachfolgend aufgeführte synchrone und asynchrone Übertragungsprotokolle zu den Chipkarten unterstützen. Die Protokolle sind nach den Vorgaben der jeweiligen internationalen Normen zu implementieren.

TIP1-A_4263 - Handhabung von Fehlerfällen, Verhinderung von Deadlock-Situationen
Das Mobile Kartenterminal MUSS das Auftreten eines Deadlocks während der Kartenkommunikation verhindern.
[<=]

TIP1-A_4256 - Zu unterstützende Übertragungsprotokolle zu den asynchronen Chipkarten
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS das asynchrone Chipkartenprotokoll:

- T=1, Block-orientiertes Halbduplex-Protokoll gemäß ISO/IEC 7816-3 [ISO7816-3]

unterstützen.
[<=]

TIP1-A_4257 - Zu unterstützende Übertragungsprotokolle zu den synchronen Chipkarten
Das Kartenterminal-Modul des Mobilen Kartenterminals MUSS für synchrone Chipkarten das synchrone Chipkartenprotokoll gemäß der Norm ISO/IEC 7816-10 [ISO7816-10] unterstützen. Dabei gilt:

- S=10 für 2-Wire-Bus Chipkarten gemäß ISO/IEC 7816-10 [ISO7816-10] und dort referenzierter Spezifikationen
- S=8 für I2C-Bus Chipkarten ISO/IEC 7816-10 [ISO7816-10]
- S=9 für 3-Wire-Bus Chipkarten nach Herstellerspezifikation und ISO/IEC 7816-10 [ISO7816-10].

[<=]

TIP1-A_3874 - Gewährleistung der Sicherheit bei Unterstützung kontaktloser Karten
Der Hersteller des Mobilen Kartenterminals DARF, im Fall der Unterstützung von kontaktlosen Chipkarten, bei der Implementierung die Sicherheit des Gesamtsystems "Mobiles Kartenterminal" NICHT verletzen.
[<=]

5 Anforderungen an den Mini-Anwendungskonnektor

Dieses Kapitel beschreibt die Basismechanismen und Basisdienste des Mini-AK sowie die umzusetzenden technischen Use Cases der Fachanwendungen. Das Verhalten der Basisdienste des Mini-AK ist im Kapitel 10.1 beschrieben.

5.1 Basismechanismen

Die Basismechanismen sind Protokolle und Algorithmen, die für die Basisdienste implementiert werden.

5.1.1 Zufallszahlen und Schlüssel

Der Mini-AK unterstützt das Erstellen von Zufallszahlen und Einmalschlüsseln. Sie kommen zum Beispiel für Verschlüsselungen zum Schutz von medizinischen Daten zum Einsatz.

TIP1-A_4936 - Mobiles KT: Anforderung an Zufallszahlen
Der Mini-AK des Mobilen Kartenterminals MUSS im Rahmen der Zufallszahlen die Anforderung [gemSpec_Krypt#GS-A_4367] umsetzen.
[<=]

Die Güte und der ordnungsgemäße Betrieb des Zufallsgenerators sind geeignet sicherzustellen. Der Abschnitt [gemSpec_Krypt#2.3] enthält Hinweise zur Umsetzung dieser Anforderungen für deterministische Zufallszahlengenerierung.

TIP1-A_3860 - mobile Szenarien: Verwendung des Zufallszahlengenerators einer berechtigten Karte
Das Mobile Kartenterminal KANN als Quelle für Zufallszahlen gemäß [TIP1-A_4936] den Zufallszahlengenerator der berechtigten Karte verwenden, welcher die Anforderungen gemäß [gemSpec_Krypt#GS-A_4367] an Qualität und Güte der Zufallszahlen erfüllt.
[<=]

TIP1-A_4937 - Mobiles KT: Anforderung an Einmalschlüssel
Der Mini-AK des Mobilen Kartenterminals MUSS im Rahmen der Einmalschlüssel die Anforderung [gemSpec_Krypt# GS-A_4368] umsetzen.
[<=]

5.2 Basisdienste

Die Basisdienste enthalten die fachlogikneutralen Teile des Mini-AK. Sie stellen primär die verfügbaren Sicherheitsfunktionen des Mini-AK bereit und regeln den Zugriff auf die verfügbaren Karten.

5.2.1 Kartenterminaldienst

Der Kartenterminaldienst des Mobilen Kartenterminals hat bei Zugriff auf Ressourcen eines Kartenterminal-Moduls die Kommunikation zu koordinieren. Er empfängt und verarbeitet vom Kartenterminal-Modul gesendete Ereignisse und stellt den Zugriff auf die

Ressourcen „Tastatur (PIN-Pad)", „Display" und die „Kartenslots" bereit. Die Schnittstellen des Kartenterminaldienstes sind herstellerspezifisch.

Das Kartenterminal-Modul sendet Ereignisse über das Stecken und Ziehen einer Karte an den Kartenterminaldienst des Mini-AK, welcher empfangene Ereignisse entweder an den Kartendienst weiterleitet oder selber dafür Sorge trägt, dass die Liste der vom Kartendienst verwalteten Karten aktualisiert wird.

Meldet während einer Kartenaktion das Kartenterminal das Ziehen der Karte, so kann die ausgeführte Aktion nicht erfolgreich zu Ende geführt werden.

TIP1-A_3840 - mobile Szenarien: Freigabe von Ressourcen bei Fehlersituation
Das Mobile Kartenterminal MUSS, falls während einer Kartenaktion das Ziehen der Karte gemeldet wird, die entsprechende Ressource nach Erkennung der Fehlersituation freigeben.
[<=]

TIP1-A_3868 - mobile Szenarien: Freigabe von Ressourcen ohne manuelles Eingreifen
Der Kartenterminaldienst des Mobilen Kartenterminals DARF zur Freigabe der Ressource gemäß [TIP1-A_3840] ein manuelles Eingreifen NICHT erfordern.
[<=]

Weitere Details zur Umsetzung sind herstellerspezifisch.

5.2.2 Kartendienst

TIP1-A_4956 - Mobiles KT: Kartendienstunterstützung für eGK, HBA, SMC-B und KVK
Der Mini-AK des Mobilen Kartenterminals MUSS in der Lage sein, mindestens die Karten eGK [eGK], HBA [HBA], SMC-B [SMC-B] und KVK [KVK] zu erkennen und zu unterstützen.
[<=]

Der Kartendienst stellt für die von ihm verwalteten Karten die im Folgenden beschriebenen Funktionen bereit:

5.2.2.1 Identifikation des Kartentyps und der Version

TIP1-A_3788 - Mobiles KT: Bestimmung des AID einer Prozessorkarte nach [ISO7816-3]
Der Mini-AK des Mobilen Kartenterminals MUSS für die Identifikation des Kartentyps und der Version einer Karte den Typ einer Prozessorkarte nach [ISO7816-3] anhand des Application Identifier (AID) des Master File (MF) gemäß Tab_MobKT_002 "Application Identifier der Kartentypen" bestimmen.
[<=]

TIP1-A_3815 - Mobiles KT: Bestimmung der AID aus File Control Parameter oder Application Template
Der Mini-AK des Mobilen Kartenterminals MUSS für die Identifikation des Kartentyps und der Version einer Karte gemäß [TIP1-A_3788] die AID aus dem File Control Parameter des Master File über ein SELECT oder aus dem Application Template in /MF/EF.DIR beziehen.
[<=]

TIP1-A_4938 - Mobiles KT: Bestimmung der AID einer Speicherkarte nach [KVK#4.1]
Der Mini-AK des Mobilen Kartenterminals MUSS für die Identifikation der KVK den Typ der Speicherkarte anhand des Application Identifier (AID) in DIR-data (siehe [KVK#6.2.2]) bestimmen.
[<=]

Tabelle 1: Tab_MobKT_002 Application Identifier der Kartentypen

Kartentyp	Kriterien
eGK	AID des MF: siehe [eGK]
HPC	AID des MF: siehe [HBA]
SMC-B	AID des MF: siehe [SMC-B]
KVK	AID innerhalb der DIR-data: siehe [KVK#6.2.2]

TIP1-A_4957 - Mobiles KT: Unterstützung Kartenversionen von eGK, HBA und SMC-B
Der Mini-AK des Mobilen Kartenterminals MUSS die Versionen für [eGK], [HBA] und [SMC-B] unterstützen, wenn die Versionen des Betriebssystems und des Objektsystems der jeweiligen Karte dem Mini-AK bekannt sind.
[<=]

Die Kartenversion der Kartentypen eGK, HBA und SMC-B setzt sich aus der Version des Betriebssystems (COS) und der Objektsystemversion des jeweiligen Kartentyps zusammen. Im Rahmen der Prüfung auf Karten-Inkompatibilität gemäß [TIP1-A_3816] sind diese beiden Versionsnummern zu berücksichtigen.

Für die Karten-Generation 2 und 2.1 werden zum jeweiligen Release, in welchem der Produkttypsteckbrief des Mobilen Kartenterminals enthalten ist, die Versionen der zu unterstützenden Karten veröffentlicht.

TIP1-A_3816 - Mobiles KT: Karten-Inkompatibilität als Ergebnis der Kompatibilitätsprüfung
Der Mini-AK des Mobilen Kartenterminals MUSS in einem ersten Schritt, wenn die durch das Mobile Kartenterminal ermittelte Kartenversion kleiner als alle durch den Mini-AK zu unterstützenden Kartenversionen gemäß [TIP1-A_4957] ist oder die ermittelte Kartenversion nicht gemäß [TIP1-A_4957] bekannt und kleiner als die größte zu unterstützende Kartenversion ist, von einer inkompatiblen Karte ausgehen und die weitere Verarbeitung der Karte direkt abbrechen.
Der Mini-AK des Mobilen Kartenterminals MUSS in einem zweiten Schritt, wenn die durch das Mobile Kartenterminal ermittelte Kartenversion größer als alle durch den Mini-AK zu unterstützenden Kartenversionen gemäß [TIP1-A_4957] ist, von einer kompatiblen Karte ausgehen und versuchen, diese zu verarbeiten.
[<=]

Das bedeutet, dass der Mini-AK des Mobilen Kartenterminals zunächst unbekannte ältere Versionen (mindestens die Version des Betriebssystems oder die Objektsystemversion des jeweiligen Kartentyps ist kleiner als die zu unterstützenden Versionen) bzw. unbekannte Versionen, die aber kleiner als die größte ihm bekannte Version sind, als inkompatibel identifiziert und die Verarbeitung der zugehörigen Karte direkt mit einer Fehlermeldung gemäß [TIP1-A_4271] abbricht.

Der Mini-AK muss dann bei unbekannten neueren Versionen (mindestens die Version des Betriebssystems oder die Objektsystemversion des jeweiligen Kartentyps ist größer als die zu unterstützenden Versionen) von einer kompatiblen Karte ausgehen und versuchen, diese zu verarbeiten.

TIP1-A_4271 - Mobiles KT: Fehlermeldung Karten Inkompatibilität
Der Mini-AK des Mobilen Kartenterminals MUSS, wenn die durch das Mobile Kartenterminal ermittelte Kartenversion zu keiner dem Mini-AK bekannten gemäß [TIP1-A_4957] kompatibel ist, eine geeignete Fehlermeldung auf dem erweiterten Display des Mobilen Kartenterminals darstellen.
[<=]

5.2.2.2 Zugriff auf Dateien der Karte

Die Daten der verschiedenen fachlichen Anwendungen wie auch die Zertifikate sind auf der Karte in Dateien verschiedener Ausprägung (transparent, Record orientiert, Data Object orientiert) gespeichert.

TIP1-A_4939 - Mobiles KT: Extended Length der Karten
Der Kartendienst des Mobilen Kartenterminals MUSS das Extended Length Feature der Karten unterstützen.
[<=]

Das heißt, der Mini-AK muss zunächst anhand des ATRs der Karte erkennen, ob Extended Length unterstützt wird. Anschließend muss er EF.ATR auswerten, um zu bestimmen, welche Längen für Datenfelder in den APDUs unterstützt werden (siehe hierzu [eGK], [HBA] und [SMC-B]). Beim Lesen und Schreiben von Daten auf die Karte muss, basierend auf der maximal unterstützten Länge, die Anzahl der benötigten APDUs zum Übertragen der Daten von oder zu der Karte minimiert werden. Der Zugriff auf die Dateien der eGK erfordert in der Regel eine vorausgehende Card-to-Card-Authentisierung.

Die Durchführung dieser für die eGK benötigten Autorisierungen wird in der Regel durch das jeweilige Fachmodul im Mini-AK angestoßen (siehe auch Kapitel 5.2.2.5).

5.2.2.3 PIN-Verifikation und PIN-Management

Der Zugriff auf Sicherheitsfunktionen oder Dateien der Karte kann u. a. durch PIN geschützt sein. Eine Karte kann mehrere PINs haben (z. B. eine separate PIN für die qualifizierte elektronische Signatur, wobei diese im Bereich des mobilen Einsatzszenarios nicht betrachtet wird).

Bei HBA und SMC-B stößt der Kartendienst des Mini-AK bei Bedarf automatisch eine PIN-Verifikation an, um den Zugriff auf einen privaten Schlüssel der Karte zu autorisieren (s. a. TUC_MOKT_405 authenticateCardToCard).

5.2.2.4 Ereignisse

Der Kartendienst muss die vom Kartenterminaldienst empfangenen Ereignisse verarbeiten. Die vom Kartenterminal mitgeteilten Statusänderungen der Karten müssen direkt nach Eintreffen zu einer Anpassung des Status der vom Kartendienst verwalteten Kartenobjekte führen. Wird eine Karte gesteckt, so wird ein entsprechender Eintrag in die Liste der verfügbaren Karten aufgenommen werden. Wird eine Karte gezogen, so wird der entsprechende Eintrag aus der Liste der verfügbaren Karten entfernt.

5.2.2.5 Card-to-Card-Authentisierung und sichere Kanäle

TIP1-A_3787 - Mobiles KT: durch Kartendienst bereitzustellende Funktionen für sichere Kommunikation zwischen Karten
Der Kartendienst des Mini-AK des Mobilen Kartenterminals MUSS Funktionen für die Durchführung von Card-to-Card-Authentisierung ohne Aufbau eines sicheren Kanals (d. h. Aushandeln eines symmetrischen Schlüssels für die sichere Kommunikation zwischen beiden Karten) bereitstellen, und ggf. die benötigten Cross-CVCs bereithalten und bei Bedarf in die Karten laden.
[<=]

Ein Beispiel für Card-to-Card-Authentisierung ohne Aufbau eines sicheren Kanals ist die Authentisierung zwischen HBA bzw. SMC-B und eGK (siehe hierzu [eGK], [HBA] und [SMC-B]).

Die Umsetzung von C2C mit Aufbau eines sicheren Kanals kann optional unterstützt werden.

Wenn die Herausgeber-CV-Zertifikate beider Karten ihren Ursprung bei derselben Root haben, lassen sich die Zertifikatsketten auf geradem Weg durchlaufen. Wenn die Roots aber unterschiedlich sind, kann eine Karte das fremde CA-Zertifkat nicht mit dem eigenen Root-Key prüfen. Sie benötigt ein Zertifikat, das von der eigenen Root signiert ist und den Root-Key der fremden Karte bestätigt. Diese Zertifikate heißen Cross-CV-Zertifikate (Cross-CVCs). Der Mini-AK muss für jedes mögliche Paar aus Root-Keys zwei Cross-CVCs bereithalten (in jeder Richtung eines) und bei Bedarf in die Zertifikatskette einhängen. Damit verlängert sie sich um einen Schritt, kann letztlich aber auf dieselbe Weise wie bisher abgearbeitet werden: als mehrfache Abarbeitung der Sequenz {Schlüssel des Signierers selektieren + Zertifikat prüfen}.

Die Referenz des Root-Keys ist im CA-Zertifikat der Karte als Parameter CAR (Certificate Authority Reference) enthalten. Da die CAR weltweit eindeutig ist, genügt es, die CARs der CA-Zertifikate der beiden beteiligten Karten zu vergleichen, um festzustellen, ob sie von unterschiedlichen Roots abstammen.

Daher müssen im Mini-AK die entsprechenden Cross-CVCs zur Verfügung stehen.

TIP1-A_4940 - Mobiles KT: Nachladen von Cross-CVCs
Der Kartendienst des Mobilen Kartenterminals MUSS bei einer Card-to-Card-Authentisierung erkennen, ob und welche Cross-CVCs nötig sind und diese dann bei Bedarf in die jeweilige Karte laden.
[<=]

Der Ablauf einer Card-to-Card-Authentisierung ist im Rahmen von Kapitel 10.1.7 dargestellt. Bei Rollenauthentisierungen mit HBA und SMC-B stößt dabei der Kartendienst des Mini-AK bei Bedarf automatisch eine PIN-Verifikation an, um den Zugriff auf den für die Card-to-Card-Authentisierung verwendeten privaten Schlüssel der Karte zu autorisieren.

5.2.2.6 Datenzugriffsaudit

Der Mini-AK hat für bestimmte Aktionen Protokolleinträge auf die eGK zu schreiben. Wann eine Protokollierung vorzunehmen ist und welchen konkreten Inhalt der Eintrag jeweils hat, legen die Fachanwendungen fest.

TIP1-A_3724 - Schreibender Zugriff auf die eGK nur auf den Logging-Container
Der Kartendienst des Mobilen Kartenterminals MUSS sicherstellen, dass schreibende Zugriffe ausschließlich auf den Logging-Container der eGK möglich sind.
[<=]

TIP1-A_3842 - Referenzuhr zur Bestimmung des Zeitpunktes für Log-Einträge der eGK
Das Mobile Kartenterminal MUSS zur Bestimmung des Erfassungszeitpunktes zum Logging auf die eGK die Systemuhr des Mini-AKs verwenden.
[<=]

5.2.3 Verschlüsselungsdienst

Der Verschlüsselungsdienst stellt Funktionen zur Ver- und Entschlüsselung von Daten und Dokumenten zur Verfügung und wird z. B. vom Mini-PS verwendet, um die zwischengespeicherten Daten zu ver- bzw. entschlüsseln.

TIP1-A_3755 - Verwendung der Ver- und Entschlüsselungsfunktionen berechtigter Karten
Das Mobile Kartenterminal MUSS die Verwendung der Ver- und Entschlüsselungsfunktionen der berechtigten Karten ermöglichen.
[<=]

TIP1-A_4424 - mobile Szenarien Verschlüsselung: Zu verwendende Verfahren
Der Verschlüsselungsdienst des Mobilen Kartenterminals MUSS für die Ver- und Entschlüsselung von Daten und Dokumenten die in [gemSpec_Krypt# GS-A_4367], [gemSpec_Krypt#GS-A_4368],[gemSpec_Krypt#GS-A_4389], [gemSpec_Krypt#GS-A_4390], [gemSpec_Krypt#A_17575] und [gemSpec_Krypt#GS-A_5016] beschriebenen Verfahren und Algorithmen verwenden.

[<=]

5.2.4 Zertifikatsdienst

TIP1-A_3739 - mobile Szenarien: Ausschließliche Nutzung von HBA oder SMC-Bs
Der Zertifikatsdienst des Mobilen Kartenterminals MUSS sicherstellen, dass ausschließlich HBA und SMC-B als berechtigte Karten eine C2C-Authentisierung mit der eGK durchführen können.
[<=]

TIP1-A_4952 - mobile Szenarien: Zeitpunkt für Prüfung auf berechtigte Karte
Das Mobile Kartenterminal MUSS spätestens beim ersten Zugriff auf die Karte nach deren Initialisierung prüfen, ob es sich bei einer Karte um eine berechtigte Karte (also HBA oder SMC-B) handelt.
[<=]

TIP1-A_4953 - mobile Szenarien, Zertifikatsdienst: Überprüfung der Gültigkeit der X.509-Zertifikate einer Karte
Der Zertifikatsdienst des Mobilen Kartenterminals MUSS nach der Prüfung gemäß [TIP1-A_4952] anhand des Ablaufdatums des jeweiligen X.509-AUT-Zertifikates einer berechtigten Karte (C.HP.AUT bzw. C.HCI.AUT) und der Systemuhr nachprüfen, dass diese nicht abgelaufen sind.
[<=]

5.3 Fachanwendung VSDM

Das Fachmodul Versichertenstammdatenmanagement (mobKT) muss die Anwendungsfälle

- VSDM-UC_14: VSD von eGK im mobilen Einsatzszenario lesen
- VSDM-UC_15: Versichertendaten von KVK im mobilen Einsatzszenario lesen

gemäß [gemSysL_VSDM] umsetzen:

5.3.1 Übergreifende Anforderungen

Nachfolgend werden die Anforderungen an das Fachmodul VSDM (mobKT) beschrieben, die übergreifend für die fachlichen Anwendungsfälle zu betrachten sind.

Der Schutzbedarf der verarbeiteten Informationsobjekte der Anwendung VSDM wird durch die sie verarbeitenden Sicherheitsanalysegegenstände (Komponenten, Dienste, Schnittstellen) sichergestellt.

Kann eine Aktivität oder der ganze Anwendungsfall nicht durchgeführt werden bzw. wird eine Aktivität vorzeitig beendet, muss eine eindeutige, unverwechselbare Fehlermeldung erzeugt werden. Diese Fehlermeldung muss wie in Kapitel 6.2.4 beschrieben dem Anwender signalisiert und zur Anzeige im Hinblick auf [TIP1-A_4266] gespeichert werden.

VSDM-A_2782 - Fachmodul VSDM (mobKT): Pflichtfelder zum Anzeigen auf dem Display
Das Fachmodul VSDM (mobKT) MUSS Versichertendaten mit den in Tab_mobKT_ST2_18 aufgelisteten Feldern auf seinem Display anzeigen können.
[<=]

Tabelle 2: Tab_mobKT_ST2_18 Pflichtfelder zum Anzeigen auf dem Display

Feld	Beschreibung	Gilt für	Führt zum Abbruch, wenn Feld nicht gelesen werden kann
Vorname	Vorname des Versicherten	KVK, eGK	Ja
Nachname	Nachname des Versicherten	KVK, eGK	Ja
Geburtsdatum	Geburtsdatum des Versicherten	KVK, eGK	Ja
VersichertenNr.	Versichertennummer	KVK, eGK	Ja
Kostenträger	Name des Kostenträgers	KVK, eGK	Ja

Kassen-Nr.	IK der abrechnenden Krankenkasse	KVK, eGK	Ja
EndeVersicherungsnachweis	Ende des Versicherungsnachweises	KVK, eGK	Nein
Versichertenart	Art des Versicherten (Mitglied, Familienversicherter, Rentner und ihre Familienangehörigen)	KVK, eGK	Ja
Status (wird nur angezeigt, wenn für die Freischaltung der eGK die verwendete Leistungserbringerkarte zum Lesen der GVD berechtigt ist)	Zuzahlungsstatus	eGK	Nein
Ruhender Leistungsanspruch • Art des Ruhens (wird nur angezeigt, wenn für die Freischaltung der eGK die verwendete Leistungserbringerkarte zum Lesen der GVD berechtigt ist)	Angabe des ruhenden Leistungsanspruchs (falls zum Behandlungszeitpunkt vorhanden)	eGK	Nein

VSDM-A_2880 - Fachmodul VSDM (mobKT): Versichertendaten auf dem Display unverändert anzeigen
Das Fachmodul VSDM (mobKT) MUSS die Versichertendaten unverändert auf dem Display anzeigen.
[<=]

A_18379 - Fachmodul VSDM (mobKT): unterstützte Versionen der eGK
Das Fachmodul VSDM (mobKT) MUSS das Auslesen der Versichertenstammdaten von einer eGK der Generation 2 und 2.1 unterstützen.**[<=]**

Die für die Fachanwendung VSDM spezifischen Speicherstrukturen der eGK werden in [gemSpec_eGK_Fach_VSDM] beschrieben. Die Version der VSDM Speicherstrukturen wird in `EF.StatusVD.Version_Speicherstruktur`-Datei der eGK vorgegeben.

VSDM-A_2980 - Fachmodul VSDM: unterstützte Versionen der VSDM Speicherstrukturen auf der eGK
Das Fachmodul VSDM (MobKT) MUSS, falls die EF.StatusVD.Version_Speicherstruktur-Datei der eGK eine unbekannte Version der VSDM Speicherstrukturen referenziert, mit der folgenden, auf dem Display angezeigten, Fehlermeldung abbrechen: „Nicht unterstützte Version der VSDM Speicherstrukturen der eGK".
[<=]

VSDM-A_2995 - Fachmodul VSDM (mobKT): Unterstützung einer neuen VSD-Speicherstruktur
Der Hersteller des mobKTs MUSS innerhalb einer jeweils durch die gematik festzulegenden Frist eine neue Version der VSD-Speicherstruktur der eGK unterstützen. Der Hersteller muss die Unterstützung in Rahmen der Zulassung erklären. Die Mindestfrist zwischen der Bekanntgabe und der Verfügbarkeit einer ggf. neuen Firmware-Version beträgt 6 Monate.
[<=]

Im Falle von geänderten Anforderungen zu den VSD (z.B. aufgrund gesetzlicher Änderungen oder neuer Vereinbarungen zwischen den Vertragspartnern) kann eine Schemaänderung notwendig werden.

VSDM-A_2962 - Fachmodul VSDM (mobKT): Unterstützung einer neuen VSD-Schemaversion
Der Hersteller des mobKTs MUSS innerhalb einer jeweils durch die gematik festzulegenden Frist eine neue VSD-Schemaversion unterstützen. Der Hersteller muss die Unterstützung in Rahmen der Zulassung erklären. Die Mindestfrist zwischen der Bekanntgabe und der Verfügbarkeit einer ggf. neuen Firmware-Version beträgt 6 Monate.
[<=]

A_18380 - Fachmodul VSDM (mobKT): alte Versionen der eGK
Das Fachmodul VSDM (mobKT) SOLL beim Auslesen der Versichertenstammdaten von einer eGK mit einer älteren Version als Generation 2 mit einer Fehlermeldung abbrechen.**[<=]**

VSDM-A_2927 - Anzeigen zwischengespeicherter Versichertendaten
Das Fachmodul VSDM (mobKT) MUSS das Anzeigen zwischengespeicherten Versichertendaten auf dem Display gemäß [VSDM-A_2782] ermöglichen.
[<=]

VSDM-A_2928 - Drucken von Versichertendaten
Das Fachmodul VSDM (mobKT) KANN die Kommunikation mit einem Drucker unterstützen und das Ausdrucken von VSD- oder KVK-Daten auf ein Standardformular ermöglichen.
[<=]

VSDM-A_2878 - Fachmodul VSDM (mobKT): Übertragung von Arztnummer und die Betriebsstättennummer zum Drucker
Das Fachmodul VSDM (mobKT) MUSS beim Drucken (sofern unterstützt) von VSD- oder KVK-Daten auf ein Standardformular die Arztnummer und die Betriebsstättennummer zum Drucker übertragen.
[<=]

Die genaue Ausprägung des Druckmechanismus ist herstellerspezifisch.

VSDM-A_2877 - Fachmodul VSDM (mobKT): Bedruckungsvorschriften für Formularköpfe
Das Fachmodul VSDM (mobKT) MUSS beim Drucken (sofern unterstützt) von VSD- oder KVK-Daten auf ein Standardformular mindestens die Version 1.06 die Bedruckungsvorschriften für Formularköpfe gemäß [KBV_ITA_VGEX_Mapping_KVK_1.06#2.3.3] mit Ausnahme der Bedruckungsvorschriften zum ASV-Kennzeichen einhalten (siehe auch [BMV-Ä 2014]).
[<=]

Die Bedruckungsvorschriften zum ASV-Kennzeichen (Ambulante Spezialfachärztliche Versorgung) können optional implementiert werden.

VSDM-A_3049 - Fachmodul VSDM (mobKT): Bedruckungsvorschriften ASV-Kennzeichen
Das Fachmodul VSDM (mobKT) SOLL beim Drucken (sofern unterstützt) die Bedruckungsvorschriften zum ASV-Kennzeichen umsetzen.
[<=]

Nur bei Geräten, die auf Basis eines migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 zugelassen werden, kann auf eine Umsetzung von [VSDM-A_3049] verzichtet werden.

Die Umsetzung der Bedruckungsvorschriften zum ASV-Kennzeichen bedingt zusätzliche Konfigurationsmöglichkeiten zur ASV-Teamnummer (analog zu [TIP1-A_3810] und [TIP1-A_3832]) und zusätzliche Logik (wenn ein Formularkopf mit ASV-Kennzeichen gedruckt werden soll, dann ist das ASV-Kennzeichen „1" in das Statusfeld - Druckzeile 6, Position 30 - zu drucken und anstatt der Betriebstättennummer ist die ASV-Teamnummer zu drucken). Im Falle einer Umsetzung wird die Implementierung zum ASV-Kennzeichen auf Vollständigkeit und Korrektheit geprüft.

Mit neueren Versionen der Bedruckungsvorschriften können weitere zusätzliche Funktionalitäten eingeführt werden, die gegebenenfalls weitere Konfigurationsmöglichkeiten und zusätzliche Logik im Mobilen Kartenterminal erfordern, z.B. die Angabe eines TSS-Kennzeichens.

VSDM-A_3052 - Fachmodul VSDM (mobKT): Weitere Funktionalitäten aktueller Bedruckungsvorschriften
Bei Umsetzung einer höheren Version der Bedruckungsvorschriften als der in [VSDM-A_2877] angegebenen Mindestversion SOLL das Fachmodul VSDM (mobKT) alle Funktionalitäten dieser Bedruckungsvorschriften umsetzen.
[<=]

Nur bei Geräten, die auf Basis eines migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 zugelassen werden, kann auf eine Umsetzung von [VSDM-A_3052] verzichtet werden.

VSDM-A_3050 - Version der Bedruckungsvorschriften
Der Hersteller des Mobilen Kartenterminals MUSS im Rahmen der Zulassung erklären, welche Version der Bedruckungsvorschriften [KBV_ITA_VGEX_Mapping_KVK] die gemäß [VSDM-A_2877] bzw. [VSDM-A_3051] implementierte Druckfunktionalität umsetzt. Der Hersteller MUSS ebenfalls angeben, ob die Bedruckungsvorschriften zum ASV-Kennzeichen gemäß [VSDM-A_3049] implementiert sind und welche Funktionalitäten gemäß [VSDM-A_3052] der angegebenen Version der Bedruckungsvorschriften nicht umgesetzt wurden. Der Hersteller MUSS diese Informationen öffentlich zugänglich machen.
[<=]

Die gematik wird die Information zur umgesetzten Version der Bedruckungsvorschriften und ggf. Ausnahmen zu bestimmten Funktionalitäten der Bedruckungsvorschriften im Rahmen der Veröffentlichung der Zulassung mit veröffentlichen.

VSDM-A_3051 - Fachmodul VSDM (mobKT): Aktuelle Bedruckungsvorschriften für Formularköpfe
Das Fachmodul VSDM (mobKT) SOLL über [VSDM-A_2877] hinaus beim Drucken (sofern unterstützt) von VSD- oder KVK-Daten auf ein Standardformular die Bedruckungsvorschriften für Formularköpfe gemäß [KBV_ITA_VGEX_Mapping_KVK] einhalten.
[<=]

Nur bei Geräten, die auf Basis eines migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 zugelassen werden, kann auf eine Umsetzung von [VSDM-A_3051] verzichtet werden.

VSDM-A_2903 - Fachmodul VSDM (mobKT): Löschen von VSD
Der Hersteller des Mobilen Kartenterminals MUSS den Leistungserbringer in der Benutzerdokumentation darauf hinweisen, dass dieser die zwischengespeicherten Versichertenstammdaten aus Datenschutzgründen spätestens nach Wegfall der Zweckbindung (Quartalsabrechnung) aus dem Zwischenspeicher löschen muss, falls diese nicht schon vorher an das PVS übertragen wurden.
[<=]

5.3.2 VSD von eGK im mobilen Einsatzszenario lesen

VSDM-A_2766 - Fachmodul VSDM (mobKT): Aktivitäten beim Lesen von der eGK
Das Fachmodul VSDM (mobKT) MUSS beim Lesen der Versichertendaten von der eGK die Aktivitäten gemäß Tab_mobKT_ST2_10 durchführen.
[<=]

Zusätzlich zu den in [gemSysL_VSDM] geforderten Aktivitäten, müssen die VSD im Zwischenspeicher des Mobilen Kartenterminals abgelegt werden.

VSDM-A_2876 - Fachmodul VSDM (mobKT): Speicherung von VSD und Protokollierungsdaten im dafür vorgesehenen Zwischenspeicher
Das Fachmodul VSDM (mobKT) MUSS VSD sowie der zugehörigen Protokollierungsdaten ausschließlich im dafür vorgesehenen Zwischenspeicher des Mini-PS persistieren.
[<=]

Tabelle 3 : Tab_mobKT_ST2_10 – VSDM-UC_14 Aktivitäten

Schritt	Aktivität	TUCs
1	Technische Nutzbarkeit und Offline-Gültigkeit der eGK prüfen	TUC_MOKT_418 checkEGK, TUC_MOKT_438 checkEGKAuthCertificate
2	Echtheit der beteiligten Karten prüfen	TUC_MOKT_220 fulfillAccessConditions
3	VSD-Status-Container Lesen	TUC_MOKT_202 readFile
4	PD und VD von eGK lesen	TUC_MOKT_202 readFile
5	GVD von eGK lesen	TUC_MOKT_202 readFile
6	Protokolleintrag auf eGK schreiben	TUC_MOKT_406 writeEGKAudit
7	PD, VD und GVD im Zwischenspeicher ablegen	TUC_MOKT_010 writeToInternalStorage
8	Anzeigen des gelesen Datensatzes im Display	

VSDM-A_2725 - Fachmodul VSDM (mobKT): Technische Fehler beim Lesen von VSD
Das Fachmodul VSDM (mobKT) MUSS das Lesen von VSD von der eGK mit der Fehlermeldung "Technischer Lesefehler" und dem jeweiligen Fehlercode des TUCs abbrechen, wenn ein technischer Fehler auftritt.
[<=]

VSDM-A_2963 - Fachmodul VSDM (mobKT): Nicht bekanntes Schema beim Lesen von VSD
Das Fachmodul VSDM (mobKT) MUSS, falls das Schema der Versichertenstammdaten nicht bekannt ist, die Verarbeitung fortführen.
[<=]

Damit können zukünftige Änderungen im Schema rückwärtskompatibel sein.

VSDM-A_3000 - Fachmodul VSDM (mobKT): Weitere Prüfungen beim Lesen von VSD
Das Fachmodul VSDM (mobKT) MUSS das Lesen von VSD von der eGK und die Ablage im Zwischenspeicher gemäß VSDM-A_2766 in folgenden Fällen mit einer entsprechenden Fehlermeldung gemäß Kapitel 6.2.4 abbrechen:

- Daten im Container nicht lesbar (z.B. Fehler beim Entpacken des gezippten Files),
- XML nicht gültig (well-formed) oder
- ein XML-Element ist nicht korrekt gefüllt oder nicht vorhanden, das in Tabelle Tab_mobKT_ST2_18 als „Führt zum Abbruch, wenn Feld nicht gelesen werden kann" gekennzeichnet ist.

[<=]

Das Fachmodul VSDM (mobKT) macht für die gelesenen VSD keine XML-Schema-Validierung, sondern liest die in der Tabelle Tab_mobKT_ST2_18 aufgelistete Pflichtfelder für das anschließende Anzeigen auf dem Display. Falls einige der den Pflichtfeldern entsprechenden Elemente nicht aus den gelesenen VSD extrahiert werden können (z.B. aufgrund einer XML Schema Änderung, indem Namen einiger XML-Elementen geändert wurden) und der Fehler entsprechend Tab_mobKT_ST2_18 nicht zum Abbruch führen soll, wird das mobKT die Verarbeitung fortsetzen und nur die erkannten Pflichtfelder anzeigen.

5.3.2.1 Technische Nutzbarkeit und Offline-Gültigkeit der eGK prüfen

Das Fachmodul VSDM (mobKT) muss mittels TUC_MOKT_418 checkEGK und TUC_MOKT_438 checkEGKAuthCertificate die Aktivität „Technische Nutzbarkeit und Offline-Gültigkeit der eGK prüfen" ausführen, indem sie die Vorgaben der Tabelle 4 prüft.

VSDM-A_2714 - Fachmodul VSDM (mobKT): technische Nutzbarkeit und Offline-Gültigkeit der eGK prüfen
Das Fachmodul VSDM (mobKT) MUSS, wenn beim Prüfen der technischen Nutzbarkeit und Offline-Gültigkeit der eGK ein Fehlerzustand der Tabelle Tab_mobKT_ST2_11 eintritt, die Verarbeitung abbrechen und die entsprechende Fehlermeldung anzeigen.
[<=]

Tabelle 4 : Tab_mobKT_ST2_11 – Fehlerzustände Technische Nutzbarkeit und Offline-Gültigkeit der eGK prüfen

Fehlerzustand	Auslöser	Fehlercode	Fehlermeldung (max. 26 Zeichen)
Karte gesperrt	Im Falle der eGK bedeutet dies, das DF.HCA gesperrt ist	1120	Karte gesperrt
Karte ungültig	AUT-Zertifikat ist nach Offline-Prüfung zeitlich nicht gültig	1501	Karte ungültig

Eine weitergehende Prüfung des AUT-Zertifikats, z.B. auf gültige Signatur, soll nicht durchgeführt werden, da das Mobile Kartenterminal nicht die Liste der vertrauenswürdigen Zertifikatsherausgeber kennt. Im mobilen Einsatzszenario ohne Onlineverbindung ist es nicht möglich, die Aktualität dieser Liste zu gewährleisten.

5.3.2.2 Echtheit der beteiligten Karten prüfen

VSDM-A_2762 - Fachmodul VSDM (mobKT): Echtheit der beteiligten Karten prüfen
Das Fachmodul VSDM (mobKT) MUSS die Echtheit der beteiligten Karten prüfen, indem mittels TUC_MOKT_220 fulfillAccessConditions eine gegenseitige C2C-Authentisierung durchführt.
[<=]

Der Ablauf der C2C-Authentisierung ist in Kapitel 10.1.7 dargestellt.

VSDM-A_2763 - Fachmodul VSDM (mobKT): HPC im Ablauf freischalten
Das Fachmodul VSDM (mobKT) MUSS, falls die Leistungserbringerkarte (SMC-B/HBA) noch nicht freigeschaltet ist, den Anwender dazu im Ablauf auffordern.
[<=]

5.3.2.3 VSD Status Container Lesen

Das Fachmodul VSDM (mobKT) muss das Statusflag im Container EF.StatusVD mittels TUC_MOKT_202 readFile lesen. Der Wert 1 im Element Status weist auf eine nicht abgeschlossene Transaktion und damit inkonsistente VSD hin.

VSDM-A_2717 - Fachmodul VSDM (mobKT): VSD Status Container prüfen
Das Fachmodul VSDM (mobKT) MUSS, wenn der Status-Container im Feld Status den Wert '1' enthält, die Verarbeitung abbrechen und die entsprechende Fehlermeldung gemäß Tab_mobKT_ST2_13 anzeigen.
[<=]

Die Details der Datenstruktur von EF.StatusVD sind für die eGK der Generation 2 und 2.1 in [gemSpec_eGK_Fach_VSDM] spezifiziert.

Tabelle 5: Tab_mobKT_ST2_13 – Fehlerzustände VSD Status Container Lesen

Fehlerzustand	Auslöser	Fehlercode	Fehlermeldung (max. 26 Zeichen)
VSD ungültig/nicht konsistent	EF.StatusVD ist ‚1'	3001	Daten inkonsistent

5.3.2.4 PD und VD von eGK lesen

VSDM-A_2718 - Fachmodul VSDM (mobKT): PD und VD lesen
Das Fachmodul VSDM (mobKT) MUSS die PD und VD aus den Containern EF.PD und EF.VD der eGK mittels TUC_MOKT_202 readFile lesen.
[<=]

VSDM-A_2764 - Fachmodul VSDM (mobKT): Warnung wenn kein Versicherungsschutz besteht
Das Fachmodul VSDM (mobKT) MUSS bei von der eGK eingelesenen Versichertendaten durch Vergleich der in den Feldern "Versicherungsschutz.Ende" und "Versicherungsschutz.Beginn" eingetragenen Werten mit der Systemuhr überprüfen, ob ein Versicherungsschutz besteht, und, wenn kein Versicherungsschutz besteht, die entsprechende Warnmeldung gemäß Tab_mobKT_ST2_14 auf dem Display des Kartenterminals anzeigen.
[<=]

Die XML-Elemente Beginn und Ende finden sich in den allgemeinen Versichertendaten im Element Versicherter unterhalb des Elements Versicherungsschutz. Falls die Elemente Beginn oder Ende leer sind, entfällt die jeweilige Prüfung.

Tabelle 6: Tab_mobKT_ST2_14 – Durch das Fachmodul VSDM (mobKT) zu erzeugende Warnmeldung

Zustand	Warnmeldung
Beginn noch nicht erreicht	Der Versicherungsschutz hat noch nicht begonnen.
Ende bereits erreicht	Das Ende des Versicherungsschutzes ist erreicht

VSDM-A_2985 - Fachmodul VSDM (mobKT): Warnung bei ruhendem Leistungsanspruch
Das Fachmodul VSDM (mobKT) MUSS dem Benutzer eine Warnmeldung gemäß Tab_mobKT_ST2_19 auf dem Display des Kartenterminals anzeigen, wenn die eGK aufgrund eines ruhenden Leistungsanspruchs keinen gültigen oder einen eingeschränkten Leistungsanspruchsnachweis darstellt.
[<=]

Der XML-Element RuhenderLeistungsanspruch findet sich in den geschützten Versichertendaten.

Tabelle 7: Tab_mobKT_ST2_19 – Durch das Fachmodul VSDM (mobKT) zu erzeugende Warnmeldung

Zustand	Warnmeldung
Ein vollständiger Leistungsanspruch	Ein vollständiger ruhender Leistungsanspruch besteht
Ein eingeschränkt ruhender Leistungsanspruch	Ein eingeschränkt ruhender Leistungsanspruch besteht

5.3.2.5 GVD von eGK lesen

VSDM-A_2719 - Fachmodul VSDM (mobKT): GVD lesen
Das Fachmodul VSDM (mobKT) MUSS die GVD aus dem Container EF.GVD der eGK mittels TUC_MOKT_202 readFile lesen, wenn bei der Freischaltung der eGK mittels C2C die Rolle der dabei verwendeten Leistungserbringerkarte zum Lesen der GVD berechtigt ist.
[<=]

Die Berechtigung der Leistungserbringerkarte wird vorher im Schritt 5.3.2.2 geprüft.

Nicht berechtigte Rollen sind gemäß [gemSpec_eGK_P2] bzw. [gemSpec_eGK_ObjSys] CHA.7 (Mitarbeiter im Rettungswesen) und CHA.1 SMC–B eKiosk.

Die eGK enthält derzeit eine Kopie der GVD im EF.VD Container, welcher nicht zugriffsgeschützt ist.

VSDM-A_2783 - Fachmodul VSDM (mobKT): GVD nicht aus dem Container EF.VD lesen
Das Fachmodul VSDM (mobKT) DARF NICHT die GVD aus dem Container EF.VD der eGK lesen.
[<=]

5.3.2.6 Protokolleintrag auf eGK schreiben

VSDM-A_2720 - Fachmodul VSDM (mobKT): Protokolleintrag auf eGK schreiben
Das Fachmodul VSDM (mobKT) MUSS den Protokolleintrag zum Protokollieren der Lesezugriffe auf die GVD mittels TUC_MOKT_406 writeEGKAudit gemäß Tab_mobKT_ST2_15 erzeugen und in den Container EF.Logging schreiben.
[<=]

Tabelle 8: Tab_mobKT_ST2_15 – Durch das Fachmodul VSDM (mobKT) zu erzeugender Protokolleintrag

Data-Type	Type of Access	Auslöser
1	R	Erfolgreicher, lesender Zugriff auf die geschützten Versichertendaten.

5.3.2.7 PD, VD, GVD und StatusVD im Zwischenspeicher ablegen

VSDM-A_2721 - Fachmodul VSDM (mobKT): PD, VD, GVD und StatusVD im Zwischenspeicher ablegen
Das Fachmodul VSDM (mobKT) MUSS die von der eGK gelesenen PD, VD, GVD und StatusVD sowie die Protokollierungsdaten (Erfassungszeitpunkt und Zulassungsnummer) mittels TUC_MOKT_010 writeToInternalStorage im sicheren Zwischenspeicher ablegen, um den Schutzbedarf an die VSD durchzusetzen und dabei für den Zeitstempel die Systemuhr des Mobilen Kartenterminals verwenden.
[<=]

Die Sicherheitsmechanismen sind in Kapitel 3.5 beschrieben.

VSDM-A_2768 - Fachmodul VSDM (mobKT): Versichertendaten im Zwischenspeicher überschreiben
Das Fachmodul VSDM (mobKT) MUSS, falls die Daten des Versicherten in demselben Quartal bereits im Zwischenspeicher abgelegt wurden, die Versichertendaten im sicheren Zwischenspeicher überschreiben. Ein Überschreiben der Versichertendaten im Zwischenspeicher ist nur bezogen auf denselben Kartentyp (eGK bzw. KVK) möglich.
[<=]

Eindeutiges Identifikationskriterium des Versicherten auf der eGK ist die lebenslang gültige Krankenversichertennummer (10-stelliger unveränderlicher Teil). Die eindeutige Identifikation im mobKT erfolgt über diese KVNR. Für die KVK existiert kein eindeutiges Identifikationskriterium. Die Prüfung kann daher anhand der Kriterien Vorname, Nachname, Geburtsdatum erfolgen.

5.3.3 Versichertendaten von KVK im mobilen Einsatzszenario lesen

VSDM-A_2765 - Fachmodul VSDM (mobKT): Aktivitäten KVK Lesen
Das Fachmodul VSDM (mobKT) MUSS beim Lesen der Versichertendaten von der KVK die Aktivitäten gemäß Tab_mobKT_ST2_16 durchführen.
[<=]

Zusätzlich zu den in [gemSysL_VSDM] geforderten Aktivitäten müssen die Versichertendaten im Zwischenspeicher des Mobilen Kartenterminals abgelegt werden.

Tabelle 9: Tab_mobKT_ST2_16 – VSDM-UC_14 Aktivitäten

Schritt	Aktivität	TUCs
1	Versichertendaten von KVK lesen	TUC_MOKT_202 readFile
2	Versichertendaten prüfen	
3	Versichertendaten im Zwischenspeicher ablegen	TUC_MOKT_010 writeToInternalStorage
4	Anzeigen des gelesen Datensatzes im Display	

5.3.3.1 Versichertendaten von KVK lesen

VSDM-A_2730 - Fachmodul VSDM (mobKT): KVK Lesen
Das Fachmodul VSDM (mobKT) MUSS die Versichertendaten von der KVK mittels TUC_MOKT_202 readFile lesen
[<=]

5.3.3.2 Versichertendaten prüfen

Das Fachmodul VSDM (mobKT) muss die Vorgaben aus Anhang B – Prüfvorgaben KVK prüfen.

VSDM-A_2731 - Fachmodul VSDM (mobKT): KVK prüfen
Das Fachmodul VSDM (mobKT) MUSS, falls die Daten der KVK nicht den Vorgaben in Anhang B – Prüfvorgaben KVK entsprechen, den Lesevorgang mit der Fehlermeldung gemäß Tab_mobKT_ST_17 abrechen.
[<=]

Tabelle 10: Tab_mobKT_ST2_17 – Fehlerzustände Versichertendaten prüfen

Fehlerzustand	Auslöser	Fehlercode	Fehlermeldung (max. 26 Zeichen)
KVK Prüfsumme falsch, Daten korrupt	Die Überprüfung der Prüfsumme des KVK Satzes oder der Vorgaben aus Anhang B – Prüfvorgaben KVK ergab einen Fehler.	3021	Daten inkonsistent

VSDM-A_2732 - Fachmodul VSDM (mobKT): Felder hinzufügen
Das Fachmodul VSDM (mobKT) MUSS nach der KVK-Prüfung die Felder EinleseDatum, Zulassungsnummer und PrüfsummeZusatz gemäß Tab_mobKT_ST2_03 den Daten der KVK hinfügen.
[<=]

Tabelle 11: Tab_mobKT_ST2_03 Festformat des VersichertenDatenTemplates der KVK

Datenobjekt	Länge in Bytes	Format
EinleseDatum*	8	TTMMJJJJ
Zulassungsnummer*	38	alphanumerisch
PrüfsummeZusatz*	1	XOR

*) Die Datenfelder Zulassungsnummer, EinleseDatum und PrüfsummeZusatz sind nicht auf der KVK vorhanden und werden vom Mobilen Kartenterminal erzeugt. Der PrüfsummeZusatz wird über die Datenelemente EinleseDatum und ZulassungsNummer gebildet.

VSDM-A_2769 - Fachmodul VSDM (mobKT): "GültigkeitsDatum" mit der Systemuhr überprüfen
Das Fachmodul VSDM (mobKT) MUSS bei von der KVK eingelesenen Versichertendaten durch Vergleich des im Feld "GültigkeitsDatum" eingetragenen Wertes mit der Systemuhr überprüfen, ob das Gültigkeitsdatum der Karte überschritten ist und wenn das Gültigkeitsdatum überschritten ist, die Warnmeldung „Das Gültigkeitsdatum der Karte ist überschritten" auf allen Displays des Kartenterminals anzeigen.
[<=]

Zusätzlich kann auf diese Warnung optisch oder akustisch hingewiesen werden.

5.3.3.3 Versichertendaten im Zwischenspeicher ablegen

VSDM-A_2734 - Fachmodul VSDM (mobKT): VSD im Zwischenspeicher ablegen
Das Fachmodul VSDM (mobKT) MUSS die von der KVK gelesenen VSD mittels TUC_MOKT_010 writeToInternalStorage im sicheren Zwischenspeicher ablegen, um den Schutzbedarf an die VSD durchzusetzen.
[<=]

Die Sicherheitsmechanismen sind in Kapitel 3.5 beschrieben. Wurden die Daten des Versicherten im demselben Quartal bereits eingelesen, werden sie inklusive der Protokolldaten (Erfassungszeitpunkt und Zulassungsnummer) im Zwischenspeicher überschrieben. [VSDM-A_2768]

6 Anforderungen an das Mini-Primärsystem

Das Mini-PS hat die geforderten Anwendungsfälle bereitzustellen.

6.1 Abbildung fachlicher Anwendungsfälle auf technische Use Cases

Der Leistungserbringer kann die im Folgenden als Ellipsen dargestellten fachlichen Anwendungsfälle direkt über die Benutzerschnittstelle des Mobilen Kartenterminals auslösen. Abbildung 4 stellt die Anwendungsfälle der Fachanwendung VSDM im Mobilen Kartenterminal dar.

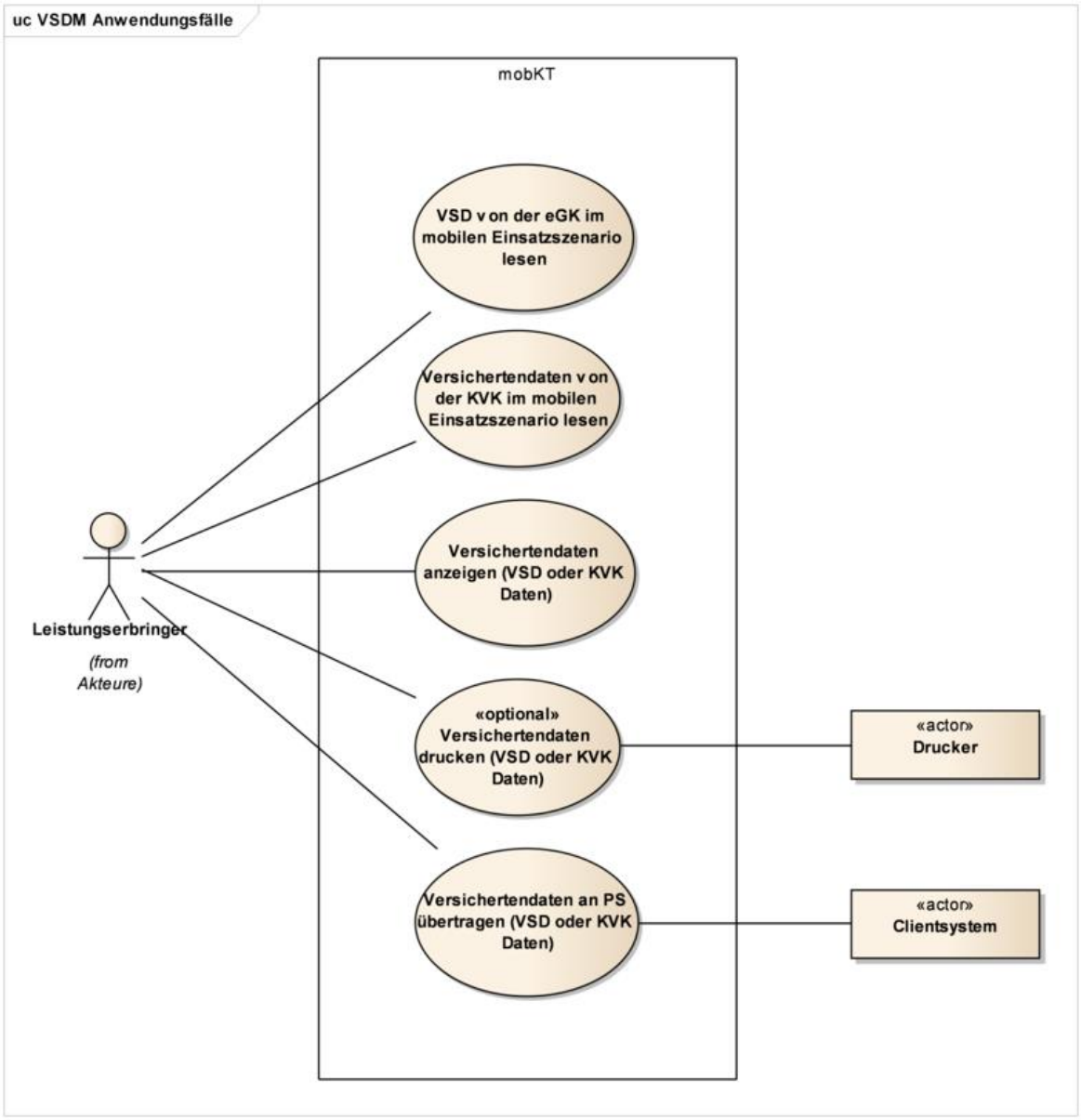


Abbildung 3: Anwendungsfälle der Fachanwendung VSDM

Abbildung 5 beschreibt Use Cases, die nicht von Fachanwendungen bereitgestellt werden.

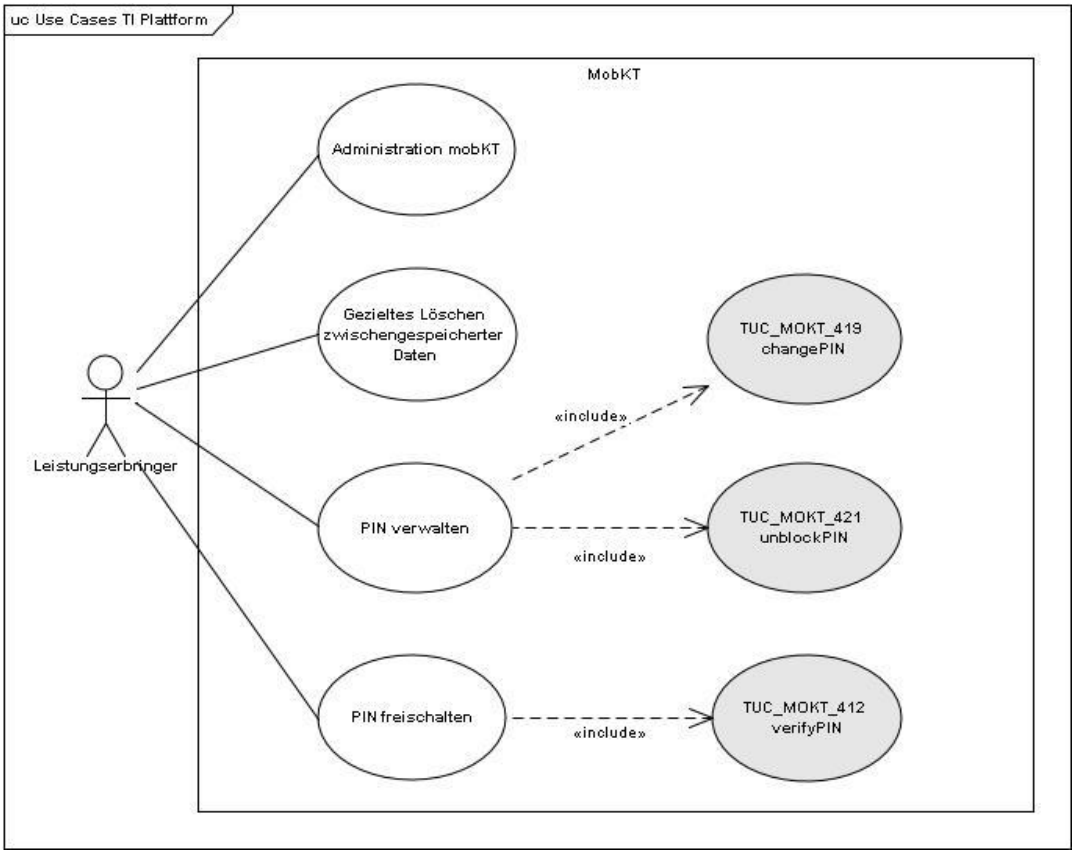


Abbildung 4: Nicht fachliche Anwendungsfälle

6.2 Benutzerführung

6.2.1 Allgemeine Anforderungen

TIP1-A_4974 - Anzeige Systemzeit
Das Mini-PS des Mobilen Kartenterminals MUSS die Systemzeit im Rahmen des Startvorgangs bis zum ersten fachlichen Aufruf mindestens einmal lesbar anzeigen.
[<=]

Hierunter fällt auch die Möglichkeit zur Anzeige der Systemzeit in der Betriebsbereitschaftsanzeige bzw. im Rahmen der Freischaltung der berechtigten Karte.

TIP1-A_4975 - Prüfung Systemzeit
Der Hersteller des Mobilen Kartenterminals MUSS in der Benutzerdokumentation den Leistungserbringer darauf hinweisen, dass er die Systemzeit regelmäßig zu prüfen hat.
[<=]

6.2.2 Fachliche Aufrufe

TIP1-A_4921 - Mobiles KT: Fachliche Anwendungsfälle
Das Mini-PS des Mobilen Kartenterminals MUSS die nach Kapitel 6.1 geforderten fachlichen Anwendungsfälle bereitstellen.
[<=]

Eventuelle automatische Aufrufe von fachlichen Abläufen, z. B. beim Stecken der eGK, können herstellerspezifisch angeboten werden(Gegebenenfalls auch konfigurierbar).

6.2.3 Warnmeldungen

Vom Zertifikatsdienst des Mini-AK wird geprüft, ob die Gültigkeit der berechtigten Karte gegeben ist.

TIP1-A_3872 - Mobiles KT: Information bei Ablauf der Zertifikatsgültigkeit
Das Mini-PS des Mobilen Kartenterminals SOLL zur Erhöhung der Benutzerfreundlichkeit den Leistungserbringer auf den Ablauf der Gültigkeit des Zertifikates zu dem konfigurierten Zeitpunkt, spätestens jedoch sechs Wochen vor Ablauf des X.509-Zertifikates (EF.C.HP.AUT bzw. EF.C.HCI.AUT) der berechtigten Karte (HBA oder SMC-B), aufmerksam machen.
[<=]

TIP1-A_3873 - Mobiles KT: Konfiguration Zeitpunkt Warnung vor Ablauf Zertifikatsgültigkeit
Das Mini-PS des Mobilen Kartenterminals SOLL dem Leistungserbringer ermöglichen, den Zeitpunkt der Warnung zum Ablauf der Gültigkeit des X.509-Zertifikates der berechtigten Karte (HBA oder SMC-B) zu konfigurieren.
[<=]

TIP1-A_3856 - Mobiles KT: Einschränkungen bei Ablauf der Zertifikatsgültigkeit
Der Hersteller des Mobilen Kartenterminals MUSS den Benutzer im Handbuch des Mobilen Kartenterminals über Einschränkungen im Falles des Ablaufs der Gültigkeit des Zertifikates der berechtigten Karte informieren.
[<=]

Weitere verpflichtende Warnmeldungen sind nicht umzusetzen. Herstellerspezifische Meldungen sind freigestellt.

6.2.4 Fehlermeldungen

TIP1-A_4261 - Mobile Szenarien: Mechanismen zur Fehleranzeige
Das Mobile Kartenterminal MUSS einen Fehler optisch (z. B. LED) signalisieren.
[<=]

Die Art der Signalisierung ist herstellerspezifisch.

TIP1-A_4426 - Mobiles KT: Fehlersignalisierung über erweitertes Display
Das Mobile Kartenterminal MUSS die Signalisierung eines Fehlers über das erweiterte Display mittels eines für den Nutzer verständlichen Textes sowie eines spezifischen Fehlercodes (hierbei müssen z.B. die Fehlercodes der TUCs des Mini-AK verwendet werden, welche exaktere Informationen über die Fehlerursache liefern) realisieren.
[<=]

TIP1-A_3697 - Mobile Szenarien: Interpretation der Fehleranzeige
Der Hersteller des Mobilen Kartenterminals MUSS die Interpretation des von dem mobilen Kartenterminal signalisierten Fehlers im Benutzerhandbuch beschreiben.
[<=]

TIP1-A_4266 - mobile Szenarien: Abfrage Statusinformation über Managementschnittstelle
Das Mobile Kartenterminal MUSS es dem Benutzer ermöglichen, dass eventuelle, zur Fehleranalyse notwendige weiterführende Informationen über die Managementschnittstelle des Geräts abgefragt werden können.
[<=]

6.3 Zwischenspeicher

TIP1-A_4404 - Zwischenspeicher zur Sicherung von Daten
Das Mini-PS des Mobilen Kartenterminals MUSS über einen Zwischenspeicher zur Speicherung von Daten verfügen.
[<=]

TIP1-A_3708 - Erhaltung zwischengespeicherter Daten ohne Strom
Das Mobile Kartenterminal SOLL in seinem Speicher die in ihm zwischengespeicherten Daten auch ohne Strom erhalten.
[<=]

TIP1-A_4412 - Erhaltung zwischengespeicherter Daten mittels Pufferbatterie
Das Mobile Kartenterminal MUSS, wenn der Speicher des Mobilen Kartenterminals nicht in der Lage ist, die Daten auch ohne Strom zu erhalten, über eine Pufferbatterie verfügen, um kurzzeitige Stromausfälle zu überbrücken.
[<=]

TIP1-A_4951 - Dimensionierung des Zwischenspeichers: Mindestanzahl zwischenzuspeichernder VSD
Das Mini-PS des Mobilen Kartenterminals SOLL seinen Zwischenspeicher so dimensionieren, dass mindestens 275 verschlüsselte VSD-Datensätze in der maximalen Größe samt zugehörigen Protokollierungsdaten zwischengespeichert werden können.
[<=]

Die maximale Größe eines VSD-Datensatzes lässt sich anhand der Größenangabe „numberOfOctet" in [gemSpec_eGK_ObjSys#5.4.2,5.4.4,5.4.9] berechnen. Zusätzlich sind die in [VSDM-A_2881] geforderten Erweiterungen zu berücksichtigen, wobei Zulassungsnummer und Prüfsumme nicht zwangsläufig zu jedem Datensatz zwischengespeichert werden müssen.

TIP1-A_4403 - Schutz der zwischengespeicherten Daten
Der Zwischenspeicher des Mini-PS des Mobilen Kartenterminals MUSS die in ihm zwischengespeicherten Daten vor Löschen, Überschreiben, unberechtigtem Auslesen und Manipulation über externe Schnittstellen schützen.
[<=]

TIP1-A_3756 - mobile Szenarien: Verschlüsselung zwischenzuspeichernder Daten
Das Mobile Kartenterminal MUSS sicherstellen, dass die zwischengespeicherten Daten mittels Verschlüsselungsdienst des Mini-AK unter Verwendung eines hybriden Verfahrens nach [gemSpec_Krypt] verschlüsselt sind.
[<=]

TIP1-A_3808 - Verschlüsselung zwischengespeicherter Daten
Das Mobile Kartenterminal MUSS sicherstellen, dass der symmetrische Schlüssel, mit dem die Daten verschlüsselt wurden, im Zuge des hybriden Verfahrens mit dem öffentlichen ENC-Key der freigeschalteten berechtigten Karte verschlüsselt wird.
[<=]

TIP1-A_3789 - Mobiles KT: unterschiedliche berechtigte Karten für die Verschlüsselung und Ablage von Daten im Zwischenspeicher
Das Mobile Kartenterminal MUSS die Nutzung von unterschiedlichen berechtigten Karten für die Verschlüsselung und Ablage von Daten im Zwischenspeicher des Mini-PS unterstützen.
[<=]

6.3.1 Zugriffsschutz Zwischenspeicher

TIP1-A_4270 - Zugriff auf zwischengespeicherte Daten erst nach Authentisierung zugelassen.
Das Mini-PS des Mobilen Kartenterminals MUSS sicherstellen, dass, bevor es Zugriff auf die Daten im Zwischenspeicher erlaubt, der autorisierte Benutzer einen aktiven Authentifizierungsstatus erreicht hat, was bedeutet, dass das Mini-PS Zugriff auf eine freigeschaltete berechtigte Karte (HBA oder SMC-B) hat, die im Kartenterminal-Modul gesteckt ist.
[<=]

TIP1-A_3722 - Verlust der aktiven Authentifizierungsstatus
Das Mobile Kartenterminal MUSS sicherstellen, dass, wenn die berechtigte Karte im mobilen Kartenterminal den Sicherheitszustand verliert oder das Mini-PS den Zugriff auf die berechtigte Karte verliert, der Benutzer seinen aktiven Authentifizierungsstatus verliert.
[<=]

TIP1-A_3710 - Manuelles Rücksetzen des Authentifikationsstatus
Das Mobile Kartenterminal MUSS dem Benutzer ermöglichen, den Sicherheitsstatus des Mobilen Kartenterminals aktiv zurückzusetzen, wobei die Karte den Sicherheitszustand verlieren MUSS.
[<=]

TIP1-A_3850 - Automatisches Rücksetzen des Sicherheitsstatus bei Inaktivität
Das Mobile Kartenterminal MUSS sicherstellen, dass der Sicherheitsstatus des Benutzers sowie der Sicherheitszustand der berechtigten Karte nach der konfigurierten Zeit bei Benutzerinaktivität zurückgesetzt wird.
[<=]

TIP1-A_3851 - Automatisches Rücksetzen des Sicherheitsstatus bei Abschalten
Das Mobile Kartenterminal MUSS sicherstellen, dass der Sicherheitsstatus des Benutzers sowie der Sicherheitszustand der berechtigten Karte bei Abschalten des Gerätes zurückgesetzt wird.
[<=]

TIP1-A_3759 - Verhalten bei Rücksetzen des Sicherheitsstatus
Das Mobile Kartenterminal MUSS sicherstellen, dass bei Rücksetzen des Sicherheitsstatus alle entschlüsselten Daten sowie temporär erzeugte Schlüssel im mobilen Kartenterminal gelöscht werden.
[<=]

6.4 Zwischenspeichern von Daten

Die in diesem Abschnitt beschriebenen Vorgaben sind vom Mini-PS bei der Durchführung der fachlichen Abläufe mit Zwischenspeicherung einzuhalten (siehe Kapitel 6.1). Das Mini-PS speichert die von der EGK gelesenen VSD mit Protokolldaten ab. Die abzuspeichernden Daten setzen sich folgendermaßen zusammen:

Die VSD bestehen aus:

- EF.StatusVD: Dem Status des Versichertendatensatzes
- EF.PD: Den persönlichen Versichertendaten
- EF.VD: Den allgemeinen Versicherungsdaten
- EF.GVD: Den geschützten Versichertenstammdaten

Die Protokolldaten bestehen aus:

- Dem Erfassungszeitpunkt des Datensatzes. Die Systemuhr des Mini-PS dient hierbei als Referenzuhr.
- Der Zulassungsnummer des Mobilen Kartenterminals mit welchem die Daten gelesen wurden.

TIP1-A_3733 - Erhalt eventuell vorhandener Daten eines Versicherten bei Fehler während des Zwischenspeicherns
Das Mobile Kartenterminal MUSS sicherstellen, dass, wenn während der Zwischenspeicherung ein Fehler auftritt bzw. die Daten nicht zwischengespeichert werden können, eventuell vorhandene Daten desselben Versicherten erhalten bleiben.
[<=]

Das Format, in dem die Daten verschlüsselt und zwischengespeichert werden, ist herstellerspezifisch. Der Ablauf ist in Kapitel 10.2.1 „TUC_MOKT_010 writeToInternalStorage" beschrieben.

TIP1-A_3798 - Mobiles KT: Keine Zwischenspeicherung zusätzlicher Daten
Das Mobile Kartenterminal DARF über die von Fachmodulen übergebenen Daten hinausgehende medizinische oder personenbezogene Daten des Versicherten wie z. B. Diagnoseschlüssel NICHT persistent speichern.
[<=]

6.5 Übertragen von Daten

Die in diesem Abschnitt beschriebenen Vorgaben sind vom Mini-PS bei der Durchführung der fachlichen Abläufe mit Übertragung von Daten zum Primärsystem einzuhalten (siehe Kapitel 6.1).

Die Übertragung der am Mobilen Kartenterminal zwischengespeicherten Daten an das Primärsystem erfolgt über eine Schnittstelle – protokollseitig auch Host-Schnittstelle genannt –, deren technische Ausprägung herstellerspezifisch sein kann (siehe auch Kapitel 3.3.6).

Es werden jeweils nur die Daten im Zwischenspeicher entschlüsselt und an das Primärsystem übertragen, die auch mit der berechtigten Karten zwischengespeichert wurden, die zur Übertragung an das Primärsystem verwendet wird.

TIP1-A_3694 - Mobile Szenarien: Zu übertragende Daten
Das Mini-PS des Mobilen Kartenterminals MUSS in der Lage sein, die zwischengespeicherten Daten an ein Primärsystem zu übertragen.
[<=]

TIP1-A_3691 - Übertragungsprotokoll bei herstellerspezifischer Host-Schnittstelle
Das Mobile Kartenterminal MUSS für die Übertragung zwischengespeicherter Daten an das Primärsystem CT-API gemäß [CT-API] als Protokoll verwenden.
[<=]

VSDM-A_2930 - Fachmodul VSDM (mobKT): Übertragungsformat der KVK-Daten an der Host-Schnittstelle
Das Fachmodul VSDM (mobKT) MUSS dem Benutzer wahlweise die Übertragung der KVK-Daten im ASN.1-Format oder im Festformat ermöglichen.
[<=]

Die Festlegung wird über Einstellungen innerhalb des Management-Moduls (siehe Kapitel 7.4.2) getroffen.

TIP1-A_3693 - Mobile Szenarien: Unverfälschtheit der Daten bei Übertragung
Das Mini-PS des Mobilen Kartenterminals MUSS seine Daten unverändert an das Primärsystem übertragen.
[<=]

TIP1-A_4272 - Mobile Szenarien: Fortschaltsperre
Das Mini-PS des Mobilen Kartenterminals MUSS bei der Übertragung von Datensätzen den übertragenen Datensatz mit der Ausführung des ersten READ Kommandos der Übertragung als übertragen markieren.
[<=]

TIP1-A_5374 - Mobile Szenarien: Fortschaltsperre, Nichtaufhebbarkeit der Markierung als übertragen
Das Mini-PS des Mobilen Kartenterminals MUSS sicherstellen, dass die Markierung eines Datensatzes als übertragen gemäß TIP1-A_4272 nicht aufgehoben werden kann, ohne den vollständigen Datensatz zu löschen.
[<=]

Eine erfolgreiche Übertragung der Daten wird vom Primärsystem angezeigt, indem es die übertragenen Daten im Rahmen des Übertragungsprotokolls explizit löscht.

TIP1-A_3695 - Mobile Szenarien: Sicherstellung der Fortschaltsperre während der Übertragung
Das Mini-PS des Mobilen Kartenterminals MUSS, falls ein als übertragen gekennzeichneter Datensatz am Mini-PS des mobilen Kartenterminal existiert, der mit der zur Übertragung verwendeten berechtigten Karte zwischengespeichert wurde, sicherstellen, dass nur dieser Datensatz an das Primärsystem übertragen werden kann (Fortschaltsperre).
[<=]

Um einen weiteren Datensatz lesen zu können, hat das Primärsystem den als übertragen markierten Datensatz zuerst zu löschen. Dadurch wird sichergestellt, dass der zuletzt übertragene Datensatz gelöscht wurde, bevor es den nächsten Datensatz übertragen kann (Fortschaltsperre).

Für die Übertragung von VSD muss das Mini-PS das in Kapitel 11 beschriebene Protokoll zur Kommunikation an der Host-Schnittstelle unterstützen.

TIP1-A_3871 - Mobile Szenarien: Übertragungsrhythmus zwischengespeicherter Daten
Der Hersteller des Mobilen Kartenterminals MUSS den Leistungserbringer in der Benutzerdokumentation darauf hinweisen, dass dieser die zwischengespeicherten Daten einmal täglich an sein Primärsystem übertragen soll.
[<=]

Dies ist insbesondere deswegen durchzuführen, weil die Daten mit der berechtigten Karte entschlüsselt werden müssen und dies im Falle des Verlustes nicht mehr durchgeführt werden kann.

6.5.1 Sonderfall Dockingstation

Falls das Mini-PS über einen Proxy (Dockingstation) an das Primärsystem angebunden wird, so muss der Proxy die Vorgaben, bezüglich der Schnittstellen und Protokolle zur Kommunikation mit dem Primärsystem, dieser Spezifikation erfüllen. Die interne Kommunikation zwischen Mini-PS und Proxy ist herstellerspezifisch, es muss jedoch sichergestellt werden, dass die zwischengespeicherten Daten (VSD), das jeweilige Erfassungsdatum und die Zulassungsnummer unverändert an das Primärsystem übertragen werden.

TIP1-A_3848 - Verhinderung von Ableiten von Daten durch die Dockingstation
Die Dockingstation des Mobilen Kartenterminals DARF, wenn das Mini-PS des Mobilen Kartenterminals über eine Dockingstation mit dem Primärsystem kommuniziert, die Daten NICHT über andere externe Schnittstellen als jene, die für die Übertragung der Daten an das Primärsystem vorgesehen sind, weitergeben.
[<=]

TIP1-A_3849 - Verhinderung von Zwischenspeichern von Daten durch die Dockingstation
Die Dockingstation des Mobilen Kartenterminals DARF, wenn das Mini-PS des Mobilen Kartenterminals über eine Dockingstation mit dem Primärsystem kommuniziert, die Daten NICHT dauerhaft speichern.
[<=]

TIP1-A_3855 - mobile Szenarien, Dockingstation: Löschen des Zwischenspeichers nach Übertragung
Die Dockingstation des Mobilen Kartenterminals MUSS, wenn das Mini-PS des mobilen Kartenterminal über diese mit dem Primärsystem kommuniziert, jeden Datensatz nach seiner Übertragung aus ihrem Speicher löschen.
[<=]

6.6 Gezieltes Löschen von zwischengespeicherten Daten

TIP1-A_4258 - Mobile Szenarien: Manuelles Löschen zwischengespeicherter VSD
Das Mini-PS des Mobilen Kartenterminals MUSS dem Benutzer ermöglichen, alle zwischengespeicherten Datensätze manuell, ohne vorherige Übertragung zu löschen.
[<=]

TIP1-A_3714 - Möglichkeit zum manuellen Löschen bereits übertragener Daten
Das Mobile Kartenterminal MUSS dem Benutzer ermöglichen, als übertragen markierte Datensätze am Mini-PS manuell zu löschen.
[<=]

TIP1-A_4259 - Mobile Szenarien: Einzelnes Löschen der zwischengespeicherten Daten
Das Mini-PS des Mobilen Kartenterminals MUSS dem Benutzer ermöglichen, gezielt einzelne Datensätze zu löschen.
[<=]

Einzelnes Löschen kann entweder direkt am Mini-PS im Rahmen der Benutzerführung durchgeführt werden oder über die Primärsystemschnittstelle. Die Ausprägung des Löschmechanismus ist herstellerspezifisch.

6.7 PIN-Verwaltung

In Abhängigkeit vom Zustand der berechtigten Karte (HBA oder SMC-B) muss das Mobile Kartenterminal dem Leistungserbringer die Möglichkeit anbieten, die PIN zu ändern bzw. die blockierte Karte mit Hilfe der PUK (Personal Unblocking Key) zu entsperren (siehe Kapitel 6.1).

6.7.1 PIN ändern

TIP1-A_3790 - Mobiles KT: PIN-Änderung für HBA und SMC-B über Benutzerschnittstelle
Das Mobile Kartenterminal MUSS dem Leistungserbringer ermöglichen, an der Benutzerschnittstelle die PIN.CH eines HBA und die PIN.SMC einer SMC-B ändern bzw. die mit einem Transportschutz versehene PIN.CH oder PIN.SMC in eine Echt-PIN umzuwandeln zu können.
[<=]

Für die Funktionalität „PIN ändern" sei auf den technischen Use Case TUC_MOKT_419 changePIN verwiesen.

6.7.2 PIN entsperren

Die Karten haben einen Wiederholungszähler für die fehlerhafte PIN-Eingabe. Bei jeder Fehleingabe wird dieser Zähler dekrementiert. Erreicht der Zähler Null, wird die Karte in den Zustand „blockiert" gesetzt, indem keine weiteren PIN-Eingaben mehr möglich sind. Mit Hilfe der PUK können dieser Zustand und der Zähler zurückgesetzt werden.

TIP1-A_3791 - Mobiles KT: PIN-Entsperren bei blockiertem HBA oder SMC-B
Das Mobile Kartenterminal MUSS es dem Leistungserbringer ermöglichen, die PIN entsperren zu können, wenn es erkennt, dass sich der HBA oder die SMC-B im Zustand "blockiert" befindet.
[<=]

Für die Funktionalität „PIN entsperren" sei auf den technischen Use Case TUC_MOKT_421 unblockPIN verwiesen.

6.8 Daten drucken

Die in diesem Abschnitt beschriebenen Vorgaben sind vom Mini-PS bei der Durchführung des fachlichen Ablaufs „Daten drucken" einzuhalten (siehe Kapitel 6.1).

TIP1-A_3809 - Kommunikation zwischen Mini-PS und Drucker
Das Mini-PS des Mobilen Kartenterminals KANN mit einem Drucker kommunizieren, um Daten ausdrucken zu können.
[<=]

TIP1-A_3811 - mobile Szenarien Ausdruck von Daten: Eingabe von Arzt- und Betriebsstättennummer während Druckvorgang
Das Mobile Kartenterminal MUSS dem Nutzer ermöglichen, vor dem Starten des Druckvorganges eventuell voreingestellte Werte für Betriebsstättennummer und Arztnummer zu ändern.
[<=]

Dies kann sowohl eine temporäre Änderung nur für einen Druckvorgang als auch eine dauerhafte ab diesem Druckvorgang sein. Somit kann diese Anforderung sowohl über die Managementfunktion umgesetzt werden als auch über einen Interaktionspunkt vor dem Start eines Druckvorgangs.

7 Anforderungen an das Management-Modul

7.1 Allgemeine Anforderungen

TIP1-A_3740 - Konfigurationsschnittstelle
Das Mobile Kartenterminal MUSS über eine Schnittstelle zur Administration verfügen.
[<=]

TIP1-A_3731 - Aktionen zur Diagnose von Betriebs und Fehlerzuständen über die Managementschnittstelle
Die Managementschnittstelle des Mobilen Kartenterminals MUSS für die Diagnose von Betriebs- und Fehlerzuständen mindestens folgende Aktionen ermöglichen:

- Anzeige der aktuellen Konfiguration,
- Abfragen der aktuellen Softwareversion.

[<=]

TIP1-A_3728 - Export und Import von Konfigurationsdaten über die Managementschnittstelle
Das Mobile Kartenterminal KANN den Export und Import der Konfigurationsdaten über die Managementschnittstelle ermöglichen.
[<=]

TIP1-A_3737 - mobile Szenarien Konfiguration: Export/Import von Konfigurationsdaten
Das Mobile Kartenterminal MUSS, wenn es den Import von Konfigurationsdaten über die Managementschnittstelle ermöglicht, diesen Import nur für baugleiche Geräte gewährleisten.
[<=]

TIP1-A_3729 - Einschränkungen der exportierbaren Konfigurationsdaten
Das Mobile Kartenterminal DARF, wenn Konfigurationsdaten über die Managementschnittstelle exportiert werden können, es NICHT ermöglichen, dass Schlüsselmaterial als Bestandteil der Konfigurationsdaten exportiert werden kann.
[<=]

TIP1-A_3741 - Rolle Administrator an der Managementschnittstelle
Das Mobile Kartenterminal MUSS an der Managementschnittstelle die Rolle Administrator vorsehen.
[<=]

Es können weitere Rollen z. B. Benutzer existieren.

TIP1-A_3742 - Berechtigungen der Rolle Administrator an der Managementschnittstelle
Das Mobile Kartenterminal MUSS sicherstellen, dass ausschließlich der Administrator berechtigt ist, Firmware Updates einzuspielen.
[<=]

TIP1-A_3859 - Berechtigungen der optionalen Rollen an der Managementschnittstelle
Das Mobile Kartenterminal MUSS sicherstellen, dass Rollen für die Administration - außer der Rolle Administrator - nur berechtigt sind, die aktuellen Einstellungen sich anzeigen zu

lassen und das Kennwort des jeweiligen Benutzers zu ändern.
[<=]

TIP1-A_3726 - Schutz der Managementschnittstelle vor unberechtigtem Zugriff
Das Mobile Kartenterminal MUSS die Managementschnittstelle vor unberechtigtem Zugriff schützen.
[<=]

TIP1-A_3727 - Schutz der Managementschnittstelle durch Username und Passwort
Das Mobile Kartenterminal MUSS sicherstellen, dass die Managementschnittstelle des Mobilen Kartenterminals durch eine Kombination aus Username und Passwort oder einen mindestens gleich starken Mechanismus vor unberechtigtem Zugriff geschützt ist.
[<=]

TIP1-A_4269 - Authentifikation der Rolle Administrator
Das Mobile Kartenterminal KANN, wenn ausschließlich die Rolle Administrator implementiert ist, während der Authentifikation auf die Abfrage des Usernamen verzichten.
[<=]

TIP1-A_4941 - Mobiles KT: Hinweis Administratorauthentisierung
Das Managementmodul des Mobilen Kartenterminals MUSS im Fall, dass die Angabe des Usernamens gemäß [TIP1-A_4269] entfällt, bei der Eingabe des Kennwortes anzeigen, dass es sich um eine Administratorauthentisierung handelt.
[<=]

TIP1-A_5006 - Dokumentation der Konfiguration
Der Hersteller des Mobilen Kartenterminals MUSS den Anwender bzw. den Administrator in geeigneter Form (z. B. in der Benutzerdokumentation) über alle für die Konfiguration notwendigen Parameter einschließlich nötiger Eigenschaften (z. B. Zweck, Wertebereich, Abhängigkeiten) informieren.
[<=]

7.2 Kennwörter zur Sicherung der Managementschnittstelle

Im Folgenden werden die Anforderungen an die Kennwörter zur Sicherung der Managementschnittstellen aufgeführt.

TIP1-A_4268 - mobile Szenarien: Geschütztes Speichern von Kennwörtern
Das Mobile Kartenterminal MUSS sicherstellen, dass Kennwörter geschützt gespeichert werden, so dass sie nicht über externe Schnittstellen ausgelesen oder verändert werden können.
[<=]

Für alle Kennwörter zur Sicherung der Managementschnittstelle gelten folgende Anforderungen.

TIP1-A_3764 - Mindestlänge, zulässige Zeichen für Kennwörter
Das Mobile Kartenterminal MUSS sicherstellen, dass Kennwörter mindestens 8 Zeichen lang sind und mindestens aus Ziffern (‚0' bis ‚9') bestehen.
[<=]

TIP1-A_3749 - mobile Szenarien: weitere Zulässige Zeichen für Kennwörter
Das Mobile Kartenterminal KANN Kennwörter, die aus einer Mischung aus Ziffern, Buchstaben und Sonderzeichen bestehen, verwenden.
[<=]

TIP1-A_3750 - mobile Szenarien: Username nicht als Bestandteil des Kennwortes
Das Mobile Kartenterminal MUSS sicherstellen, dass der Username als Teilzeichenkette nicht Bestandteil des Kennwortes sein kann.
[<=]

TIP1-A_3751 - mobile Szenarien: Kennwörter nicht auf programmierbaren Funktionstasten
Das Mobile Kartenterminal MUSS sicherstellen, dass Kennwörter nicht auf programmierbaren Funktionstasten gespeichert werden können.
[<=]

TIP1-A_3752 - mobile Szenarien: Keine Klartextanzeige des Kennwortes während Eingabe
Das Mobile Kartenterminal DARF bei der Eingabe des Kennwortes dieses NICHT im Klartext anzeigen.
[<=]

TIP1-A_3834 - mobile Szenarien: Fehlerzähler für Falscheingaben von Kennworten
Das Mobile Kartenterminal MUSS für jedes Kennwort einen Fehlerzähler für die Fehlversuche bei der Kennworteingabe vorhalten.
[<=]

TIP1-A_3753 - mobile Szenarien: Sicherung des Fehlerzählers vor Veränderung
Das Mobile Kartenterminal MUSS sicherstellen, dass der Fehlerzähler nicht über externe Schnittstellen verändert werden kann.
[<=]

TIP1-A_5007 - mobile Szenarien: Abfrage Fehlerzähler
Das Mobile Kartenterminal KANN Fehlerzähler falscher Kennworteingaben von einem Benutzer abfragbar machen.
[<=]

TIP1-A_3835 - mobile Szenarien: Sperrzeiten bei mehrfachen Fehlversuchen der Kennworteingabe
Das Mobile Kartenterminal MUSS den Zugang des jeweiligen Benutzers oder Administrators zur direkten Managementschnittstelle ab der dritten aufeinander folgenden ungültigen Kennworteingabe sperren, wobei die Dauer der Sperrzeit von der Anzahl aufeinander folgender Fehlversuche abhängig sein MUSS.

Tabelle 12: Mindestsperrzeiten in Abhängigkeit der Anzahl ungültiger Kennworteingaben

Anzahl der aufeinander folgenden ungültigen Kennworteingaben	Mindestsperrzeit für die Kennworteingabe
3-6	1 Minute
7-10	10 Minuten
11-20	1 Stunde
ab 21	1 Tag

[<=]

TIP1-A_3836 - mobile Szenarien: Erhalt des Fehlerzählers im spannungslosen Zustand
Das Mobile Kartenterminal MUSS Fehlerzähler falscher Kennworteingaben im spannungslosen Zustand erhalten.
[<=]

TIP1-A_3837 - mobile Szenarien: Erhalt der verstrichenen Wartezeit im spannungslosen Zustand
Das Mobile Kartenterminal KANN die bereits verstrichene Sperrzeit während einer Administratorenpasswort-Eingabe im spannungslosen Zustand erhalten und den Zugang nach Neustart nur für die verbleibende Zeit sperren.
[<=]

TIP1-A_3838 - mobile Szenarien: Wartezeit nach Reset ohne Erhalt der verstrichenen Wartezeit
Das Mobile Kartenterminal MUSS, falls es die bereits verstrichene Wartezeit nicht im spannungslosen Zustand erhält, die Sperrzeit nach einem Neustart, unabhängig von der bereits verstrichenen Sperrzeit, wieder der dem Fehlerzähler entsprechenden Mindestsperrzeit setzen.
[<=]

Zusätzliche, nicht normative Informationen zur Handhabung von Kennwörtern sind im vom BSI herausgegebenen Maßnahmenkatalog Organisation (M 2) Abschnitt 11 „Regelungen des Passwortgebrauchs" [BSI_2005#2.11] beschrieben.

7.3 Durchführen und Anzeigen Ergebnis-Selbsttest

TIP1-A_3760 - Softwareselbsttest
Das Mobile Kartenterminal MUSS dem Nutzer ermöglichen, die Korrektheit der installierten Software überprüfen und erkennen zu können (Selbsttest).
[<=]

7.4 Konfigurationsbereiche

Dem Architekturansatz der Unterteilung in verschiedene Module folgend, muss das Management-Modul für alle anderen Module Konfigurationsmöglichkeiten bereitstellen.

Die Mechanismen der Konfiguration sind herstellerspezifisch.

7.4.1 Konfiguration des Kartenterminal-Moduls

Für das Kartenterminal-Modul sind keine verpflichtenden Konfigurationsmöglichkeiten vorgesehen. Herstellspezifische Einstellungen sind freigestellt.

7.4.2 Konfiguration des Mini-PS

VSDM-A_2931 - Fachmodul VSDM (mobKT): Konfigurationsmöglichkeit Festformat
Das Mini-PS des Mobilen Kartenterminals MUSS es dem Benutzer ermöglichen, das Format der Datenübertragung (Festformat oder ASN.1) einstellen zu können.
[<=]

Das Mini-PS muss des Weiteren das Einstellen des Zeitraums, ab welchem vor Ablauf eines Zertifikates eine Warnung erscheinen muss (siehe Kapitel 6.2) [TIP1-A_3873], ermöglichen.

7.4.3 Konfiguration des Mini-AK

TIP1-A_3725 - Managementschnittstelle zu Diagnose- und Konfigurationszwecken des Mini-AKs
Der Mini-AK des Mobilen Kartenterminals MUSS über eine Managementschnittstelle für Konfiguration und Diagnose verfügen.
[<=]

TIP1-A_3730 - Einstellungsmöglichkeiten über die Managementschnittstelle des Mini-AKs im Falle einer Einboxlösung
Die Managementschnittstelle des Mobilen Kartenterminals MUSS für die Konfiguration des Mini-AKs des Mobilen Kartenterminals als Einboxlösung folgende Einstellungen ermöglichen:

- Sicherheitsinformationen
  a. Import (offline) von Cross-CVCs.

[<=]

Die durch die CVC-Root-CA für die Verwendung in der TI ausgegebenen Cross-CV-Zertifikate werden auf einem Server der CVC-Root-CA sowie in der TSL veröffentlicht (siehe [gemSpec_TSL]) und können dort entnommen werden. Eine ggf. notwendige Aufbereitung für den Import in das Mobile Kartenterminal erfolgt in Abhängigkeit vom implementierten Verfahren herstellerspezifisch. Um den Betrieb des Mobilen Kartenterminals mit Karten unterschiedlicher Roots nach einem planmäßigen (siehe [gemSpec_CVC_Root#TIP1-A_5215]) oder unplanmäßigen Root-Wechsel (siehe [gemSpec_CVC_Root#TIP1-A_5218]) zu ermöglichen, müssen diese Cross-CVCs im Mobilen Kartenterminal vorhanden sein.

TIP1-A_6484 - Anzahl Cross-CVCs
Das Mobile Kartenterminal MUSS zu einem Zeitpunkt mindestens sechzehn Cross-CV-Zertifikate speichern können.
[<=]

7.4.4 Konfiguration der Fachanwendungen

7.4.4.1 Fachmodul VSDM

Dieses Kapitel hat beabsichtigt keinen Inhalt. Es bleibt jedoch bestehen, um die Kapitelstruktur im Hinblick auf mögliche Verweise beizubehalten.

7.4.5 Konfiguration der Systemuhr

Die Systemzeit setzt sich aus Datum und Uhrzeit zusammen, wobei zwischen Datum, bestehend aus Jahr, Monat und Tag und Uhrzeit, bestehend aus Stunden, Minuten und Sekunden unterschieden wird.

TIP1-A_3745 - Systemuhr im Mini-PS: Aufteilung in Datum und Uhrzeit
Das Mobile Kartenterminal MUSS sicherstellen, dass, wenn keine VSD zwischengespeichert sind, die Uhrzeit und das Datum einstellbar sind.
[<=]

TIP1-A_4414 - Einschränkungen an das Einstellen des Datums bei zwischengespeicherten Daten
Das Mobile Kartenterminal MUSS sicherstellen, dass das einstellbare Datum der Systemuhr nicht veränderbar ist, solange noch VSD im Mini-PS des Mobilen Kartenterminals zwischengespeichert sind.
[<=]

Die Uhrzeit ist von dieser Einschränkung nicht betroffen und kann immer geändert werden.

7.4.6 Konfiguration der optionalen Druckerschnittstelle

TIP1-A_3810 - Aufnahme von Arzt- und Betriebstättennummer über das Mini-PS
Das Mobile Kartenterminal MUSS, wenn das Mini-PS des Mobilen Kartenterminals über die Möglichkeit verfügt, Daten an einen Drucker zu übertragen und auszudrucken, die Eingabe einer 9-stelligen Arztnummer und einer 9-stelligen Betriebsstättennummer ermöglichen.
[<=]

TIP1-A_3832 - Persistente Speicherung von Arzt- und Betriebsstättennummer am Mini-PS
Das Mini-PS des Mobilen Kartenterminals SOLL die Arzt- und Betriebsstättennummer (so vorhanden) persistent speichern.
[<=]

TIP1-A_4415 - Mobiles KT: konfigurierbares Druckmodul
Das Mobile Kartenterminal MUSS es ermöglichen, das Druckmodul mittels Konfiguration an geänderte Druckvorschriften anpassen zu können. Eine Realisierung der Anpassung an geänderte Druckvorschriften für über diese Konfigurationsmöglichkeiten des Druckmoduls hinausgehende komplexe Änderungen bleibt hiervon unberührt.
[<=]

Es wird empfohlen, dass das Mobile Kartenterminal so flexibel wie möglich an Änderungen der Druckvorschriften angepasst werden kann, ohne dass ein FW-Update notwendig ist. Unter flexibler Anpassbarkeit wird verstanden, dass

- Felder bezüglich Druckzeile und Position auf dem Formularkopf frei positioniert werden können,
- die Anzeige einzelner Felder aktiviert und deaktiviert werden kann und
- ggf. zusätzliche Felder mit Konfigurationswerten belegt werden können.

TIP1-A_6059 - Mobiles KT: flexibel konfigurierbares Druckmodul
Das Mobile Kartenterminal SOLL über die in [TIP1-A_4415] beschriebene Konfigurierbarkeit hinaus ein von der Firmware unabhängiges Druckmodul besitzen, welches eine Anpassung des Formularkopfdrucks an geänderte Druckvorschriften gemäß [KBV_ITA_VGEX_Mapping_KVK] erlaubt. Der Hersteller des Mobilen Kartenterminals SOLL bei Änderung der Druckvorschriften zeitnah, spätestens jedoch 6 Monate nach Veröffentlichung der Änderung, eine aktualisierte Version des Druckmoduls, welches diese Änderungen umsetzt, zur Verfügung stellen.
[<=]

Nur bei Geräten, die auf Basis eines migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 zugelassen werden, kann auf eine Umsetzung von [TIP1-A_6059] verzichtet werden.

TIP1-A_6060 - Mobiles KT: Zulassung einer neuen Version des Druckmoduls
Der Hersteller MUSS eine aktualisierte Version des Druckmoduls bei der gematik zur Zulassung einreichen.
[<=]

Die gematik wird im Rahmen der Veröffentlichung der Zulassungen die Information über eine neue Version des Druckmoduls und die durch diese Version des Druckmoduls umgesetzte Version der Bedruckungsvorschriften ebenfalls veröffentlichen.

7.4.7 Konfiguration des automatischen Rücksetzens des Sicherheitszustand bei Benutzerinaktivität

TIP1-A_5145 - Konfigurierbarkeit der Benutzerinaktivitätszeit
Das Mobile Kartenterminal MUSS dem Administrator ermöglichen, dass die Zeit bis zum automatischen Rücksetzen des Sicherheitszustands bei Benutzerinaktivität gemäß [TIP1-A_3850] konfigurierbar ist.
[<=]

TIP1-A_5146 - Intervall der Benutzerinaktivitätszeit
Das Mobile Kartenterminal MUSS für die Konfigurationsmöglichkeit gemäß [TIP1-A_5145] ausschließlich die Einstellung der Zeit von 1 bis 60 Minuten ermöglichen.
[<=]

TIP1-A_5147 - Benutzerinaktivitätszeit im Auslieferungszustand
Das Mobile Kartenterminal MUSS für die Benutzerinaktivitätszeit gemäß [TIP1-A_5145] den Wert von 60 Minuten im Auslieferungszustand aufweisen.
[<=]

8 Anforderungen an das erweiterte Display

TIP1-A_3854 - Mobiles Kartenterminal: erweitertes Display
Das Mobile Kartenterminal MUSS über ein erweitertes Display verfügen.
[<=]

TIP1-A_3723 - Dimensionierung des erweiterten Displays
Das erweiterte Display des Mobilen Kartenterminals MUSS mindestens ein Grafik-Display sein.
[<=]

TIP1-A_3843 - Mindestanzahl an durch ein erweitertes Display darstellbaren Zeilen und Zeichen
Das erweiterte Display des Mobilen Kartenterminals SOLL bei kleinster Schriftgröße mindestens 8 Zeilen á 16 Zeichen darstellen können.
[<=]

TIP1-A_3844 - Am erweiterten Display darstellbarer Zeichensatz
Das erweiterte Display des Mobilen Kartenterminals MUSS mindestens ISO-8859-15 kodierten Text darstellen können.
[<=]

TIP1-A_5085 - Beleuchtung erweitertes Display
Das erweiterte Display des Mobilen Kartenterminals SOLL beleuchtet sein, um einen Betrieb bei schlechten Lichtverhältnissen zu ermöglichen.
[<=]

Nur bei Geräten, die auf Basis eines migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 zugelassen werden, kann auf eine Umsetzung verzichtet werden.

8.1 Kommunikation mit dem erweiterten Display

TIP1-A_3853 - Externes Display am Mini-PS
Das Mobile Kartenterminal MUSS, wenn das erweiterte Display nicht in das Gehäuse des Mobilen Kartenterminals integriert ist, eine lokale Schnittstelle für den Anschluss des erweiterten Displays anbieten.
[<=]

TIP1-A_3762 - Verbindung zwischen Mini-PS und erweitertem Display
Das Mobile Kartenterminal MUSS, falls das erweiterte Display nicht in das Gehäuse des Mobilen Kartenterminals integriert ist, die Datenübertragung zwischen Mini-PS und erweitertem Display so realisieren (z.B. durch Kabel im Sichtbereich), dass es dem Leistungserbringer ermöglicht sicherzustellen, dass die Daten ausschließlich an das zur Übertragung bestimmte erweiterte Display gesendet werden.
[<=]

Die physikalische Ausprägung der Schnittstelle zwischen erweitertem Display und Mobilen Kartenterminal ist herstellerspezifisch.

8.2 Nutzbarkeit für das Kartenterminal-Modul

TIP1-A_4425 - Verwendung des erweiterten Displays zur PIN-Eingabe
Das erweiterte Display des Mobilen Kartenterminals MUSS, wenn es in das Gehäuse des Mobilen Kartenterminals integriert ist und die Anforderungen an das Display zur PIN-Eingabe erfüllt, als Display zur PIN-Eingabe verwendet werden.
[<=]

9 Anforderungen an die Systemuhr

TIP1-A_3709 - Erhaltung Systemzeit mittels Pufferbatterie
Das Mobile Kartenterminal MUSS über ein einstellbares Datum und eine einstellbare Uhrzeit mit batteriegepufferter Systemuhr verfügen.
[<=]

Ebenso benötigt der Mini-AK für die Zugriffsprotokollierung auf der eGK eine verlässliche Systemuhr. Anforderungen bezüglich der Einstellungen der Systemuhr sind in Kapitel 7.4.5 zu finden.

TIP1-A_3732 - Mobile Szenarien: Freilaufgenauigkeit eingesetzter Systemuhren
Das Mobile Kartenterminal MUSS sicherstellen, dass die eingesetzten Systemuhren eine Freilaufgenauigkeit von mindestens ±100ppm (das einspricht 52,6 min in 365 Tagen) besitzen.
[<=]

10 Technische Use Cases

10.1 Technische Use Cases des Mini-AK

Das Verhalten der Basisdienste des Mini-AK wird im Folgenden mittels technischer Anwendungsfälle (Technical Use Case, kurz TUC) beschrieben. Dadurch wird erreicht, dass die entsprechenden Funktionsblöcke in den Fachmodulen und im Mini-AK nicht mehrfach dargestellt werden müssen.

In Abschnitt 5.3 sind die von Fachmodulen umzusetzenden Anwendungsfälle definiert. Die Fachmodule referenzieren die TUCs dieses Abschnitts, die die entsprechende Funktionalität eines Anwendungskonnektors für das Mobile Kartenterminal angepasst modelliert.

10.1.1 TUC_MOKT_200 sendAPDU

TIP1-A_3768 - Mobiles KT: „TUC_MOKT_200 sendAPDU“
Das Mobile Kartenterminal MUSS den technischen Use Case „TUC_MOKT_200 sendAPDU" gemäß Tab_MOKT_100 umsetzen.
[<=]

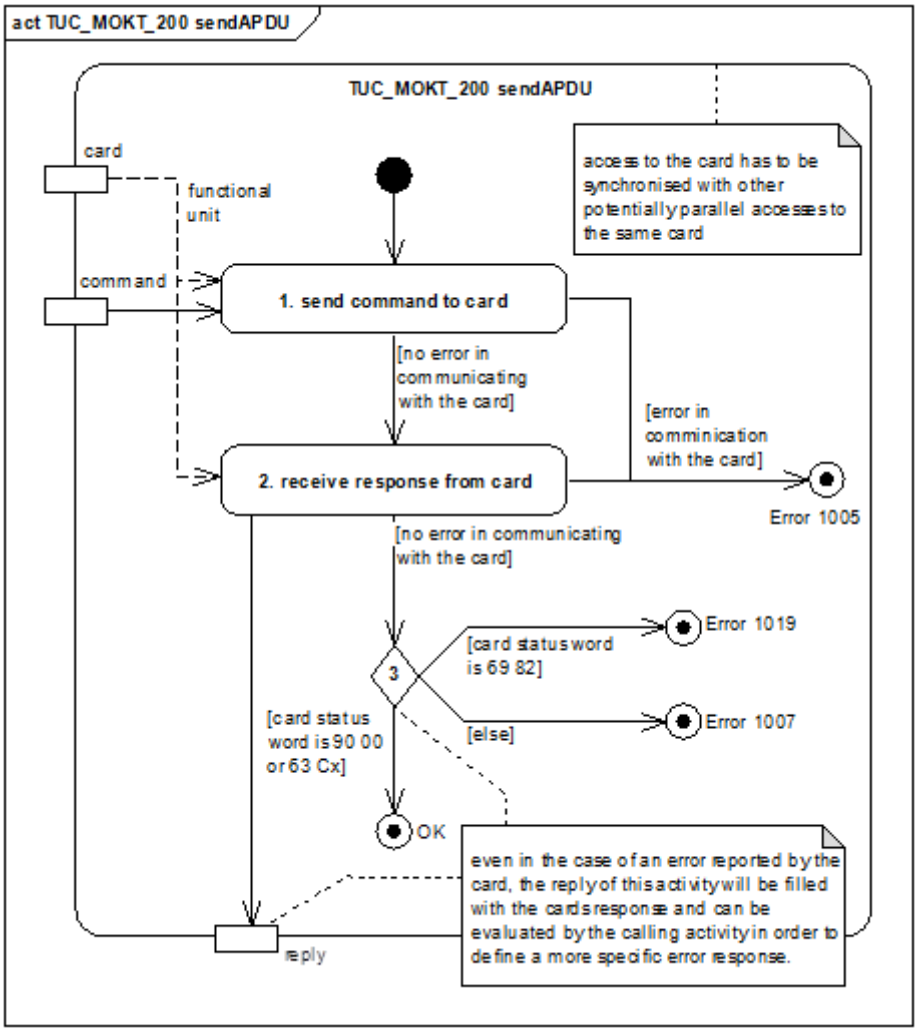


Abbildung 5: Pic_MOKT_001 Aktivitätsdiagramm zu TUC_MOKT_200 sendAPDU

Tabelle 13: Tab_MOKT_100 - TUC_MOKT_200 sendAPDU

TUC_MOKT_200 sendAPDU	
Beschreibung	TUC_MOKT_200 überträgt ein Kartenkommando an die Karte und nimmt die Antwort entgegen.
Anwendungsumfeld	Zugriff auf eine Karte im MobKT
Initiierender Akteur	MobKT
Weitere Akteure	Karte
Auslöser	TUC_MOKT_202 readFile TUC_MOKT_209 readRecord TUC_MOKT_214 appendRecord TUC_MOKT_250 selectCardFile TUC_MOKT_405 authenticateCardToCard TUC_MOKT_407 selectKeyForAsymmetricExternalAuthentication TUC_MOKT_412 verifyPIN TUC_MOKT_418 checkEGK

	TUC_MOKT_419 changePIN TUC_MOKT_471 decryptData	
Vorbedingungen	keine	
Nachbedingungen	keine	
Eingangsdaten	• card: Karte an die das Kommando gesendet werden soll • command: Kommando (APDU), das an die Karte gesendet werden soll	
Ausgangsdaten	• Antwort (APDU) der Karte	
Weitere Informationsobjekte	keine	
Standardablauf	1. Der Mini-AK MUSS das Kommando (command) über das Kartenterminal-Modul an die Karte (card) übertragen. 2. Der Mini-AK MUSS die Antwort der Karte (card) vom Kartenterminal-Modul empfangen. 3. Wenn die Karte mit dem Status NoError oder UpdateRetryWarning geantwortet hat, MUSS der Mini-AK den TUC_MOKT_200 mit OK beenden.	
Varianten/Alternativen	• Wenn es sich um eine synchrone Chipkarte nach [ISO7816-10] (z. B. KVK) handelt, MUSS das MobKT das Kommando wie in [MKT_10#Teil 7] beschrieben auf Interaktion mit der synchronen Chipkarte abbilden.	
Fehlerfälle	• 1, 2: wenn die Übertragung des Kommandos an die Karte in Schritt 1 oder der Empfang der Antwort in Schritt 2 scheitert, MUSS der Mini-AK TUC_MOKT_200 mit Fehler 1005 beenden. • 3: Wenn die Karte mit dem Status SecurityStatusNotSatisfied geantwortet hat, MUSS der Mini-AK TUC_MOKT_200 mit dem Fehler 1019 beenden • 3: Wenn die Karte mit einem anderen Status als NoError, SecurityStatusNotSatisfied oder UpdateRetryWarning geantwortet hat, MUSS der Mini-AK TUC_MOKT_200 mit dem Fehler 1007 beenden.	
Technische Fehlermeldungen	**Fehler Code**	**Bedeutung**
	1005	Kommunikationsfehler mit Kartenterminal-Modul oder Karte
	1007	Fehler beim Zugriff auf die Karte
	1019	Kartenzugriff verweigert
Weitere Anforderungen	Das MobKT MUSS Kartenkommandos, die voneinander abhängig sein können, pro Steckzyklus einer Karte im selben logischen Kanal (im Sinne der ISO 7816-4) an die Karte senden. Dieser Kanal KANN der Basiskanal 0 sein. Der Mini-AK MUSS potentiell parallele Zugriffe auf die Karten soweit synchronisieren, dass die Übertragung der Daten zu	

	und von den Karten und die Zuordnung der Antwort zu einem Kommando nicht beeinträchtigt wird.
Anmerkungen, Bemerkungen	Die Kommunikation zwischen Karte und Kartenterminal ist Basisfunktionalität des Kartenterminal-Moduls. Es werden an dieser Stelle keine diesbezüglich spezifischen Fehlerfälle, die zu unterscheiden sind, definiert. Es liegt in der Verantwortung des Herstellers, solche Fehler für den Anwender angemessen darzustellen. Aus funktionaler Sicht scheint es zurzeit nicht erforderlich, unterschiedliche Kanäle in einem Steckzyklus einer Karte zu verwenden. Diese Spezifikation definiert, mit welchem Status TUC_MOKT_200 abhängig von dem von der Karte gemeldeten Status terminiert. Der aufrufende TUC muss bei manchen Kartenkommandos ggf. ein vom Status des TUCs und vom Status, den die Karte gemeldet hat, abhängiges Verhalten definieren. So kann zum Beispiel bei der PIN-Verifikation der Trailer 63 Cx nicht eindeutig der Ursache UpdateRetryWarning zugeordnet werden. Die Trailer sind bei eGK und HBA/SMC-B soweit identisch definiert, dass oben nur auf die Spezifikation der eGK verwiesen wird (siehe [HBA_P1#16.2]) und der Mini-AK bezüglich der Antworten der Karten nicht abhängig vom Kartentyp reagieren muss.
Offene Punkte	
Referenzen	Pic_MOKT_001 Aktivitätsdiagramm zu TUC_MOKT_200 sendAPDU

10.1.2 TUC_MOKT_202 readFile

TIP1-A_3769 - Mobiles KT: "TUC_MOKT_202 readFile"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_202 readFile" gemäß Tab_MOKT_101 umsetzen.
[<=]

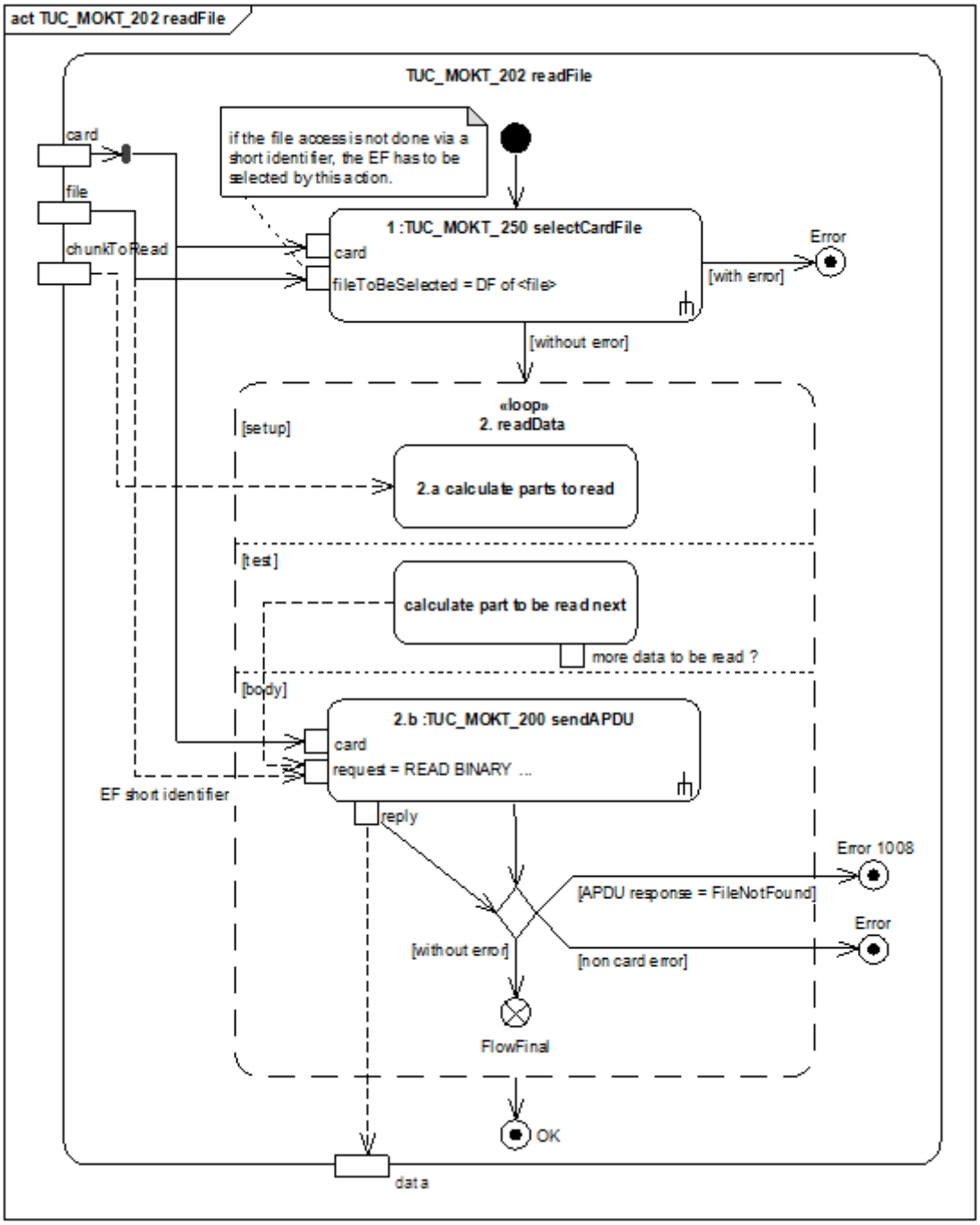


Abbildung 6: Pic_MOKT_002 Aktivitätsdiagramm zu TUC_MOKT_202 readFile

Tabelle 14: Tab_MOKT_101 - TUC_MOKT_202 readFile

TUC_MOKT_202 readFile	
Beschreibung	TUC_MOKT_202 liest Daten aus einem transparenten Elementary File (EF) einer Karte.
Anwendungsumfeld	Lesen von fachlichen Daten, Zertifikaten u. ä von Karten

Initiierender Akteur	MobKT
Weitere Akteure	Karte
Auslöser	Fachmodule TUC_MOKT_438 checkEGKAuthCertificate TUC_MOKT_470 encryptData
Vorbedingungen	keine
Nachbedingungen	keine
Eingangsdaten	• card: Karte, von der gelesen werden soll • file: Identifikation des EF, aus dem gelesen werden soll (siehe Anmerkungen) • chunkToRead: Teil der Datei, der gelesen werden soll
Ausgangsdaten	• data: die von der Karte gelesenen Daten
Weitere Informationsobjekte	keine
Standardablauf	1. Der Mini-AK MUSS gemäß TUC_MOKT_250 mit i. card = card ii. fileToBeSelected = DF, in dem der zu lesende EF liegt, das DF zum EF selektieren. 2. Endet TUC_MOKT_250 ohne Fehler, MUSS der Mini-AK in einer Schleife die Daten lesen. Dazu MUSS der Mini-AK i. abhängig von der von der Karte unterstützen extended length die zu lesenden Datenbereiche in geeignete Stücke zerlegen (hierbei SOLL der Mini-AK einen optimalen Datendurchsatz anstreben) ii. und die einzelnen Teile gemäß TUC_MOKT_200 mit A. card = card B. command = READ BINARY mit shortFileIdentifier entspricht dem EF aus den Eingangsparametern und offset und length entsprechen dem zu lesenden Teil lesen. Wenn TUC_MOKT_200 in der obigen Schleife jeweils ohne Fehler endet, MUSS der Mini-AK TUC_MOKT_202 mit OK beenden. Ergebnis der Operation sind hierbei die von der Karte gelesenen Daten.

Varianten/Alternativen	• Wenn auf die Datei nicht mit shortFileIdentifier zugegriffen wird, MUSS der Mini-AK in Schritt 1 nicht nur das DF sondern bereits das EF zur Selektion vorgeben und bei READ BINARY in Schritt 2.b.2 keinen shortFileIdentifier angeben.	
Fehlerfälle	• 1: Wenn TUC_MOKT_250 in Schritt 1 mit Fehler endet, MUSS der Mini-AK TUC_MOKT_202 mit diesem Fehler beenden. • 2.b: Wenn TUC_MOKT_200 in Schritt 2.b mit dem Kartenstatus FileNotFound endet, MUSS der Mini-AK TUC_MOKT_202 mit dem Fehler 1008 beenden. • 2.b: Wenn TUC_MOKT_200 in Schritt 2.b mit einem Fehler aber Kartenstatus nicht gleich FileNotFound endet, MUSS der Mini-AK TUC_MOKT_202 mit diesem Fehler beenden.	
Technische Fehlermeldungen	**Fehler Code**	**Bedeutung**
	1008	Kartenapplikation existiert nicht
	Siehe auch aufgerufene TUCs: TUC_MOKT_250 selectCardFile TUC_MOKT_200 sendAPDU	
Weitere Anforderungen	keine	
Anmerkungen, Bemerkungen	Eine Datei auf einer Karte wird letztlich durch das Dedicated File, in dem sich die Datei befindet, und einen fileIdentifier identifiziert. Optional kann auch ein shortFileIdentifier definiert sein. Es wird nicht im Detail spezifiziert, in welchen Fällen der Zugriff über einen shortFileIdentifier erfolgen oder nicht über einen shortFileIdentifier erfolgen soll. Der Hersteller soll diesbezüglich eine bezüglich der benötigten Laufzeit günstige Umsetzung wählen.	
Offene Punkte		
Referenzen	Pic_MOKT_002 Aktivitätsdiagramm zu TUC_MOKT_202 readFile	

10.1.3 TUC_MOKT_209 readRecord

TIP1-A_3770 - Mobiles KT: "TUC_MOKT_209 readRecord"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_209 readRecord" gemäß Tab_MOKT_102 umsetzen.
[<=]

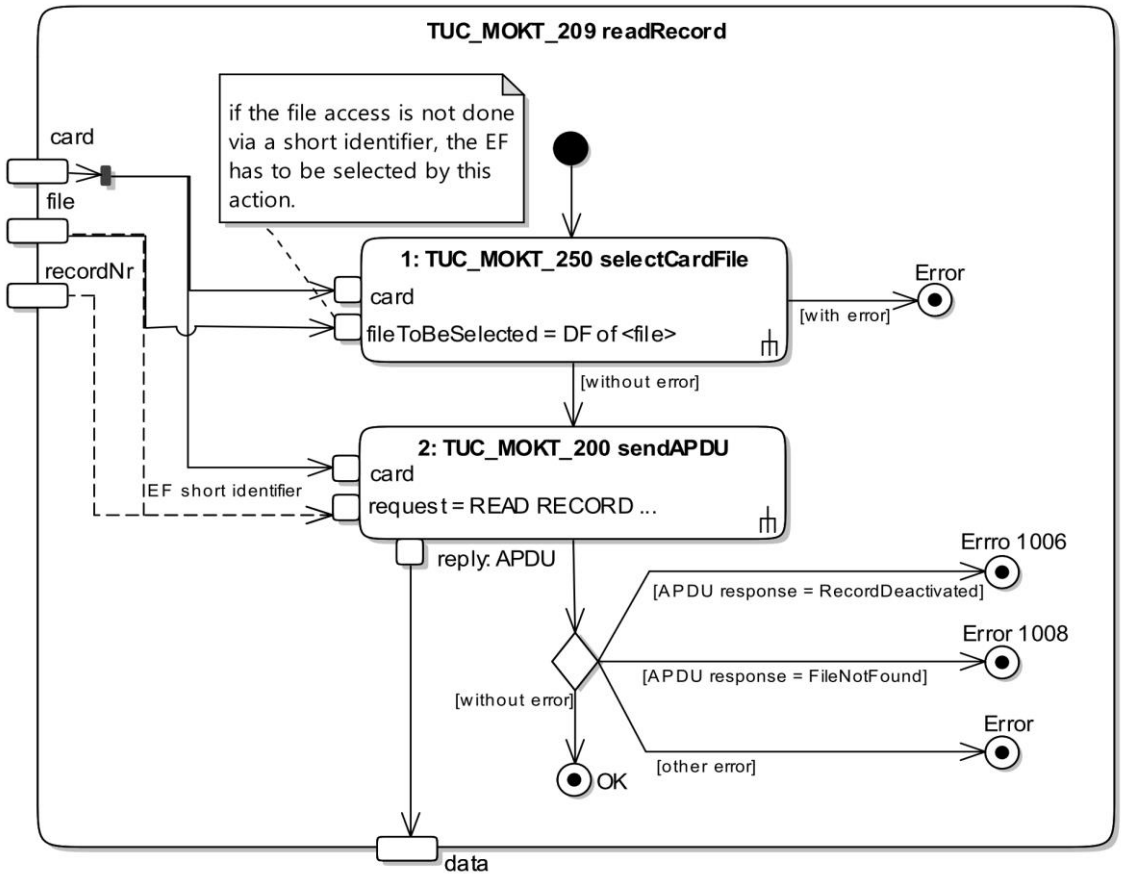


Abbildung 7: Pic_MOKT_003 Aktivitätsdiagramm zu TUC_MOKT_209 readRecord

Tabelle 15: Tab_MOKT_102 - TUC_MOKT_209 readRecord

TUC_MOKT_209 readRecord	
Beschreibung	TUC_MOKT_209 liest einen Record aus einem strukturierten Elementary File einer Karte
Anwendungsumfeld	Lesen von Record-basierten Daten
Initiierender Akteur	MobKT
Weitere Akteure	Karte (eGK, HBA oder SMC-B)
Auslöser	Fachmodule
Vorbedingungen	keine
Nachbedingungen	keine

Eingangsdaten	• card: Karte, von der gelesen werden soll • file: Identifikation des strukturieren Elementary Files • recordNr: Nummer des Records
Ausgangsdaten	Daten des gelesenen Records
Weitere Informationsobjekte	keine
Standardablauf	1. Der Mini-AK MUSS den DF, in dem der strukturierte Elementary File liegt, gemäß TUC_MOKT_250 mit a. card = card b. file = der Dedicated File, in dem der strukturierte File file liegt, selektieren 2. Wenn der obige Schritt ohne Fehler endet, MUSS der Mini-AK den Record gemäß TUC_MOKT_200 mit a. card = card b. command = Kommando READ RECORD mit shortFileIdentifier entsprechend file und recordNumber gleich recordNr; die (maximale) length ergibt sich aus der Spezifikation des strukturierten Elementary Files; lesen. Wenn TUC_MOKT_200 ohne Fehler endet, MUSS der Mini-AK TUC_MOKT_209 mit OK beenden.
Varianten/Alternativen	• Wenn auf den strukturierten Elementary File nicht über ein shortFileIdentifier zugegriffen wird, MUSS der Mini-AK bereits in Schritt 1 den strukturierten Elementary File selektieren und in Schritt 2 bei READ RECORD keinen shortFileIdentifier angeben.
Fehlerfälle	• 1: Wenn TUC_MOKT_250 in Schritt 1 mit einem Fehler endet, MUSS der Mini-AK TUC_MOKT_209 mit diesem Fehler beenden. • 2: Wenn TUC_MOKT_200 in Schritt 2 mit dem Kartenstatus RecoredDeactivated endet, MUSS der Mini-AK TUC_MOKT_209 mit dem Fehler 1006 beenden. • 2: Wenn TUC_MOKT_200 in Schritt 2 mit dem Kartenstatus FileNotFound endet, MUSS der Mini-AK TUC_MOKT_209 mit dem Fehler 1008 beenden. • 2: Wenn TUC_MOKT_200 in Schritt 2 mit einem anderen Fehler als Kartenstatus FileNotFound endet, MUSS der Mini-AK TUC_MOKT_209 mit diesem anderen Fehler beenden.
	Fehler Code | **Bedeutung**

Technische Fehlermeldungen	1006	Kartenapplikation ist deaktiviert
	1008	Kartenapplikation existiert nicht
	Siehe auch aufgerufene TUCs: TUC_MOKT_250 selectCardFile TUC_MOKT_200 sendAPDU	
Weitere Anforderungen	keine	
Anmerkungen, Bemerkungen	keine	
Offene Punkte		
Referenzen	Pic_MOKT_003 Aktivitätsdiagramm zu TUC_MOKT_209 readRecord	

10.1.4 TUC_MOKT_214 appendRecord

TIP1-A_3771 - Mobiles KT: "TUC_MOKT_214 appendRecord"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_214 appendRecord" gemäß Tab_MOKT_103 umsetzen.
[<=]

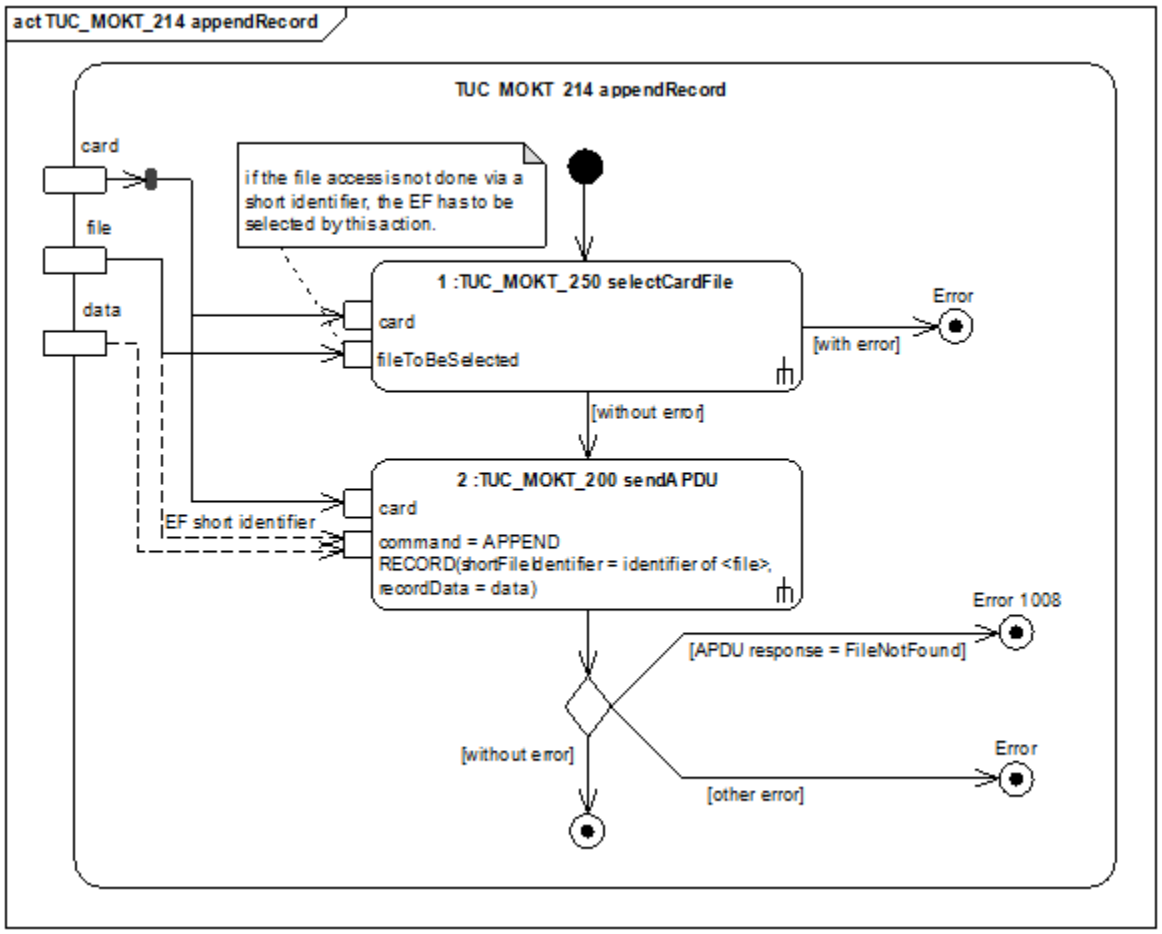


Abbildung 8: Pic_MOKT_004 Aktivitätsdiagramm zu TUC_MOKT_214 appendRecord

Tabelle 16: Tab_MOKT_103 - TUC_MOKT_214 appendRecord

TUC_MOKT_214 appendRecord	
Beschreibung	TUC_MOKT_214 fügt einen Record einem strukturierten Elementary File einer Karte hinzu
Anwendungsumfeld	Schreiben der Audit-Daten
Initiierender Akteur	MobKT
Weitere Akteure	Karte
Auslöser	TUC_MOKT_406 writeEGKAudit
Vorbedingungen	keine
Nachbedingungen	keine

Eingangsdaten	• card: Karte auf die geschrieben werden soll • file: Identifikation des strukturierten Elementary Files • data: Daten, die in den Record geschrieben werden sollen
Ausgangsdaten	keine
Weitere Informationsobjekte	keine
Standardablauf	1. Der Mini-AK MUSS den Dedicated File, in dem der strukturierte Elementary File liegt, gemäß TUC_MOKT_250 mit a. card = card b. fileToBeSelected = Dedicated File, in dem file liegt, selektieren. 2. Wenn der obige Schritt ohne Fehler endet, MUSS der Mini-AK den Record gemäß TUC_MOKT_200 mit a. card = card b. command = APPEND RECORD mit shortFileIdentifier entsprechend dem strukturierten Elementary File und recordData = data, schreiben. Wenn TUC_MOKT_200 ohne Fehler endet, MUSS der Mini-AK TUC_MOKT_214 mit OK beenden.
Varianten/Alternativen	• Wenn auf den strukturierten Elementary File nicht über ein shortFileIdentifier zugegriffen wird, MUSS der Mini-AK in Schritt 1 bereits den strukturierten Elementary File selektieren und in Schritt 2 bei APPEND BINARY keinen shortFileIdentifier angeben.
Fehlerfälle	• 1: Wenn TUC_MOKT_250 in Schritt 1 mit einem Fehler endet, MUSS der Mini-AK TUC_MOKT_214 mit diesem Fehler beenden. • 2: Wenn TUC_MOKT_200 in Schritt 2 mit dem Kartenstatus FileNotFound endet, MUSS der Mini-AK TUC_MOKT_214 mit dem Fehler 1008 beenden. • 2: Wenn TUC_MOKT_200 in Schritt 2 mit einem Fehler aber nicht Kartenstatus FileNotFound endet, MUSS der Mini-AK TUC_MOKT_214 mit diesem Fehler beenden.
Technische Fehlermeldungen	**Fehler Code** / **Bedeutung** 1008 / Kartenapplikation existiert nicht Siehe auch aufgerufene TUCs:

	TUC_MOKT_250 selectCardFile TUC_MOKT_200 sendAPDU
Weitere Anforderungen	keine
Anmerkungen, Bemerkungen	keine
Offene Punkte	-
Referenzen	Pic_MOKT_004 Aktivitätsdiagramm zu TUC_MOKT_214 appendRecord

10.1.5 TUC_MOKT_220 fulfillAccessConditions

TIP1-A_3772 - Mobiles KT: "TUC_MOKT_220 fulfillAccessConditions"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_220 fulfillAccessConditions" gemäß Tab_MOKT_104 umsetzen.
[<=]

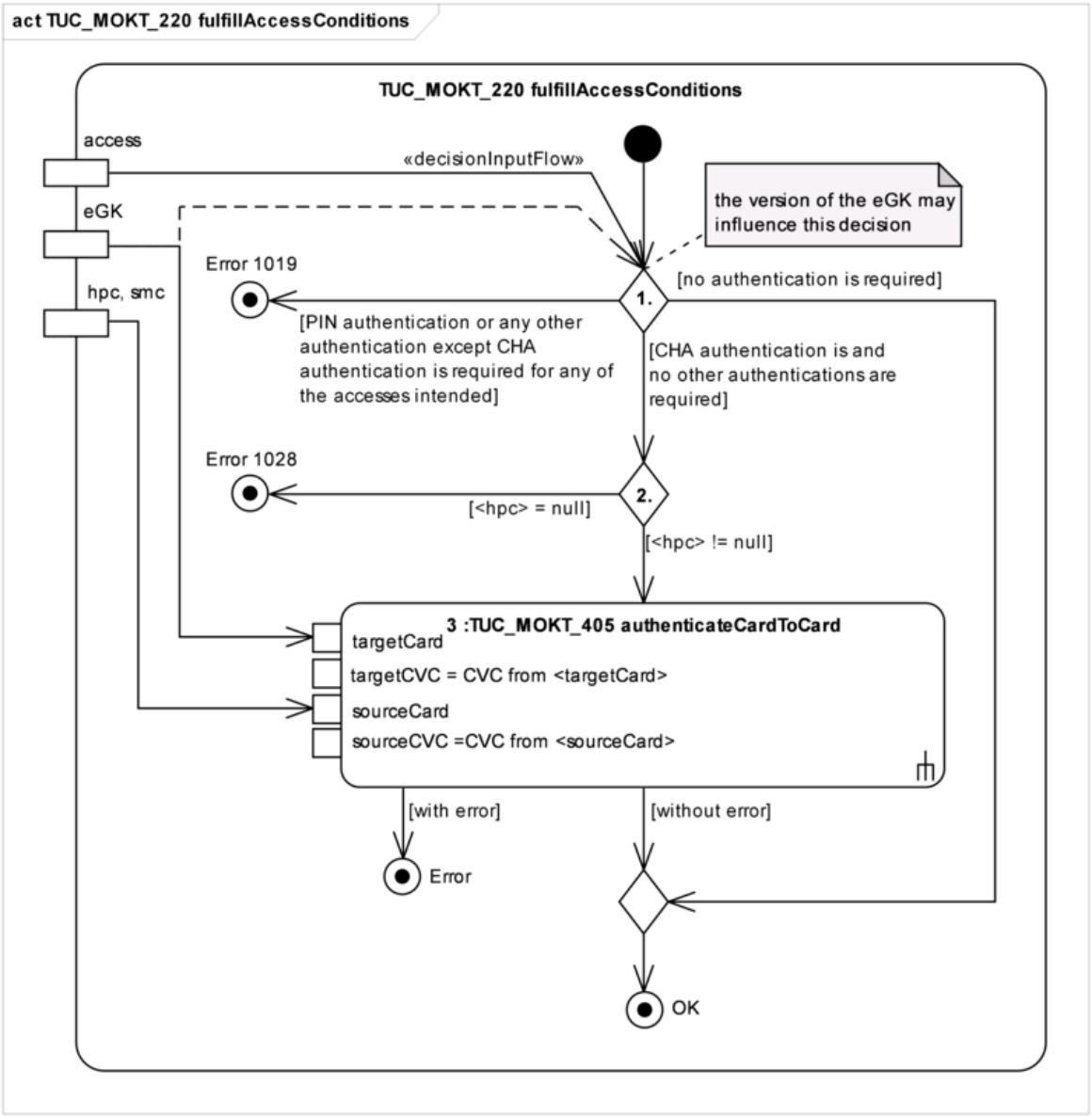


Abbildung 9: Pic_MOKT_005 Aktivitätsdiagramm zu TUC_MOKT_220 fulfillAccessConditions

Tabelle 17: Tab_MOKT_104 - TUC_MOKT_220 fulfillAccessConditions

TUC_MOKT_220 fulfillAccessConditions (alias TUC_MOKT_220 accessConditions)	
Beschreibung	TUC_MOKT_220 führt die notwendigen Authentisierungen gegenüber der eGK durch, welche für die vorgesehenen Zugriffe erforderlich sind. Zurzeit ist die einzige vorgesehene Authentisierung eine Card-to-Card-Authentisierung mit einer Leistungserbringerkarte.
Anwendungsumfeld	Zugriff auf geschützte Daten der eGK durch Leistungserbringer in mobilen Szenarien

Initiierender Akteur	MobKT
Weitere Akteure	eGK, HBA/SMC-B
Auslöser	Fachmodule TUC_MOKT_417 readFromEGK
Vorbedingungen	• eGK ist eine Karte vom Typ eGK mit einer vom Mini-AK unterstützten Version. • hpc, falls angegeben, ist eine Karte vom Typ HBA oder SMC-B mit einer vom Mini-AK unterstützten Version.
Nachbedingungen	keine
Eingangsdaten	• egk: eGK, auf die zugegriffen werden soll • hpc: HBA oder SMC-B mit der auf die eGK zugegriffen werden soll • access: Liste der beabsichtigen Zugriffe, d. h. jeweils das Objekt der eGK, auf das zugegriffen wird, und die Art des Zugriffes. Zurzeit sind in diesem Rahmen nur Zugriffe auf Dateien (EF und die DF, in denen sie liegen, zu berücksichtigen)
Ausgangsdaten	keine
Weitere Informationsobjekte	eGK, HPC (HBA und SMC-B)

<table>
<tr><td>Standardablauf</td><td colspan="2">1. Der Mini-AK MUSS prüfen, ob alle geplanten Zugriffe auf die eGK ohne eine Authentisierung durchgeführt werden können. Diese Entscheidung ist anhand der Spezifikation der eGK zu treffen. Versionsabhängigkeiten sind zu berücksichtigen.
Wenn obige Bedingung erfüllt ist, MUSS der Mini-AK TUC_MOKT_220 ohne weitere Aktionen mit OK terminieren.
Ansonsten MUSS der Mini-AK prüfen, ob alle geplanten Zugriffe jeweils ohne Authentisierung oder nach einer Rollenauthentisierung von der eGK gewährt werden. Die konkreten Rollen der Zugriffsbedingungen oder der HPC werden hierbei nicht berücksichtigt.
Falls dies nicht der Fall ist, MUSS der Mini-AK TUC_MOKT_220 ohne weitere Aktionen mit dem Fehler 1019 beenden.
2. Falls die Bedingung zuvor hingegen erfüllt ist, MUSS der Mini-AK prüfen, ob ein hpc angegeben wurde.
Falls kein hpc angegeben wurde, MUSS der Mini-AK den TUC_MOKT_220 mit dem Fehler 1028 beenden.
3. Falls ein hpc angegeben wurde, MUSS der Mini-AK gemäß TUC_MOKT_405,
a. bei einer eGK Generation 2 und 2.1 mit
• targetCard = egk,
• targetCVC = /MF/EF.C.eGK.AUT_CVC.E256,
• sourceCard = hpc,
• sourceCVC = /MF/EF.C.HPC.AUTR_CVC.E256 bzw. /MF/EF.C.SMC.AUTR_CVC.E256,
eine C2C-Authentisierung zwischen hpc und egk durchführen.
Endet TUC_MOKT_405 ohne Fehler, MUSS der Mini-AK TUC_MOKT_220 mit OK beenden.</td></tr>
<tr><td>Varianten/Alternativen</td><td colspan="2"></td></tr>
<tr><td>Fehlerfälle</td><td colspan="2">Wenn TUC_MOKT_405 in Schritt 3 mit einem Fehler endet, MUSS der Mini-AK TUC_MOKT_220 mit diesem Fehler beenden</td></tr>
<tr><td rowspan="4">Technische Fehlermeldungen</td><td>Fehler Code</td><td>Bedeutung</td></tr>
<tr><td>1019</td><td>Kartenzugriff verweigert</td></tr>
<tr><td>1028</td><td>Quellkarte für Card-to-Card fehlt</td></tr>
<tr><td colspan="2">Siehe auch aufgerufene TUCs:
TUC_MOKT_405 authenticateCardToCard</td></tr>
<tr><td>Weitere Anforderungen</td><td colspan="2">keine</td></tr>
</table>

Anmerkungen, Bemerkungen	Das MobKT prüft nicht die spezifischen Rollen der berechtigten Karten. Wenn die Karte eines Leistungserbringers aufgrund der Rolle nicht genügend Berechtigungen gegenüber der eGK besitzt, so wird zwar ein C2C durchgeführt, der Zugriff wird aber letztlich mit einer Zugriffsverweigerung der eGK abbrechen. Dieses Verhalten des MobKT stellt somit keine Einbuße an Sicherheit dar. Eine gegebenenfalls vorliegende Einschränkung der Ergonomie, da der Leistungserbringer seine PIN Eingeben muss, aber dennoch den Zugriff nicht erfolgreich durchführen kann, wird in Kauf genommen. Das MobKT ist für den Einsatz mit entsprechend berechtigten Heilberufsausweisen vorgesehen. Zurzeit gibt es in diesem Punkt keine Abhängigkeit von der individuellen eGK, da diese alle die gleichen rollenbasierten Zugriffsbedingungen haben.
Offene Punkte	
Referenzen	Pic_MOKT_005 Aktivitätsdiagramm zu TUC_MOKT_220 fulfillAccessConditions

10.1.6 TUC_MOKT_250 selectCardFile

TIP1-A_3773 - Mobiles KT: "TUC_MOKT_250 selectCardFile"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_250 selectCardFile" gemäß Tab_MOKT_105 umsetzen.
[<=]

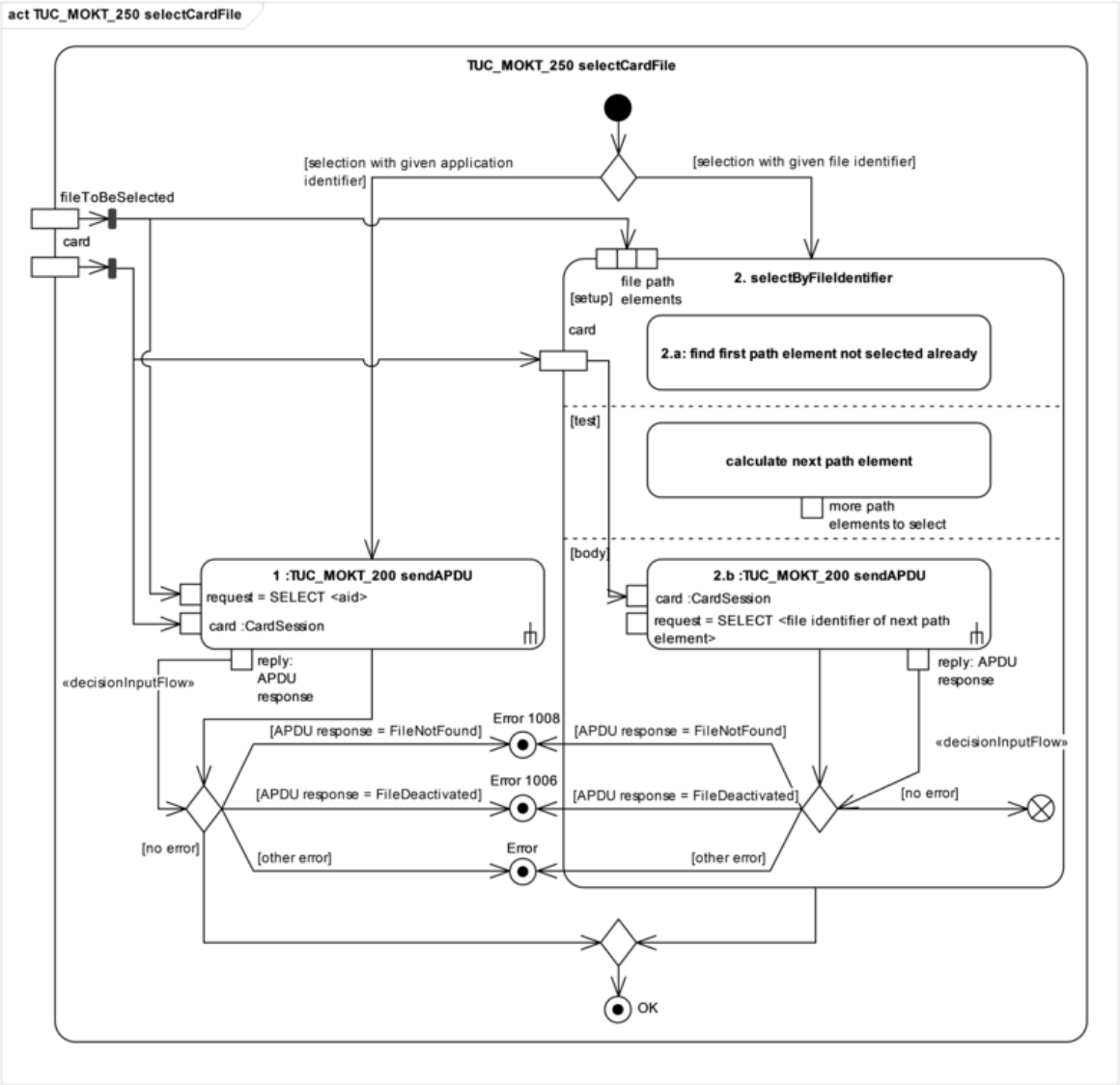


Abbildung 10: Pic_MOKT_006 Aktivitätsdiagramm zu TUC_MOKT_250 selectCardFile

Tabelle 18: Tab_MOKT_105 - TUC_MOKT_250 selectCardFile

TUC_MOKT_250 selectCardFile	
Beschreibung	TUC_MOKT_250 selektiert ein DF oder EF auf einer Chipkarte
Anwendungsumfeld	Selektion eines DF oder EF zwecks folgender Zugriffe auf Daten in dem Dedicated File bzw. Elementary Files
Initiierender Akteur	MobKT
Weitere Akteure	Karte

Auslöser	TUC_MOKT_202 readFile TUC_MOKT_209 readRecord TUC_MOKT_214 appendRecord TUC_MOKT_471 decryptData
Vorbedingungen	keine
Nachbedingungen	keine
Eingangsdaten	• card: Karte auf der DF bzw. EF selektiert werden sollen. • fileToBeSelected: Identifikation des DF bzw. EF, der selektiert werden soll.
Ausgangsdaten	keine
Weitere Informationsobjekte	keine
Standardablauf	1. soll die Selektion über einen Application Identifier erfolgen, MUSS der Mini-AK die Anwendung gemäß TUC_MOKT_200 mit a. card = card b. command = SELECT mit aid = <fileToBeSelected> selektieren. Endet TUC_MOKT_200 ohne Fehler, MUSS der Mini-AK TUC_MOKT_250 mit OK beenden. 2. soll die Selektion über File Identifier erfolgen, MUSS der Mini-AK a. einen Selektionspfad vom zuletzt selektierten DF zum neu zu selektierenden File bestimmen b. und in einer Schleife über die Pfadelemente gemäß TUC_MOKT_200 mit i. card = card ii. command = SELECT mit fid = Pfadelement die entsprechenden Files (DF bzw. EF) selektieren. Enden alle TUC_MOKT_200 ohne Fehler, MUSS der Mini-AK TUC_MOKT_250 mit OK beenden.
Varianten/Alternativen	• Der Ablauf nach Schritt 1 und Schritt 2 KANN auch kombiniert sein, d. h., dass der Pfad zu einem DF über den Application Identifier und in dem DF ein EF über File Identifier selektiert werden kann.

Fehlerfälle	• 1: Endet TUC_MOKT_200 in Schritt 1 mit Kartenstatus FileNotFound, MUSS der Mini-AK TUC_MOKT_250 mit Fehler 1008 beenden. • 1: Endet TUC_MOKT_200 in Schritt 1 mit Kartenstatus FileDeactivated, MUSS der Mini-AK TUC_MOKT_250 mit Fehler 1006 beenden. • 1: Endet TUC_MOKT_200 in Schritt 1 mit einem anderen Fehler, MUSS der Mini-AK TUC_MOKT_250 mit diesem Fehler beenden. • 2.b: Endet TUC_MOKT_200 in Schritt 2.b mit Kartenstatus FileNotFound, MUSS der Mini-AK TUC_MOKT_250 mit Fehler 1008 beenden. • 2.b: Endet TUC_MOKT_200 in Schritt 2.b mit Kartenstatus FileDeactivated, MUSS der Mini-AK TUC_MOKT_250 mit Fehler 1006 beenden. • 2.b: Endet TUC_MOKT_200 in Schritt 2.b mit einem anderen Fehler, MUSS der Mini-AK TUC_MOKT_250 mit diesem Fehler beenden.	
Technische Fehlermeldungen	**Fehler Code**	**Bedeutung**
	1006	Objekt ist deaktiviert
	1008	Objekt existiert nicht
	Siehe auch aufgerufene TUCs: TUC_MOKT_200	
Weitere Anforderungen	keine	
Anmerkungen, Bemerkungen	keine	
Offene Punkte		
Referenzen	Pic_MOKT_006 Aktivitätsdiagramm zu TUC_MOKT_250 selectCardFile	

10.1.7 TUC_MOKT_405 authenticateCardToCard

TIP1-A_3774 - Mobiles KT: "TUC_MOKT_405 authenticateCardToCard"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_405 authenticateCardToCard" gemäß Tab_MOKT_107 umsetzen.
[<=]

TUC_MOKT_405 verwendet zur besseren Lesbarkeit die in Tabelle Tab_MOKT_120 beschriebene Generalisierung von Artefakten der beteiligten Karten in Zusammenhang mit verschiedenen eGK-Kartengenerationen.

Tabelle 19: Tab_MOKT_120 - Generalisierte Bezeichnung von Artefakten bei CardToCard-Authentication

Bezeichner generalisiert	G1/G1+	G2
asymRoleCheck	rsaRoleCheck	elcRoleCheck
asymRoleAuthentication	rsaRoleAuthentication	elcRoleAuthentications
EF.C.eGK.AUT_CVC	EF.C.eGK.AUT_CVC	EF.C.eGK.AUT_CVC.E256
EF.C.CA_eGK.CS	EF.C.CA_eGK.CS	EF.C.CA_eGK.CS.E256
PrK.eGK.AUT_CVC	PrK.eGK.AUT_CVC	PrK.eGK.AUT_CVC.E256
EF.C.CA_HPC.CS	EF.C.CA_HPC.CS.R2048	EF.C.CA_HPC.CS.E256
EF.C.CA_SMC.CS	EF.C.CA_SMC.CS.R2048	EF.C.CA_SMC.CS.E256
PrK.HPC.AUTR_CVC	PrK.HPC.AUTR_CVC.R2048	PrK.HPC.AUTR_CVC.E256
PrK.SMC.AUTR_CVC	PrK.SMC.AUTR_CVC.R2048	PrK.SMC.AUTR_CVC.E256

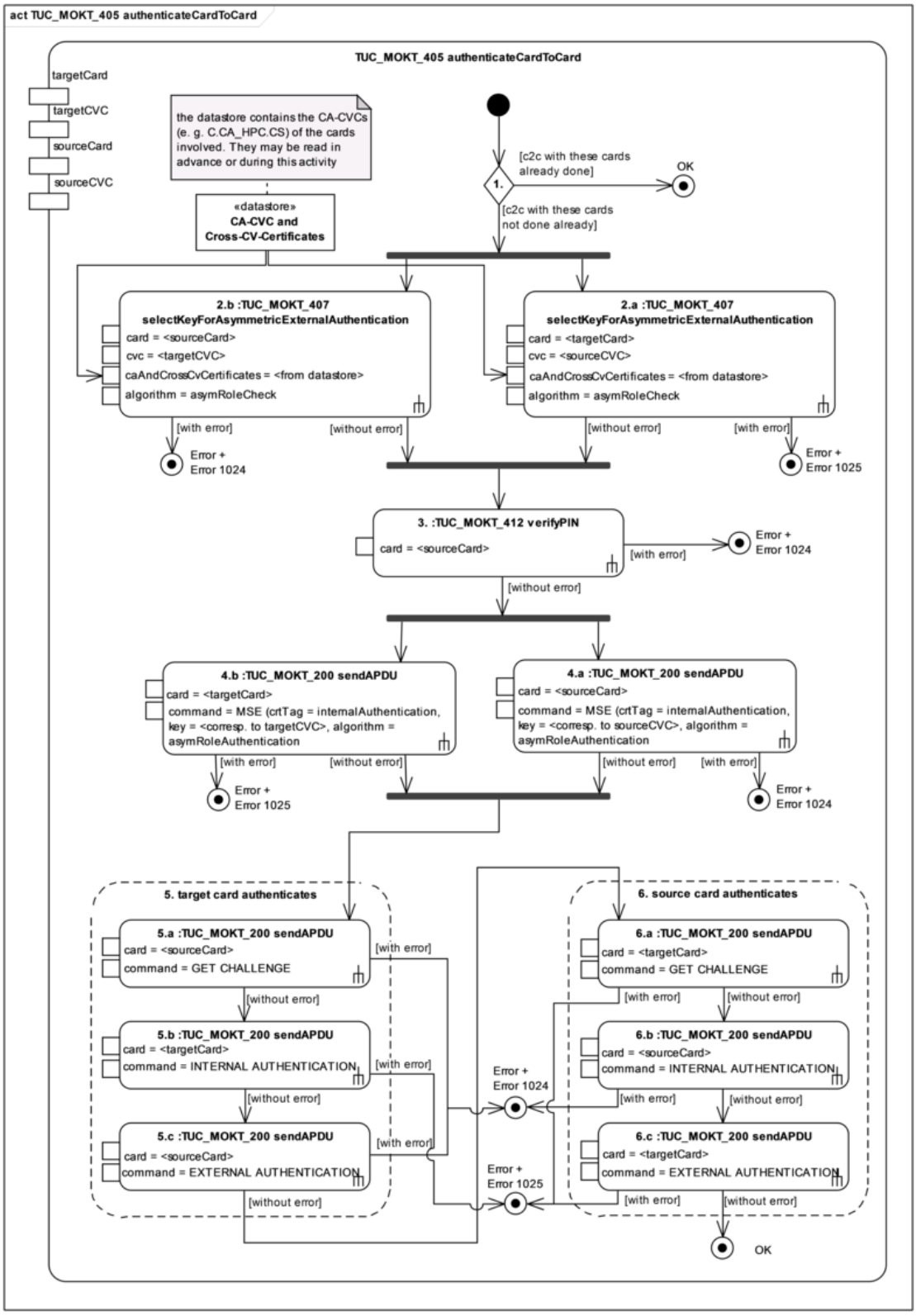


Abbildung 11: Pic_MOKT_008 Aktivitätsdiagramm zu TUC_MOKT_405 authenticateCardToCard

Tabelle 20: Tab_MOKT_107 - TUC_MOKT_405 authenticateCardToCard

TUC_MOKT_405 authenticateCardToCard (alias TUC_MOKT_405 authenticateC2C)	
Beschreibung	TUC_MOKT_405 führt eine asymmetrische Card-to-Card Authentisierung zwischen einer Leistungserbringerkarte (HPC) und einer Gesundheitskarte (eGK) durch. Es wird keine Aushandlung von Sitzungsschlüssel veranlasst.
Anwendungsumfeld	Freischaltung der eGK im Rahmen fachlicher Zugriffe
Initiierender Akteur	MobKT
Weitere Akteure	eGK, HPC (HBA oder SMC-B)
Auslöser	TUC_MOKT_220 fulfillAccessConditions
Vorbedingungen	• targetCard ist eine Karte vom Typ eGK. • sourceCard ist eine Karte vom Typ HBA oder vom Typ SMC-B. • sourceCard Zertifikat ist nicht abgelaufen (siehe Kapitel 5.2.4) • targetCard und sourceCard haben vom Mini-AK unterstützte Versionen. • targetCVC[4] entspricht /MF/EF.C.eGK.AUT_CVC. • sourceCVC[4] entspricht /MF/EF.C.HPC.AUTR_CVC bzw. /MF/EF.C.SMC.AUTR_CVC.
Nachbedingungen	• Eine beidseitige Card-to-Card-Authentisierung zwischen sourceCard und targetCard ist durchgeführt worden.
Eingangsdaten	• targetCard: Zielkarte • targetCVC: Festlegung des CV-Zertifikats der Zielkarte • sourceCard: Quellkarte • sourceCVC: Festlegung des CV-Zertifikats der Quellkarte
Ausgangsdaten	Keine
Weitere Informationsobjekte	

Standardablauf	1. wenn eine Card-to-Card Authentisierung mit denselben Parametern bereits einmal erfolgreich durchgeführt wurde, ohne dass seitdem der Sicherheitsstatus der Zielkarte vom MobKT zurückgesetzt wurde, dann MUSS der Mini-AK den TUC_MOKT_405 sofort mit OK beenden. 2. Anderenfalls MUSS der Mini-AK gemäß TUC_MOKT_407 die öffentlichen Schlüssel für die asymmetrische externe Authentisierung ohne SM selektieren, und zwar a. in der Zielkarte mit i. card = targetCard, ii. cvc = sourceCVC, iii. zu CV-CA- und Cross-CV-Zertifikaten siehe unten iv. algorithm = asymRoleCheck b. und in der Quellkarte mit i. card = sourceCard, ii. cvc = targetCVC, iii. zu CV-CA- und Cross-CV-Zertifikaten siehe unten iv. algorithm = asymRoleCheck Die notwendigen CA-CV-Zertifikate (/MF/EF.C.CA_eGK.CS, /MF/EF.C.CA_HPC.CS, bzw. MF/EF.C.CA_SMC.CS) KANN der Mini-AK den beteiligten Karten entnehmen. Eventuell notwendige Cross-CV-Zertifikate MUSS der Mini-AK selbst bereitstellen. 3. Wenn der vorherige Schritt ohne Fehler beendet ist, MUSS der Mini-AK eine PIN-Eingabe für die PIN.CH bzw. PIN.SMC der Quellkarte gemäß TUC_MOKT_412 mit a. card = sourceCard durchführen. 4. Wenn der vorherige Schritt ohne Fehler beendet ist, MUSS der Mini-AK gemäß TUC_MOKT_200 die Schlüssel und Algorithmen für die interne Authentisierung selektieren, und zwar: a. für die Quellkarte mit i. card = sourceCard, ii. command = MANAGE SECURITY ENVIRONMENT mit crtTag = internalAuthenticate, dem Schlüssel(Es sind die zum CV-Zertifikat korrespondierenden Schlüssel zu selektieren. Zurzeit werden im MobKT nur diese Zertifikate/Schlüssel verwendet, sodass man die Schlüssel an dieser Stelle fest vorgeben kann.) /MF/PrK.HPC.AUTR_CVC bzw. MF/PrK.SMC.AUTR_CVC und dem Algorithmus asymRoleAuthentication,

	b. und für die Zielkarte mit i. card = targetCard, ii. command = MANAGE SECURITY ENVIRONMENT mit crtTag = internalAuthenticate, dem Schlüssel /MF/PrK.eGK.AUT_CVC und dem Algorithmus asymRoleAuthentication. 5. Wenn der vorherige Schritt ohne Fehler beendet ist, MUSS der Mini-AK die Authentisierung der Zielkarte gegenüber der Quellkarte durchführen. Dazu MUSS der Mini-AK in der dargestellten Reihenfolge a. von der Quellkarte eine Challenge anfordern gemäß TUC_MOKT_200 mit i. card = sourceCard, ii. command = GET CHALLENGE, b. die Challenge von der Zielkarte signieren lassen gemäß TUC_MOKT_200 mit i. card = targetCard, ii. command = INTERNAL AUTHENTICATION, c. und diese Signatur von der Quellkarte prüfen lassen gemäß TUC_MOKT_200 mit i. card = sourceCard, ii. command = EXTERNAL AUTHENTICATION. 6. Wenn der vorherige Schritt ohne Fehler beendet ist, MUSS der Mini-AK die Authentisierung der Quellkarte gegenüber der Zielkarte durchführen. Dazu MUSS der Mini-AK in der dargestellten Reihenfolge a. von der Zielkarte eine Challenge anfordern gemäß TUC_MOKT_200 mit i. card = targetCard, ii. command = GET CHALLENGE, b. von der Quellkarte die Challenge signieren lassen gemäß TUC_MOKT_200 mit i. card = sourceCard, ii. command = INTERNAL AUTHENTICATION, c. und diese Signatur von der Zielkarte prüfen lassen gemäß TUC_MOKT_200 mit i. card = targetCard ii. command = EXTERNAL AUTHENTICATION. 7. Wenn der vorherige Schritt ohne Fehler beendet ist, MUSS der Mini-AK den TUC_MOKT_405 mit OK beenden.

<table>
<tr><td>Varianten/Alternativen</td><td colspan="2">keine</td></tr>
<tr><td>Fehlerfälle</td><td colspan="2">

2.a: endet TUC_MOKT_407 in 2.a mit einem Fehler, so MUSS der Mini-AK TUC_MOKT_405 sofort mit diesem Fehler und Fehler 1025 beenden.
2.b: endet TUC_MOKT_407 in 2.b mit einem Fehler, so MUSS der Mini-AK TUC_MOKT_405 sofort mit diesem Fehler und Fehler 1024 beenden.
3: endet TUC_MOKT_412 in 3 mit einem Fehler, so MUSS der Mini-AK TUC_MOKT_405 sofort mit diesem Fehler und 1024 beenden.
2.b: endet TUC_MOKT_200 in 4.a mit einem Fehler, so MUSS der Mini-AK TUC_MOKT_405 sofort mit diesem Fehler und Fehler 1024 beenden.
2.b: endet TUC_MOKT_200 in 2.b mit einem Fehler, so MUSS der Mini-AK TUC_MOKT_405 sofort mit diesem Fehler und Fehler 1025 beenden.
5.a, 5.c, 6.b: endet TUC_MOKT_200 in 5.a, 5.c oder 6.b mit einem Fehler, so MUSS der Mini-AK TUC_MOKT_405 jeweils sofort mit diesem Fehler und Fehler 1024 beenden.
5.b, 6.a, 6.c: endet TUC_MOKT_200 in 5.b, 6.a oder 6.c mit einem Fehler, so MUSS der Mini-AK TUC_MOKT_405 jeweils sofort mit diesem Fehler und Fehler 1025 beenden.

Das MobKT MUSS es bei der Darstellung obiger Fehler neben der Angabe der eigentlichen Fehlerursache ermöglichen zu unterscheiden, bezüglich welcher der beiden beteiligten Karten der Fehler aufgetreten ist, d. h. ob der Fehler beim Zugriff auf die Quellkarte (Error 1024) oder die Zielkarte (Error 1025) erfolgte.
</td></tr>
<tr><td rowspan="4">Technische Fehlermeldungen</td><td>Fehler Code</td><td>Bedeutung</td></tr>
<tr><td>1024</td><td>Fehler bei der C2C-Authentisierung, Quellkarte</td></tr>
<tr><td>1025</td><td>Fehler bei der C2C-Authentisierung, Zielkarte</td></tr>
<tr><td colspan="2">Siehe auch aufgerufene TUCs:
TUC_MOKT_407 selectKeyForAsymmetricExternalAuthentication
TUC_MOKT_412 verifyPIN
TUC_MOKT_200 sendAPDU</td></tr>
<tr><td>Weitere Anforderungen</td><td colspan="2">keine</td></tr>
<tr><td>Anmerkungen, Bemerkungen</td><td colspan="2">keine</td></tr>
</table>

Offene Punkte	
Referenzen	Pic_MOKT_008 Aktivitätsdiagramm zu TUC_MOKT_405 authenticateCardToCard

10.1.8 TUC_MOKT_406 writeEGKAudit

TIP1-A_3775 - Mobiles KT: "TUC_MOKT_406 writeEGKAudit"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_406 writeEGKAudit" gemäß Tab_MOKT_108 umsetzen.
[<=]

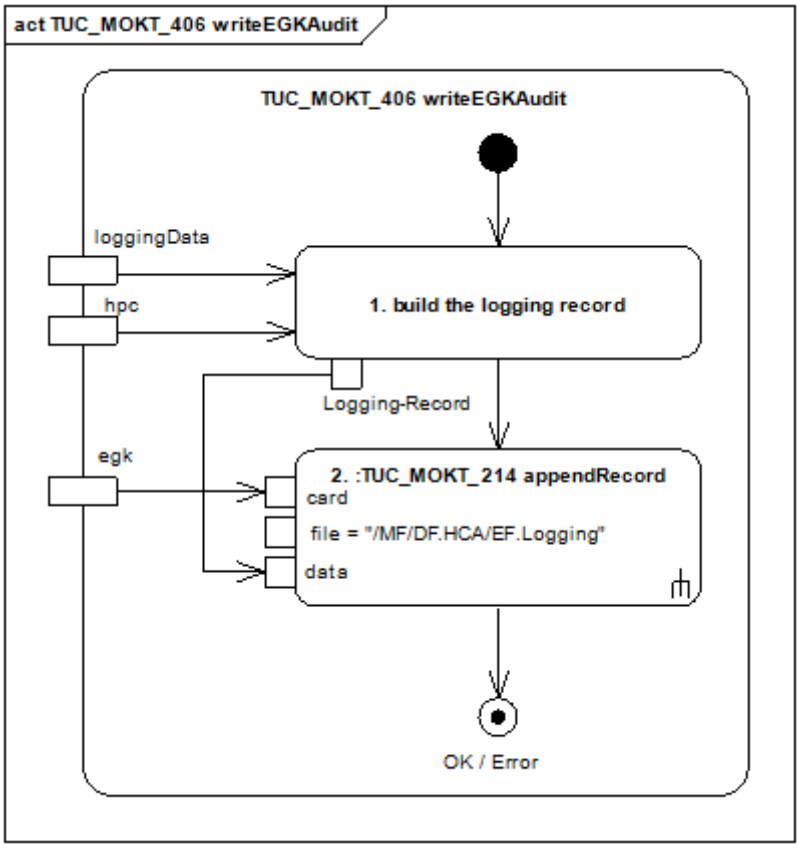


Abbildung 12: Pic_MOKT_009 Aktivitätsdiagramm zu TUC_MOKT_406 writeEGKAudit

Tabelle 21: Tab_MOKT_108 - TUC_MOKT_406 writeEGKAudit

TUC_MOKT_406 writeEGKAudit	
Beschreibung	TUC_MOKT_406 schreibt einen Audit-Eintrag in EF.Logging der eGK
Anwendungsumfeld	Zugriffe auf geschützte Daten der eGK müssen auf der eGK auditiert werden.

Initiierender Akteur	MobKT
Weitere Akteure	eGK, HPC (HBA oder SMC-B)
Auslöser	Fachmodule
Vorbedingungen	• hpc ist eine Karte vom Typ HBA oder SMC-B. • Das AUT- bzw. OSIG-Zertifikat der zugreifenden Karte ist verfügbar und korrekt, d. h. es ist syntaktisch korrekt und enthält einen Subject-DN. • eGK ist eine Karte vom Typ eGK. • eGK und hpc haben vom Mini-AK unterstützte Versionen. • die ICCSN der zugreifenden Karte (hpc) ist verfügbar.
Nachbedingungen	Der Audit-Eintrag wurde mit Selektion von EF.Logging und dem Kommando APPEND RECORD an die eGK übertragen.

Eingangsdaten	• loggingData: die Logging-Daten soweit sie nicht von der zugreifenden Karte oder dem System bezogen werden, d. h.:
	  • Data Type
	  • und Type of Access.
	• hpc: die zugreifende Karte
	• eGK: als Karte auf die der Protokolldatensatz geschrieben werden soll

Ausgangsdaten	keine
Weitere Informationsobjekte	Audit-Eintrag

Standardablauf	1. Der Mini-AK MUSS einen Protokolldatensatz in der Struktur der Datei EF.Logging gemäß [gemSpec_eGK_Fach_TIP#TIP1-A_5144] mit folgenden Daten zusammenstellen:
	  a. Timestamp: die aktuelle Systemzeit des MobKT
	  b. Data Type: entsprechend der Eingangsdaten
	  c. Type of Access: entsprechend der Eingangsdaten
	  d. Actor-ID: ICCSN der zugreifenden Karte
	  e. Actor-Name: entsprechend dem Zertifikat der zugreifenden Karte
	2. Der Mini-AK MUSS den Protokolldatensatz schreiben gemäß TUC_MOKT_214 mit
	  a. card = eGK,
	  b. file = /MF/DF.HCA/EF.Logging (siehe [eGK])

	c. data = Protokolldatensatz aus dem Schritt oben. Der Mini-AK MUSS TUC_MOKT_406 mit dem Fehlerstatus von TUC_MOKT_214 beenden.
Varianten/Alternativen	Keine
Fehlerfälle	
Technische Fehlermeldungen	Siehe aufgerufene TUCs: TUC_MOKT_214 appendRecord
Weitere Anforderungen	keine
Anmerkungen, Bemerkungen	TUC_MOKT_406 veranlasst kein C2C, um auf die Auditdaten der eGK schreiben zu können. D. h., dies muss bereits vorher erfolgt sein. Wenn nicht, wird TUC_MOKT_406 mit einer entsprechenden Zugriffsverweigerung der Karte terminieren.
Offene Punkte	
Referenzen	Pic_MOKT_009 Aktivitätsdiagramm zu TUC_MOKT_406 writeEGKAudit

10.1.9 TUC_MOKT_407 selectKeyForAsymmetricExternalAuthentication

TIP1-A_3776 - Mobiles KT: "TUC_MOKT_407 selectKeyForAsymmetricExternalAuthentication"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_407 selectKeyForAsymmetricExternalAuthentication" gemäß Tab_MOKT_109 umsetzen.
[<=]

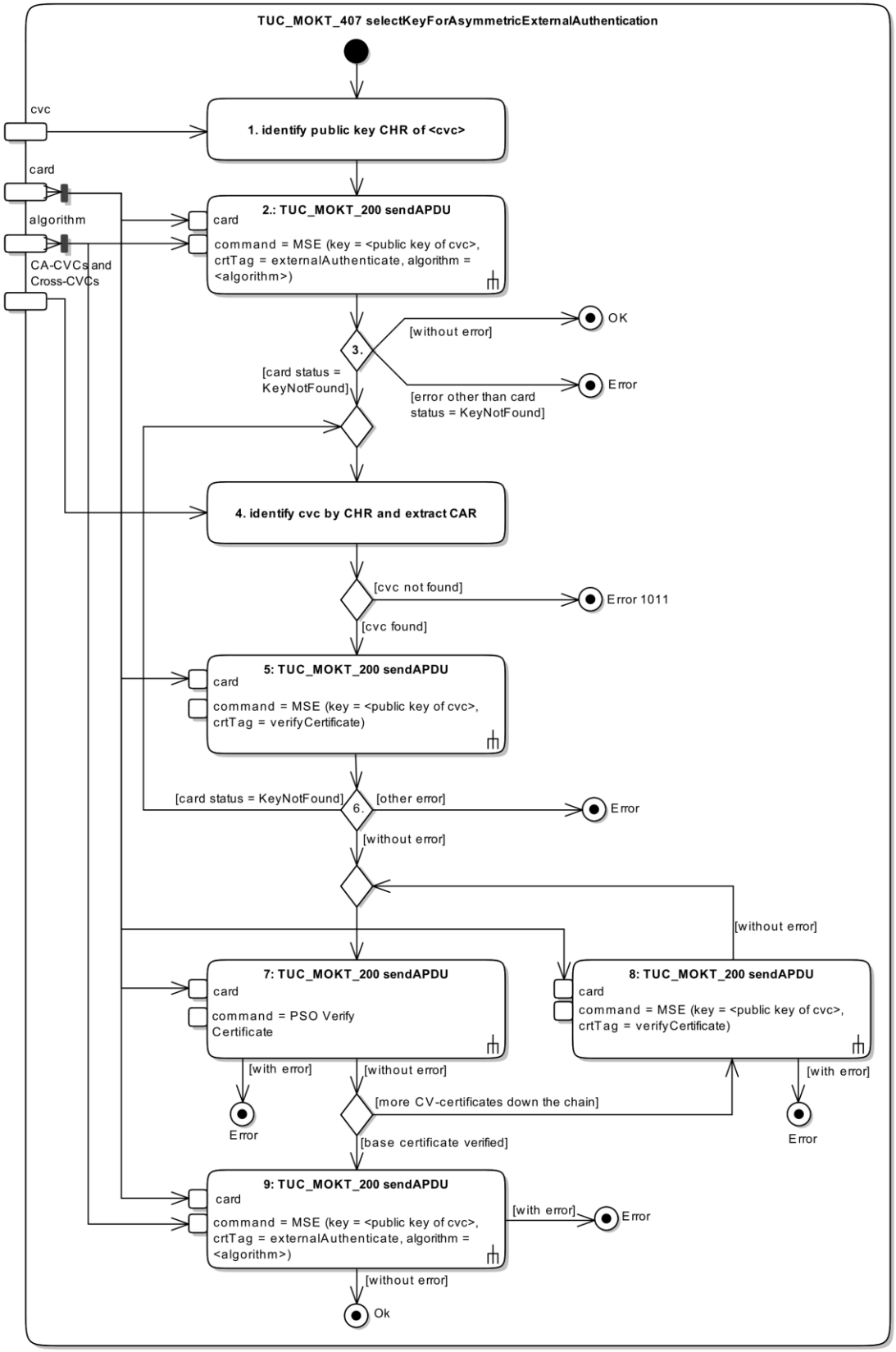


Abbildung 13: Pic_MOKT_010 Aktivitätsdiagramm zu TUC_MOKT_407 selectKeyForAsymmetricExternalAuthentication

Tabelle 22: Tab_MOKT_109 - TUC_MOKT_407 selectKeyForAsymmetricExternalAuthentication

TUC_MOKT_407 selectKeyForAsymmetricExternalAuthentication	
Beschreibung	TUC_MOKT_407 selektiert den öffentlichen Schlüssel eines importierten CV-Zertifikates. Nach Bedarf werden Zertifikate aus der Kette bis zur Root-CV-CA oder sogar bis zu einem Cross-CVC in der Karte verifiziert.
Anwendungsumfeld	Card-to-Card-Authentisierung
Initiierender Akteur	MobKT
Weitere Akteure	Karte (eGK, HBA, SMC-B)
Auslöser	TUC_MOKT_405 authenticateCardToCard
Vorbedingungen	• card ist eine Karte vom Typ eGK, HBA oder SMC-B und hat eine vom Mini-AK unterstützte Version.
Nachbedingungen	• Der öffentliche Schlüssel des CV-Zertifikats wurde in der Karte selektiert.
Eingangsdaten	• card: Karte, in der der Schlüssel selektiert werden soll • cvc: CV-Zertifikat des zu selektierenden Schlüssels • CV-CA-Zertifikate und Cross-CV-Zertifikate aus der Zertifikatskette des CV-Zertifikates bis zum Root-CA-Zertifikat der Karte. • algorithm: Algorithmus, der ausgewählt werden soll (z. B. rsaRoleCheck)
Ausgangsdaten	keine
Weitere Informationsobjekte	keine

Standardablauf	1. Der Mini-AK MUSS aus dem CV-Zertifikat die Referenz des Zertifikates (CHR) extrahieren. 2. Der Mini-AK MUSS in der Karte den zum CV-Zertifikat gehörigen öffentlichen Schlüssel für externe asymmetrische Authentisierung selektieren gemäß TUC_MOKT_200 mit a. card = card, b. Command = MANAGE SECURITY ENVIRONMENT mit Schlüsselreferenz = CVC.CHR, crtTag = externalAuthenticate und dem Algorithmus = algorithm. 3. Wenn der vorherige Schritt ohne Fehler beendet wurde, MUSS der Mini-AK den TUC_MOKT_407 sofort mit OK beenden. Wenn der vorherige Schritt mit dem Kartenstatus KeyNotFound beendet wurde, MUSS der Mini-AK mit dem folgenden Schritt fortfahren. 4. Der Mini-AK MUSS das CV-Zertifikat zu dem zuvor in Schritt 2 bzw. 5 vergebens selektierten öffentlichen Schlüssel identifizieren (CVC.CHR = Schlüsselreferenz) und die Zertifikatsreferenz der ausstellenden CA (CVC.CAR) aus diesem extrahieren. Durch dieses Vorgehen bildet sich eine Kette von Zertifikaten mit $CVC_{Nachfolger}$.CHR = $CVC_{Vorgänger}$.CAR. 5. Wenn das CV-Zertifikat vorliegt, MUSS der Mini-AK den öffentlichen Schlüssel zu obiger Zertifikatsreferenz der CA in der Karte zum Prüfen von CV-Zertifikaten selektieren gemäß TUC_MOKT_200 mit a. card = card, b. command = MANAGE SECURITY ENVIRONMENT mit crtTag = verifyCertificate und Schlüsselreferenz = CVC.CAR. 6. Wenn der vorherige Schritt mit dem Kartenstatus KeyNotFound endete, MUSS der Mini-AK mit dem Schritt 4 fortfahren. Wenn der vorherige Schritt ohne Fehler endete, MUSS der Mini-AK mit Schritt 7 fortfahren. 7. Der Mini-AK MUSS das Zertifikat aus Schritt 4 bzw. Schritt 8 durch die Karte überprüfen lassen gemäß TUC_MOKT_200 mit a. card = card, b. command = PSO Verify Certificate. 8. Wenn der vorherige Schritt ohne Fehler endete und es sich bei dem dabei geprüften Zertifikat um ein CA-Zertifikat aus der Zertifikatskette handelte, MUSS der Mini-AK den öffentlichen Schlüssel des in Schritt 7

	geprüften Zertifikats in der Karte selektieren gemäß TUC_MOKT_200 mit a. card = card, b. command = MANAGE SECURITY ENVIRONMENT Wenn TUC_MOKT_200 ohne Fehler endet, MUSS der Mini-AK mit dem Vorgänger-Zertifikat aus der durch Schritt 4 gebildeten Kette bei Schritt 7 fortfahren. 9. Wenn der Schritt 7 ohne Fehler endete und es sich bei dem dabei geprüften Zertifikat um das (Basis) CV-Zertifikat handelte, das heißt, dem als Parameter übergebenen ersten Zertifikat der Kette, MUSS der Mini-AK den zugehörigen öffentlichen Schlüssel in der Karte für externe asymmetrische Authentisierung selektieren gemäß TUC_MOKT_200 mit a. card = card, b. command = MANAGE SECURITY ENVIRONMENT mit crtTag = externalAuthenticate, Schlüsselreferenz = CVC.CHR und dem Algorithmus = algorithm. Endet TUC_MOKT_200 ohne Fehler, MUSS der Mini-AK TUC_MOKT_407 mit OK beenden.

Varianten/Alternativen	• Der Mini-AK KANN TUC_MOKT_407 ausgehend von der vollständigen CV-Zertifikatskette auf die Schritte 1 und 7 bis 9 beschränken Der Standardablauf optimiert die Selektion des Schlüssels unter der Maßgabe, dass CA-Zertifikate häufig der Karte bereits bekannt sind und nicht wiederholt von dieser verifiziert werden müssen. Dem Hersteller wird mit dieser Variante ermöglicht, auf diesen potentiellen Gewinn an Performanz zu verzichten, wenn er ihn für das MobKT als nachrangig betrachten sollte.
Fehlerfälle	• 3: endet TUC_MOKT_200 in Schritt 2 mit einem anderen Fehler als KeyNotFound, MUSS der Mini-AK TUC_MOKT_407 mit diesem Fehler beenden. • 4: liegt das referenzierte CV-Zertifikat dem Mini-AK nicht vor, MUSS es TUC_MOKT_407 mit dem Fehler 1011 beenden. • 6: endet TUC_MOKT_200 in Schritt 5 mit einem anderen Fehler als KeyNotFound, MUSS der Mini-AK TUC_MOKT_407 mit diesem Fehler beenden. • 7: endet Schritt 7 mit einem Fehler, MUSS der Mini-AK TUC_MOKT_407 mit diesem Fehler beenden. • 7: endet Schritt 8 mit einem Fehler, MUSS der Mini-AK TUC_MOKT_407 mit diesem Fehler beenden. • 7: endet Schritt 9 mit einem Fehler, MUSS der Mini-AK TUC_MOKT_407 mit diesem Fehler beenden.
Technische Fehlermeldungen	**Fehler Code** / **Bedeutung** 1011 / Fehler bei der C2C-Authentisierung Siehe auch aufgerufene TUCs: TUC_MOKT_200 sendAPDU
Weitere Anforderungen	keine
Anmerkungen, Bemerkungen	Die Spezifikation von CV-Zertifikaten und die in diesem TUC genutzten Kartenkommandos stimmen für eGK und HBA/SMC-B überein, sodass auch bei Zugriffen auf HBA/SMC-B die für die eGK spezifizierten Kommandos genutzt werden können.
Offene Punkte	
Referenzen	Pic_MOKT_010 Aktivitätsdiagramm zu TUC_MOKT_407 selectKeyForAsymmetricExternalAuthentication

10.1.10 TUC_MOKT_412 verifyPIN

TIP1-A_3777 - Mobiles KT: "TUC_MOKT_412 verifyPIN"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_412 verifyPIN" gemäß Tab_MOKT_110 umsetzen.
[<=]

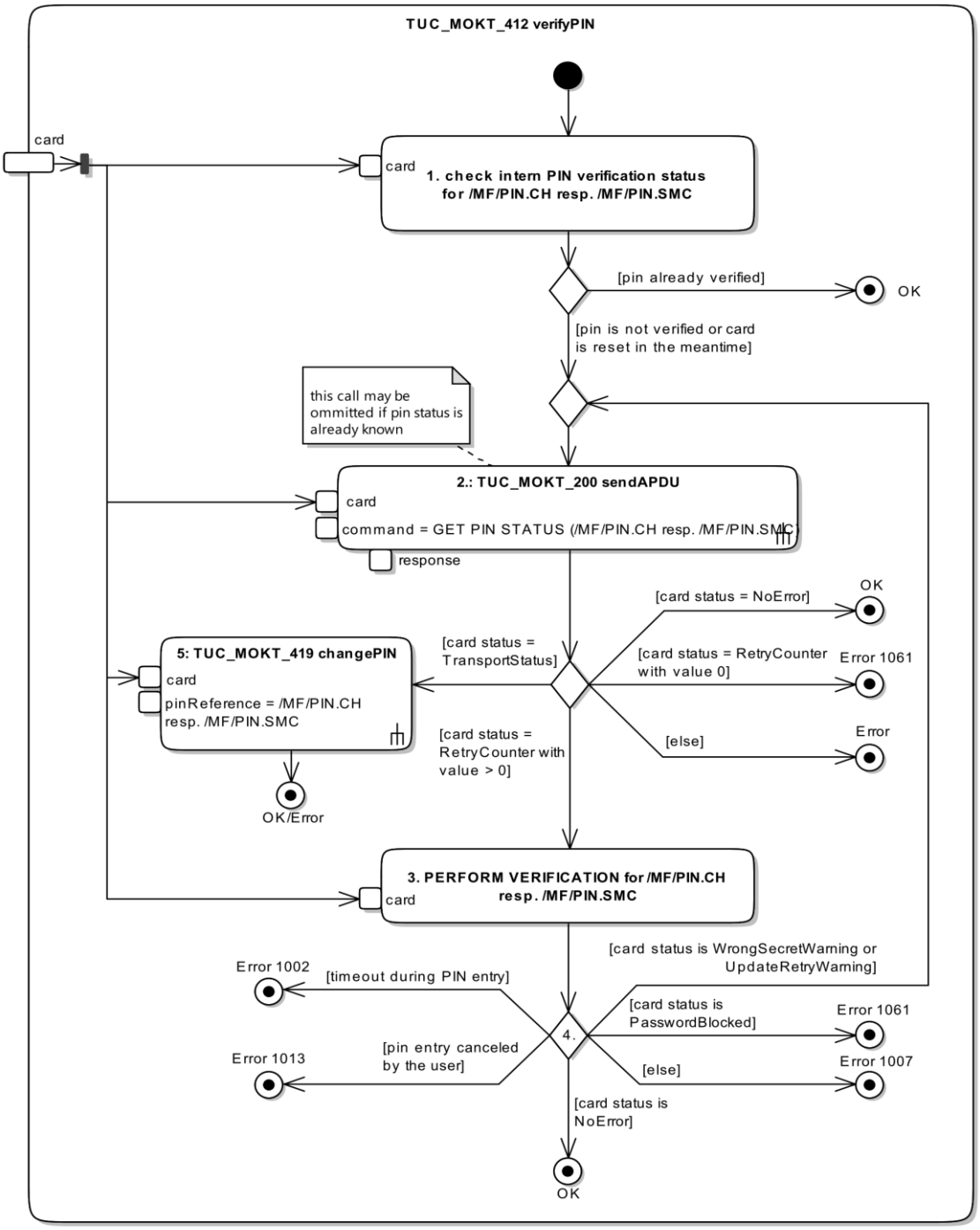


Abbildung 14: Pic_MOKT_011 Aktivitätsdiagramm zu TUC_MOKT_412 verifyPIN

Tabelle 23: Tab_MOKT_110 - TUC_MOKT_412 verifyPIN

TUC_MOKT_412 verifyPIN	
Beschreibung	TUC_MOKT_412 führt eine PIN-Eingabe zu einer Karte am MobKT durch

Anwendungsumfeld	PIN-Authorisierung von HBA und SMC-B im Mobilen Kartenterminal
Initiierender Akteur	MobKT
Weitere Akteure	Karte
Auslöser	TUC_MOKT_405 authenticateCardToCard
Vorbedingungen	• card ist eine Karte vom Typ HBA oder SMC-B mit einer vom Mini-AK unterstützten Version.
Nachbedingungen	• Die PIN wurde zur Verifikation an die Karte übertragen und die Karte hat sie akzeptiert.
Eingangsdaten	• card: Karte, mit der die PIN-Authentisierung durchgeführt werden soll.
Ausgangsdaten	keine
Weitere Informationsobjekte	keine
Standardablauf	Der Mini-AK MUSS abhängig vom Kartentyp von card die Schritte in TUC_MOKT_412 für das Passwortobjekt (pin) /MF/PIN.CH bzw. /MF/PIN.SMC durchführen. 1. Wenn pin für diese Karte bereits in diesem Steckzyklus der Karte verifiziert wurde und die Karte nicht zwischendurch zurückgesetzt wurde, MUSS der Mini-AK TUC_MOKT_412 ohne weiteren Zugriff auf die Karte mit OK beenden. Anderenfalls MUSS der Mini-AK mit dem folgenden Schritt fortfahren. 2. Der Mini-AK MUSS in diesem Schritt den Status der PIN gemäß TUC_MOKT_200 mit a. card = card b. command = GET PIN STATUS (passwordReference = pin) prüfen. Wenn TUC_MOKT_200 mit dem Kartenstatus NoError endet, MUSS der Mini-AK TUC_MOKT_412 ohne weitere Zugriffe auf die Karte mit OK beenden. 3. Wenn TUC_MOKT_200 mit dem Kartenstatus RetryCounter > 0 endet, MUSS der Mini-AK eine PIN-Authentifizierung für pin mit der Karte durchführen. Der Mini-AK MUSS die PIN mit dem Kommando VERIFY an die Karte senden. Der Mini-AK MUSS bei der PIN-Eingabe die Vorgaben zum Kommando SICCT PERFORM VERIFICATION (siehe [SICCT#5.19.1,5.19.2]) unter Berücksichtigung von Kapitel 4.2 umsetzen. Der Mini-AK MUSS dabei Display Messages nach Tabelle 24 verwenden.

	4. Wenn die Karte in Schritt 3 die PIN mit NoError akzeptiert hat, MUSS der Mini-AK TUC_MOKT_412 mit OK beenden. Wenn die Karte in Schritt 3 mit Status WrongSecretWarning/UpdateRetryWarning geantwortet hat, MUSS der Mini-AK mit Schritt 2 fortfahren.
Varianten/Alternativen	• Wenn TUC_MOKT_200 in Schritt 2 mit dem Kartenstatus TransportStatus endete, MUSS der Mini-AK die Umwandlung der Transport-PIN in eine reguläre PIN gemäß TUC_MOKT_419 mit 1. card = card durchführen. Wenn TUC_MOKT_419 ohne Fehler endet, MUSS der Mini-AK mit Schritt 3 fortfahren. Im Fehlerfall MUSS der Mini-AK TUC_MOKT_412 mit dem Status von TUC_MOKT_419 beenden. • Wenn dem Mini-AK der Status der PIN bereits bekannt ist, KANN der Mini-AK die Abfrage des Status von der Karte in Schritt 2 auslassen.
Fehlerfälle	• 2: Wenn TUC_MOKT_200 in Schritt 2 mit dem Kartenstatus RetryCounter endet und der Wert des Fehlbedienungszählers 0 ist, MUSS der Mini-AK TUC_MOKT_412 ohne weitere Zugriffe auf die Karte mit Error 1061 beenden und diese Tatsache auf dem Display anzeigen. • 2: Wenn TUC_MOKT_200 in Schritt 2 mit einem Fehler aber nicht mit dem Kartenstatus TransportStatus oder RetryCounter endet, MUSS der Mini-AK TUC_MOKT_412 mit diesem Fehler beenden. • 4: Wenn die PIN-Eingabe in Schritt 3 mit einer Zeitüberschreitung und damit ohne PIN-Eingabe endete, MUSS der Mini-AK TUC_MOKT_412 mit dem Fehler 1002 beenden. • 4: Wenn die PIN-Eingabe in Schritt 3 mit einem Abbruch durch den Anwender endete, MUSS der Mini-AK TUC_MOKT_412 mit dem Fehler 1013 beenden. • 4: Wenn die Karte die PIN in Schritt 3 mit dem Status PasswordBlocked ablehnte, MUSS der Mini-AK TUC_MOKT_412 mit dem Fehler 1061 beenden und diese Tatsache auf dem Display anzeigen. • 4: Wenn die Karte in Schritt 3 mit einem anderen Status als NoError, WrongSecretWarning/UpdateRetryWarning oder PasswordBlocked antwortete, MUSS der Mini-AK TUC_MOKT_412 mit dem Fehler 1007 beenden.
Technische Fehlermeldungen	**Fehler Code** / **Bedeutung**
	1002 / Zeitüberschreitung (Timeout)

	1007	Fehler beim Zugriff auf die Karte
	1013	Abbruch durch den Benutzer
	1061	PIN blockiert
	Siehe auch aufgerufene TUCs: TUC_MOKT_200 TUC_MOKT_419	
Weitere Anforderungen	keine	
Anmerkungen, Bemerkungen	Nach einer Ablehnung der PIN mit WrongSecretWarning ist die erneute Prüfung des PIN-Status erforderlich, da bei VERIFY WrongSecretWarning und UpdateRetryWarning nicht unterschieden werden können.	
Offene Punkte		
Referenzen	Pic_MOKT_011 Aktivitätsdiagramm zu TUC_MOKT_412 verifyPIN	

Folgende Tabelle „Tab_MoKT_111 Terminalanzeigen beim Eingeben der PIN am Kartenterminal" gibt die Terminalanzeigen für PIN- und PUK-Eingaben vor. Bei den in der Tabelle verwendeten Hexwerten „0x0B" und „0x0F" handelt es sich um herstellerbezogene Trennzeichen.

TIP1-A_3792 - Mobiles KT: Terminal-Anzeigen gemäß Vorgaben zu Darstellung von Display Messages
Das Mobile Kartenterminal MUSS die Terminalanzeigen gemäß Tab_MoKT_111 unter den Vorgaben zu Darstellung von Display Messages gemäß [SICCT#5.6.1] für PIN Eingaben umsetzen, wobei die in [SICCT#5.6.1] angegebenen maximalen Längen durch die tatsächlichen Längen der Terminalanzeigen gemäß Tab_MoKT_111 definiert werden.
[<=]

TIP1-A_3793 - Mobiles KT: Terminal-Anzeigen - Nummer der jeweiligen Functional Unit
Der Mini-AK des Mobilen Kartenterminals MUSS bei den Terminal-Anzeigen das ‚X' in 'SLOT: X' durch die Nummer der jeweiligen Functional Unit, in dem die betreffende Karte steckt, ersetzen.
[<=]

Tabelle 24: Tab_MoKT_111 Terminalanzeigen beim Eingeben der PIN am Kartenterminal

Karte/ Kontext	PIN-Referenz	I/O	Terminalanzeige
HBA	PIN.CH	I	`Eingabe•0x0BFreigabe- PIN•0x0BHBA 0x0FPIN.HBA:`

SMC	PIN.SMC	I	Eingabe•0x0B PIN•SMC•0x0BSLOT:*X* 0x0FPIN.SMC*B*:
Terminalanzeige bei erfolgreicher PIN-Eingabe	ALLE	O	PIN•0x0Berfolgreich•0x0Bverifiziert!
Terminalanzeige bei fehlerhafter PIN-Eingabe	ALLE	O	PIN•0x0Bfalsch•0x0Boder•0x0Bgesperrt!
Terminalanzeige bei PUK-Eingabe (sofern vorhanden)	HBA: PIN.CH	I	Eingabe•0x0BFreigabe- PUK•0x0BHBA 0x0FPUK.HBA:
	SMC-B: PIN.SMC	I	Eingabe•0x0BPUK•SMC •0x0BSLOT:*X* 0x0FPUK.SMC:
Terminalanzeige bei erfolgreicher PUK-Eingabe	Alle	O	PIN•0x0Berfolgreich•0x0Bentsperrt!
Terminalanzeige bei fehlerhafter PUK-Eingabe	Alle	O	PUK•0x0Bfalsch•0x0Boder•0x0Bgesperrt!
Terminalanzeige bei Eingabe einer neuen PIN	HBA: PIN.CH	I	Eingabe•0x0B Neue•0x0BFreigabe-PIN•0x0BHBA•0x0B(6-8 Ziffern) 0x0FPIN.HBA:
	SMC-B: PIN.SMC	I	Eingabe•0x0BNeue•0x0BPIN SMC• 0x0BSLOT:*X*•0x0B(6-8 Ziffern) 0x0FPIN.SMC:
Terminalanzeige bei Eingabe einer Transport-PIN	HBA: PIN.CH	I	Eingabe•0x0BTransport-0x0BPIN•0x0BHBA 0x0FT-PIN.HBA:
	SMC-B: PIN.SMC	I	Eingabe•0x0BTransport-0x0BPIN SMC•0x0BSLOT:*X* 0x0FPIN.SMC*B*:
Terminalanzeige bei	HBA: PIN.CH	I	Eingabe•0x0Bfür•HBA•0x0Bwiederholen! 0x0FPIN.HBA:

Wiederholung einer neuen PIN	SMC-B: PIN.SMC	I	Eingabe•***0x0B***PIN.SMC•***0x0B***in•SLOT:*X*•***0x0B***wiederholen! ***0x0F***PIN.SMCB:
Terminalanzeige bei Ungleichheit bei der Wiederholung der Eingabe der neuen PIN	ALLE	O	PIN•***0x0B*** nicht•***0x0B***identisch!•***0x0B***Abbruch!

10.1.11 TUC_MOKT_417 readFromEGK

TIP1-A_3778 - Mobiles KT: "TUC_MOKT_417 readFromEGK"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_417 readFromEGK" gemäß Tab_MOKT_112 umsetzen.
[<=]

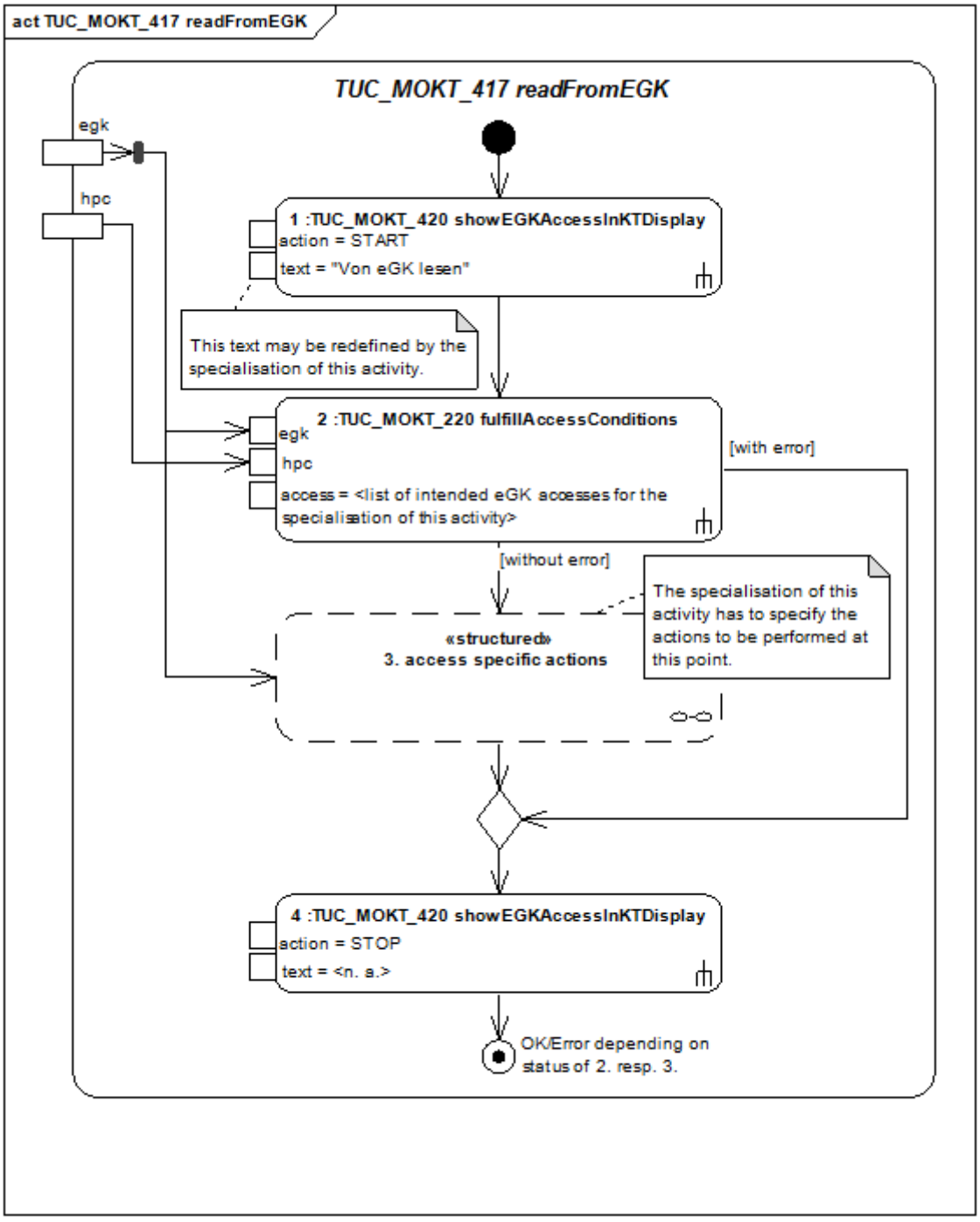


Abbildung 15: Pic_MOKT_012 Aktivitätsdiagramm zu TUC_MOKT_417 readFromEGK

Tabelle 25: Tab_MOKT_112 - TUC_MOKT_417 readFromEGK

TUC_MOKT_417 readFromEGK	
Beschreibung	Dies ist ein generischer TUC für lesende Zugriffe auf die eGK. Er definiert das grundlegende Muster eines solchen Zugriffes mit den Anzeigen der Zugriffe im Display und der vorherigen Durchführung notwendiger Authentisierungen gegenüber der eGK. Für die konkreten Anwendungsfälle werden entsprechende Ausprägungen dieses TUCs definiert, die im Besonderen die einzelnen Zugriffsoperationen auf die eGK definieren.
Anwendungsumfeld	Lesende Zugriffe auf die eGK im Rahmen von Fachanwendungen
Initiierender Akteur	MobKT
Weitere Akteure	eGK, HPC (HBA oder SMC-B), Leistungserbringer
Auslöser	Fachmodule
Vorbedingungen	• egk ist eine Karte vom Typ eGK mit vom Mini-AK unterstützter Version. • hpc, falls angegeben, ist eine Karte vom Typ HBA oder SMC-B mit vom Mini-AK unterstützter Version.
Nachbedingungen	keine
Eingangsdaten	• egk: als die Karte, auf die Zugegriffen werden soll. • hpc: als zugreifende Karte des Leistungserbringers
Ausgangsdaten	
Weitere Informationsobjekte	

Standardablauf	1. Der Mini-AK MUSS vor dem Zugriff auf die eGK diesen gemäß TUC_MOKT_420 mit a. action = START, b. text = „Von eGK lesen anzeigen. Der Text für die Anzeige kann für eine konkrete Ausprägung des TUCs anders definiert sein. 2. Der Mini-AK MUSS vor den vorgesehenen Zugriffen die notwendigen Authentisierungen gegenüber der eGK gemäß TUC_MOKT_220 mit a. egk = egk, b. hpc = hpc, c. access = die vorgesehenen Zugriffe auf die eGK, wie sie sich aus der konkreten Ausprägung des TUCs ergeben, veranlassen. Terminiert TUC_MOKT_220 mit einem Fehler, MUSS der Mini-AK direkt mit Schritt 4 fortfahren. 3. Der Mini-AK MUSS die für die konkrete Ausprägung vorgesehenen Zugriffe durchführen. 4. Unabhängig von den in Schritt 3 aufgetretenen Fehlern MUSS der Mini-AK die Löschung des Anzeigetextes im Display gemäß TUC_MOKT_420 mit a. action = STOP, b. text = n. a. veranlassen. Falls Schritt 2 oder 3 mit einem Fehler endete, MUSS der Mini-AK TUC_MOKT_417 mit diesem Fehler, andernfalls mit OK beenden.
Varianten/Alternativen	
Fehlerfälle	
Technische Fehlermeldungen	Siehe aufgerufene TUCs: TUC_MOKT_220 fulfillAccessConditions, TUC_MOKT_420 showEGKAccessInKTDisplay und Fehler definiert durch die konkrete Ausprägung
Weitere Anforderungen	keine
Anmerkungen, Bemerkungen	keine
Offene Punkte	

Referenzen	Pic_MOKT_012 Aktivitätsdiagramm zu TUC_MOKT_417 readFromEGK

10.1.12 TUC_MOKT_418 checkEGK

TIP1-A_3779 - Mobiles KT: "TUC_MOKT_418 checkEGK"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_418 checkEGK" gemäß Tab_MOKT_113 umsetzen.
[<=]

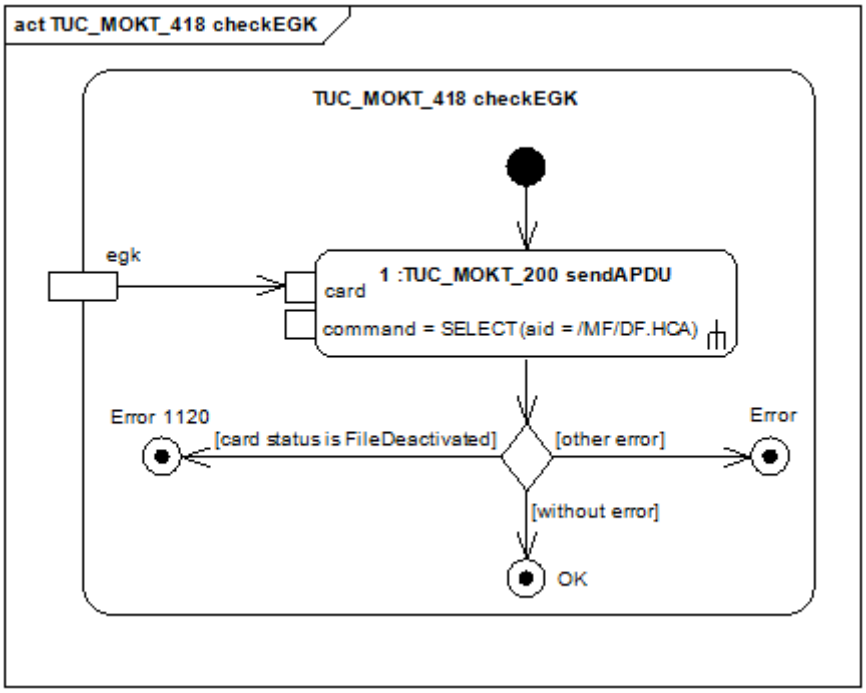


Abbildung 16: Pic_MOKT_013 Aktivitätsdiagramm zu TUC_MOKT_418 checkEGK

Tabelle 26: Tab_MOKT_113 - TUC_MOKT_418 checkEGK

TUC_MOKT_418 checkEGK	
Beschreibung	Der TUC_MOKT_418 prüft, ob eine technische Sperrung der eGK vorliegt.
Anwendungsumfeld	Fachliche Zugriffe auf die eGK
Initiierender Akteur	MobKT
Weitere Akteure	eGK
Auslöser	Fachmodul
Vorbedingungen	• egk ist eine Karte vom Typ eGK mit einer vom Mini-AK unterstützten Version.

Nachbedingungen	• dem MobKT ist bekannt, dass die eGK nicht technisch gesperrt ist.
Eingangsdaten	• egk: eGK als zu prüfende Karte
Ausgangsdaten	keine
Weitere Informationsobjekte	keine
Standardablauf	1. Der Mini-AK MUSS gemäß TUC_MOKT_200 mit i. card = egk, ii. command = SELECT mit aid gleich dem applicationIdentifier von /MF/DF.HCA , versuchen, die Gesundheitsanwendung zu selektieren. Wenn der TUC_MOKT_200 ohne einen Fehler endet, MUSS der Mini-AK den TUC_MOKT_418 mit OK beenden.
Varianten/Alternativen	• Wenn dem Mini-AK der Status bezüglich der Sperrung der Karte bereits bekannt ist, KANN der Mini-AK auf den Kartenzugriff in Schritt 1 verzichten und direkt TUC_MOKT_418 mit dem Status OK bzw. 1120 beenden.
Fehlerfälle	• 1: Wenn TUC_MOKT_200 in Schritt 1 mit dem Kartenstatus FileDeactivated endet, MUSS der Mini-AK den TUC_MOKT_418 mit dem Fehler 1120 beenden. • 1: Wenn TUC_MOKT_200 in Schritt 1 mit einem anderen Fehler als Kartenstatus gleich FileDeactivated endet, so MUSS der Mini-AK den TUC_MOKT_418 mit diesem Fehler beenden
Technische Fehlermeldungen	**Fehler Code** / **Bedeutung** 1120 / Karte gesperrt Siehe auch aufgerufene TUCs: TUC_MOKT_200 sendAPDU
Weitere Anforderungen	keine
Anmerkungen, Bemerkungen	keine
Offene Punkte	
Referenzen	Pic_MOKT_013 Aktivitätsdiagramm zu TUC_MOKT_418 checkEGK

10.1.13 TUC_MOKT_419 changePIN

TIP1-A_3780 - Mobiles KT: "TUC_MOKT_419 changePIN"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_419 changePIN" gemäß Tab_MOKT_114 umsetzen.
[<=]

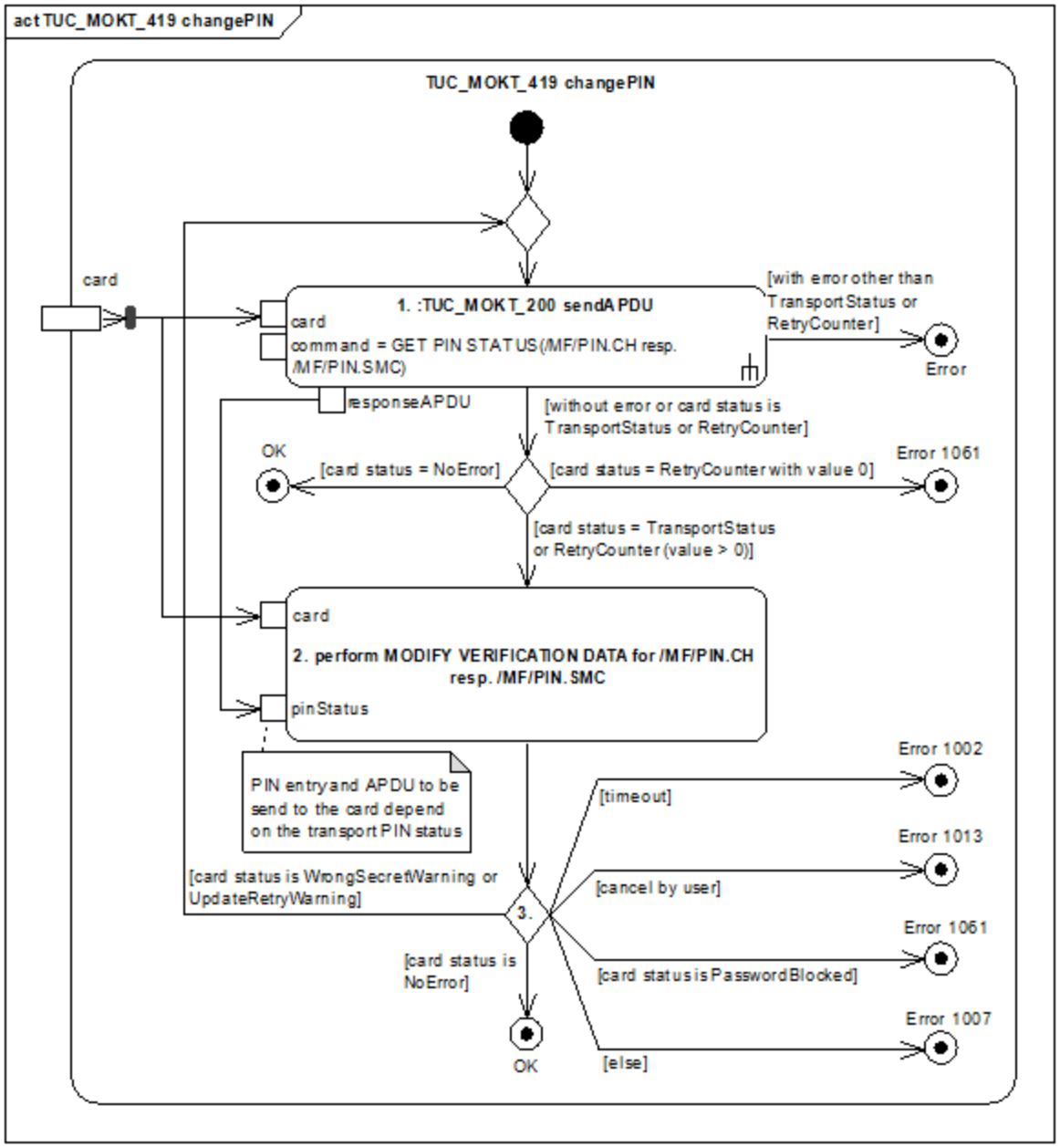


Abbildung 17: Pic_MOKT_014 Aktivitätsdiagramm zu TUC_MOKT_419 changePIN

Tabelle 27: Tab_MOKT_114 - TUC_MOKT_419 changePIN

TUC_MOKT_419 changePIN	
Beschreibung	TUC_MOKT_419 führt eine PIN-Änderung zu einer Karte durch.
Anwendungsumfeld	Ändern der PIN von HBA oder SMC-B Wandlung einer Transport-PIN von HBA oder SMC-B in eine „normale" PIN
Initiierender Akteur	MobKT

Weitere Akteure	Karte
Auslöser	TUC_MOKT_412 verifyPIN Interaktion am Mini-PS
Vorbedingungen	• hpc ist eine Karte vom Typ HBA oder SMC-B mit einer vom Mini-AK unterstützten Version.
Nachbedingungen	1. Eine PIN-Änderung ist mit der Karte durchgeführt und von der Karte akzeptiert worden.
Eingangsdaten	2. hpc: Karte, für die die PIN geändert werden soll.
Ausgangsdaten	keine
Weitere Informationsobjekte	keine
Standardablauf	1. Der Mini-AK MUSS abhängig vom Kartentyp von hpc die Schritte in TUC_MOKT_419 für das Passwortobjekt (pin) /MF/PIN.CH bzw. /MF/PIN.SMC durchführen. 2. Der Mini-AK MUSS den PIN-Status gemäß TUC_MOKT_200 mit a. card = hpc, b. command = GET PIN STATUS (passwordReference = pin) prüfen. Wenn TUC_MOKT_200 mit dem Kartenstatus NoError endet, MUSS der Mini-AK TUC_MOKT_419 mit OK beenden. 3. Wenn TUC_MOKT_200 mit Kartenstatus TransportStatus oder RetryCounter (Fehlbedienungszähler > 0) endete, MUSS der Mini-AK eine PIN-Änderung von pin mit der Karte durchführen. Der Mini-AK MUSS die neue und ggf. alte PIN mit dem Kommando CHANGE REFERENCE DATA an die Karte übergeben. Ob eine alte PIN einzugeben ist, ob sie automatisch vom MobKT in das Kartenkommando eingefügt werden kann oder ob sie entfallen kann, hängt vom TransportStatus von pin ab und der Mini-AK MUSS die Fälle entsprechend unterstützen. Der Mini-AK MUSS für die PIN-Eingaben die Vorgaben zum Kommando SICCT MODIFY VERIFICATION DATA (siehe [SICCT#5.20.1,5.20.2]) unter Berücksichtigung von Kapitel 4.2 umsetzen. Der Mini-AK MUSS bei der PIN-Änderung Display Messages nach Tabelle 24 verwenden. 4. Wenn die Karte in Schritt 2 die neue PIN mit NoError akzeptiert hat, MUSS der Mini-AK TUC_MOKT_419 mit

<table>
<tr><td></td><td>OK beenden.
Wenn die Karte in Schritt 2 mit dem Status WrongSecretWarning oder UpdateRetryWarning geantwortet hat, MUSS der Mini-AK mit Schritt 0 fortfahren.</td></tr>
<tr><td>Varianten/Alternativen</td><td>• 1: Wenn dem Mini-AK der PIN-Status bereits bekannt ist, KANN der Mini-AK in Schritt 1 auf das Kartenkommando verzichten.</td></tr>
<tr><td>Fehlerfälle</td><td>• 1: Wenn TUC_MOKT_200 in Schritt 1 mit einem Fehler außer TransportStatus oder RetryCounter endete, MUSS der Mini-AK TUC_MOKT_419 mit diesem Fehler beenden.
• 1: Wenn TUC_MOKT_200 in Schritt 1 mit dem Kartenstatus RetryCounter und einem Wert des Fehlbedienungszählers von 0 endete, MUSS der Mini-AK TUC_MOKT_419 mit Fehler 1061 beenden.
• 3: Wenn die PIN-Eingabe (alt, neu oder Wiederholung) in Schritt 3 mit einer Zeitüberschreitung und damit ohne PIN-Eingabe endete, MUSS der Mini-AK TUC_MOKT_419 mit dem Fehler 1002 beenden.
• 3: Wenn die PIN-Eingabe in Schritt 2mit einem Abbruch durch den Anwender endete, MUSS der Mini-AK TUC_MOKT_419 mit dem Fehler 1013 beenden.
• 3: Wenn die Karte in Schritt 3 mit Status PasswordBlocked antwortete, MUSS der Mini-AK TUC_MOKT_419 mit Fehler 1061 beenden.
• 3: Wenn die Karte in Schritt 3 mit einem anderen Status als NoError, WrongSecretWarning/UpdateRetryWarning oder PasswordBlocked antwortete, MUSS der Mini-AK TUC_MOKT_419 mit dem Fehler 1007 beenden.</td></tr>
<tr><td>Technische Fehlermeldungen</td><td><table><tr><th>Fehler Code</th><th>Bedeutung</th></tr><tr><td>1002</td><td>Zeitüberschreitung (Timeout)</td></tr><tr><td>1007</td><td>Fehler beim Zugriff auf die Karte</td></tr><tr><td>1013</td><td>Abbruch durch den Benutzer</td></tr><tr><td>1061</td><td>PIN blockiert</td></tr><tr><td colspan="2">Siehe auch aufgerufene TUCs:
TUC_MOKT_200 sendAPDU</td></tr></table></td></tr>
<tr><td>Weitere Anforderungen</td><td>keine</td></tr>
<tr><td>Anmerkungen, Bemerkungen</td><td>Siehe Anmerkungen zu TUC_MOKT_412 verifyPIN</td></tr>
</table>

Offene Punkte	
Referenzen	Pic_MOKT_014 Aktivitätsdiagramm zu TUC_MOKT_419 changePIN

10.1.14 TUC_MOKT_420 showEGKAccessInKTDisplay

TIP1-A_3781 - Mobiles KT: "TUC_MOKT_420 showEGKAccessInKTDisplay"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_420 showEGKAccessInKTDisplay" gemäß Tab_MOKT_115 umsetzen.
[<=]

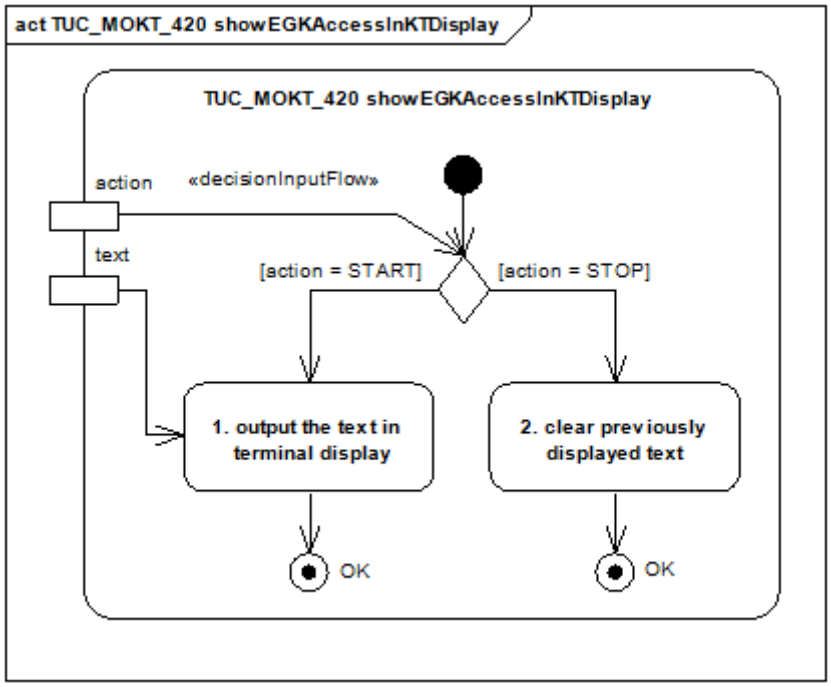


Abbildung 18: Pic_MOKT_015 Aktivitätsdiagramm zu TUC_MOKT_420 showEGKAccessInKTDisplay

Tabelle 28: Tab_MOKT_115 - TUC_MOKT_420 showEGKAccessInKTDisplay

TUC_MOKT_420 showEGKAccessInKTDisplay	
Beschreibung	TUC_MOKT_420 veranlasst die Ausgabe eines Textes auf dem Kartenterminaldisplay des Kartenterminal-Moduls oder die Löschung eines solchen Textes
Anwendungsumfeld	Hinweise auf die Nutzung der eGK an den Anwender
Initiierender Akteur	MobKT
Weitere Akteure	keine

Auslöser	TUC_MOKT_417 readFromEGK
Vorbedingungen	keine
Nachbedingungen	keine
Eingangsdaten	• action: START oder STOP, je nachdem, ob der Text angezeigt oder gelöscht werden soll • text: Text der dargestellt werden soll
Ausgangsdaten	keine
Weitere Informationsobjekte	keine
Standardablauf	1. Wenn action den Wert START hat, MUSS der Mini-AK die Anzeige des Textes text auf dem Kartenterminaldisplay, das dem Steckplatz der egk zugeordnet ist, veranlassen. Zuvor auf diese Weise ausgegebene Texte an diesem Display KANN das Kartenterminal dabei löschen. 2. Wenn action den Wert STOP hat, MUSS der Mini-AK die Löschung der Anzeige aller zuvor mit START auf dem Kartenterminaldisplay, das dem Steckplatz der egk zugeordnet, angezeigten Texte veranlassen.
Varianten/Alternativen	keine
Fehlerfälle	keine
Technische Fehlermeldungen	keine definiert
Weitere Anforderungen	keine
Anmerkungen, Bemerkungen	Falls das MobKT über mehrere Displayeinheiten verfügt, denen die Steckplätze der Karten zugeordnet sind, kann sich das zu verwendende Display aus dem Steckplatz der eGK ergeben.
Offene Punkte	
Referenzen	Pic_MOKT_015 Aktivitätsdiagramm zu TUC_MOKT_420 showEGKAccessInKTDisplay

10.1.15 TUC_MOKT_421 unblockPIN

TIP1-A_3794 - Mobiles KT: "TUC_MOKT_421 unblockPIN"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_421 unblockPIN" gemäß Tab_MOKT_121 umsetzen.
[<=]

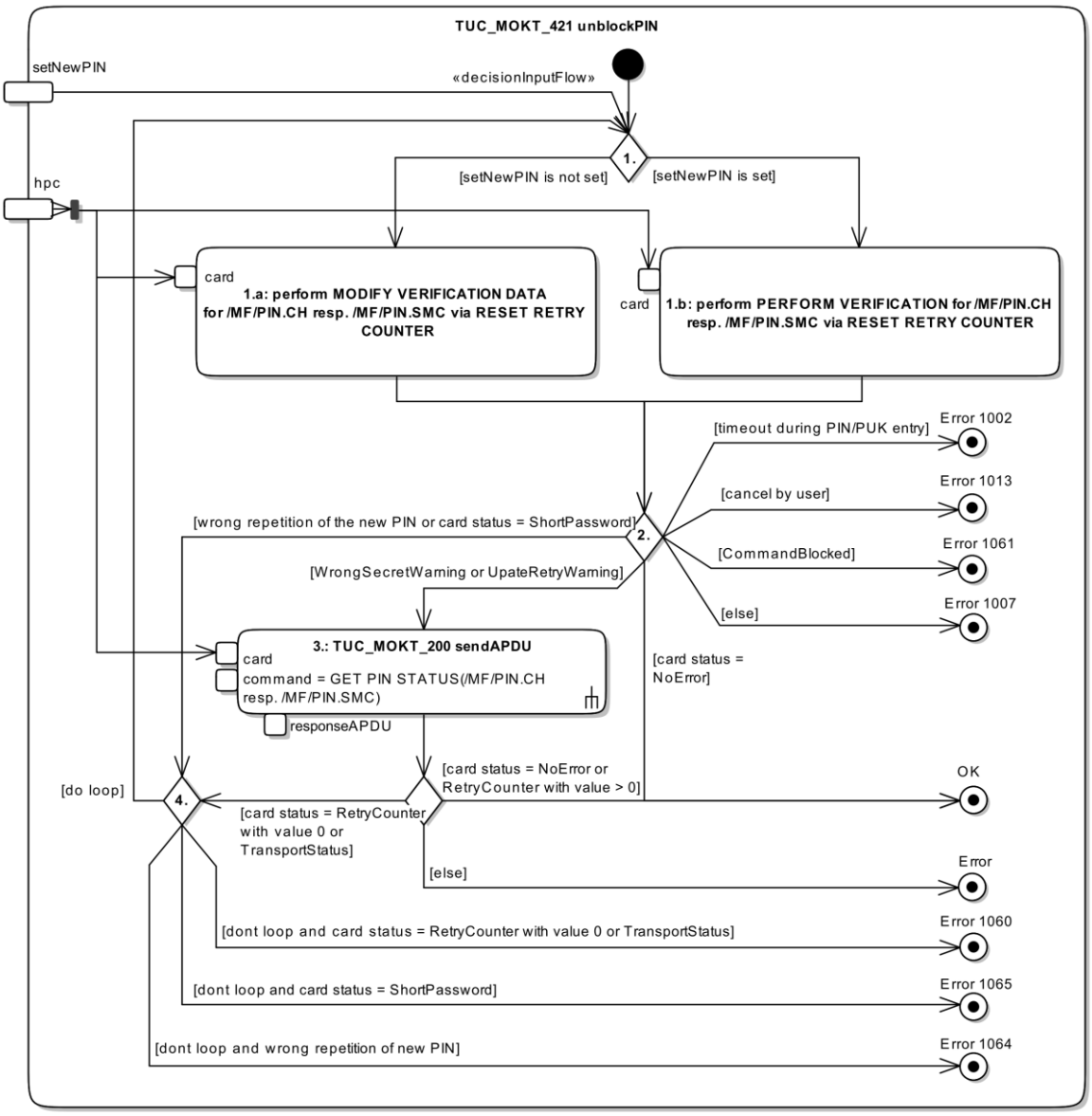


Abbildung 19: Pic_MOKT_023 – Aktivitätsdiagramm zu TUC_MOKT_421 unblockPIN

Tabelle 29: Tab_MOKT_121 - TUC_MOKT_421 unblockPIN

TUC_MOKT_421 unblockPIN	
Beschreibung	TUC_MOKT_421 setzt den Fehlbedienungszähler einer PIN von HBA oder SMC-B durch Eingabe der PUK auf seinen Startwert zurück.
Anwendungsumfeld	Zurücksetzen des Fehlbedienungszählers einer gesperrten PIN
Initiierender Akteur	MobKT
Weitere Akteure	Karte

Auslöser	PIN Verwalten
Vorbedingungen	• hpc ist eine Karte vom Typ HBA oder SMC-B mit einer vom Mini-AK unterstützten Version.
Nachbedingungen	• Eine PIN-Entsperrung (RESET RETRY COUNTER) ist mit der Karte durchgeführt und von der Karte akzeptiert worden.
Eingangsdaten	1. hpc: Karte, für die die PIN zurückgesetzt werden soll. 2. setNewPIN: Flag, das angibt, ob beim Entsperren der PIN zugleich eine neue PIN eingegeben werden soll
Ausgangsdaten	keine
Weitere Informationsobjekte	keine
Standardablauf	Der Mini-AK MUSS abhängig vom Kartentyp von hpc die Schritte in TUC_MOKT_421 für das Passwortobjekt (pin) /MF/PIN.CH bzw. /MF/PIN.SMC durchführen. 1. Der Mini-AK MUSS, a. wenn das Flag setNewPIN gesetzt ist, ein Entsperren des Passwortobjektes pin mit PIN-Änderung mit der Karte hpc durchführen. Die PUK und die neue PIN MUSS das MobKT mit dem Kommando RESET RETRY COUNTER an die Karte übergeben. Der Mini-AK MUSS bei der PUK-/PIN-Eingabe die Vorgaben zum Kommando SICCT MODIFY VERIFICATION DATA (siehe [SICCT#5.20.1,5.20.2]) unter Berücksichtigung von Kapitel 4.2 umsetzen. Das MobKT MUSS bei der PIN- bzw. PUK-Eingabe Display Messages nach Tabelle 24 verwenden. b. wenn das Flag setNewPIN nicht gesetzt ist, ein Entsperren des Passwortobjektes pin ohne PIN-Änderung mit der Karte hpc durchführen. Das MobKT MUSS die PUK mit dem Kommando RESET RETRY COUNTER an die Karte übergeben. Der Mini-AK MUSS bei der PUK-Eingabe die Vorgaben zum Kommando SICCT PERFORM VERIFICATION (siehe [SICCT#5.19.1,5.19.2]) unter Berücksichtigung von Kapitel 4.2 umsetzen. Das MobKT MUSS bei der PUK-Eingabe Display Messages nach Tabelle 24 verwenden. 2. Wenn die Karte in Schritt 1 die Entsperrung mit NoError akzeptiert hat, MUSS der Mini-AK TUC_MOKT_421 mit OK beenden. Wenn die Wiederholung der neuen PIN in Schritt 1.b nicht korrekt erfolgte oder die Karte den Status

	ShortPassword meldete, MUSS der Mini-AK mit Schritt 4 fortfahren. 3. Wenn die Karte in Schritt 1 mit dem Status WrongSecretWarning oder UpdateRetryWarning geantwortet hat, MUSS der Mini-AK den PIN-Status von pin gemäß TUC_MOKT_200 mit a. card = hpc, b. command = GET PIN STATUS (pin) prüfen. Wenn TUC_MOKT_200 mit dem Kartenstatus NoError oder RetryCounter mit Fehlbedienungszähler > 0 endet, MUSS der Mini-AK TUC_MOKT_421 mit OK beenden. 4. Wenn eine automatische Wiederholung der PIN-Eingabe vorgesehen ist, MUSS der Mini-AK mit Schritt 1 fortfahren. Der Mini-AK KANN die automatische Wiederholung vorsehen. Der Mini-AK KANN die automatische Wiederholung nicht vorsehen. Das MobKT KANN die automatische Wiederholung, auch abhängig vom konkreten Fehler, konfigurierbar gestalten.
Varianten/Alternativen	keine
Fehlerfälle	• 2: Wenn Schritt 1 mit einem Timeout während der PUK-/PIN-Eingabe endete, MUSS der Mini-AK TUC_MOKT_421 mit Fehler 1002 beenden. • 2: Wenn Schritt 1 mit einem Abbruch durch den Anwender endete, MUSS der Mini-AK TUC_MOKT_421 mit Fehler 1013 beenden. • 2: Wenn Schritt 1 mit dem Kartenstatus CommandBlocked endete, MUSS der Mini-AK TUC_MOKT_421 mit Fehler 1061 beenden. • 2: Wenn Schritt 1 mit einem anderen Kartenstatus außer CommandBlocked, ShortPasswort, WrongSecretWarning und UpdateRetryWarning endete, MUSS der Mini-AK TUC_MOKT_421 mit Fehler 1007 beenden. • 3: Wenn TUC_MOKT_200 in Schritt 3 mit einem Fehler außer card status = RetryCounter endete, MUSS der Mini-AK TUC_MOKT_421 mit diesem Fehler beenden. • 4: Wenn TUC_MOKT_200 in Schritt 3 einen card status = RetryCounter mit Wert 0 oder TransportStatus lieferte und in Schritt 4 keine automatische Wiederholung der PIN-Eingabe vorgesehen ist, MUSS der Mini-AK TUC_MOKT_421 mit dem Fehler 1060 beenden. • 4: Wenn Schritt 1 einen card status = ShortPassword (oder zusätzlich „LongPassword" bei Generation 2) lieferte und in Schritt 4 keine automatische Wiederholung der PIN-Eingabe vorgesehen ist, MUSS

	der Mini-AK TUC_MOKT_421 mit dem Fehler 1065 beenden. • 4: Wenn Schritt 1.b wegen einer falschen Wiederholung der neuen PIN endete und in Schritt 4 keine automatische Wiederholung der PIN-Eingabe vorgesehen ist, MUSS der Mini-AK TUC_MOKT_421 mit dem Fehler 1064 beenden.	
Technische Fehlermeldungen	**Fehler Code**	**Bedeutung**
	1002	Zeitüberschreitung (Timeout)
	1007	Fehler beim Zugriff auf die Karte
	1013	Abbruch durch den Benutzer
	1060	PIN gesperrt oder Änderung erforderlich
	1061	PUK gesperrt
	1064	Neue PIN nicht identisch
	1065	Neue PIN zu kurz / zu lang
	Siehe auch aufgerufene TUCs: TUC_MOKT_200 sendAPDU	
Weitere Anforderungen	Das MobKT SOLL bei der Eingabe von PUK und neuer PIN die Mindestlänge der PIN bereits bei der PIN-Eingabe prüfen und den Abschluss der Eingabe bei zu kurzen Werten nicht zulassen.	
Anmerkungen, Bemerkungen	Siehe Anmerkungen zu TUC_MOKT_412 verifyPIN	
Offene Punkte		
Referenzen	Pic_MOKT_023 – Aktivitätsdiagramm zu TUC_MOKT_421 unblockPIN	

10.1.16 TUC_MOKT_438 checkEGKAuthCertificate

TIP1-A_3782 - Mobiles KT: "TUC_MOKT_438 checkEGKAuthCertificate"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_438 checkEGKAuthCertificate" gemäß Tab_MOKT_116 - TUC_MOKT_438 checkEGKAuthCertificate umsetzen.

[<=]

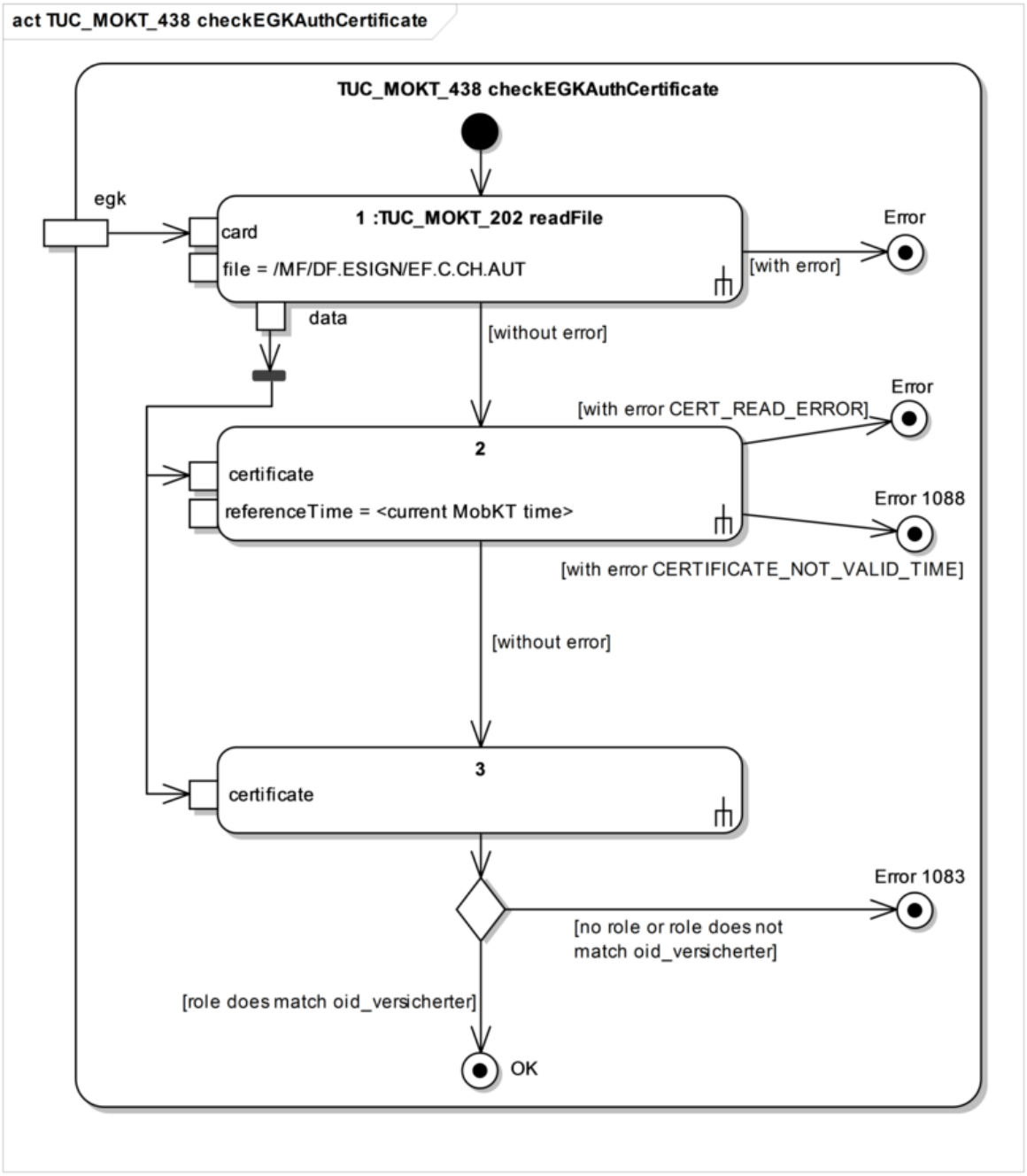


Abbildung 20: Pic_MOKT_016 Aktivitätsdiagramm zu TUC_MOKT_438 checkEGKAuthCertificate

Tabelle 30: Tab_MOKT_116 - TUC_MOKT_438 checkEGKAuthCertificate

TUC_MOKT_438 checkEGKAuthCertificate (alias TUC_MOKT_438 checkEGKAuthCert)	
Beschreibung	TUC_MOKT_438 prüft das /MF/DF.ESIGN/EF.C.CH.AUT Zertifikat der eGK
Anwendungsumfeld	Fachliche Zugriffe auf die Gesundheitskarte

Initiierender Akteur	MobKT
Weitere Akteure	eGK
Auslöser	Fachmodule
Vorbedingungen	• egk ist eine Karte vom Typ eGK mit einer vom Mini-AK unterstützten Version.
Nachbedingungen	• Das eGK-AUT-Zertifikat der eGK ist dem MobKT als gültiges Zertifikat eines Versicherten bekannt.
Eingangsdaten	• egk: eGK deren Zertifikat geprüft werden soll
Ausgangsdaten	keine
Weitere Informationsobjekte	
Standardablauf	1. Der Mini-AK MUSS das eGK-AUT-Zertifikat der eGK gemäß TUC_MOKT_202 mit a. card = card b. file = /MF/DF.ESIGN/EF.C.C.CH.AUT, von der Karte lesen. 2. Wenn das Zertifikat in Schritt 1 ohne Fehler ermittelt wurde, MUSS der Mini-AK das Zertifikat gemäß TUC_PKI_002 mit a. Zertifikat = eGK-AUT-Zertifikat aus Schritt 1, b. Referenzzeitpunkt = Systemzeit des MobKT auf Gültigkeit prüfen. 3. Wenn TUC_PKI_002 in Schritt 2 ohne Fehler endet (das Zertifikat ist gültig), MUSS der Mini-AK die im Zertifikat ausgewiesene Rolle gemäß TUC_PKI_009 mit a. End-Entity-Zertifikaten = AUT-Zertifikat aus Schritt 1 ermitteln. Wenn TUC_PKI_009 in Schritt 3 eine Rolle liefert und die ermittelte Rolle oid_versicherter (siehe [gemSpec_OID]) entspricht, MUSS der Mini-AK TUC_MOKT_438 mit OK beenden.
Varianten/Alternativen	• Wenn der Mini-AK das Zertifikat der eGK bereits in dem Steckzyklus der Karte gelesen hat, KANN der Mini-AK in Schritt 1 auf das erneute Lesen des Zertifikats verzichten und das bereits vorliegende Zertifikat im restlichen Ablauf von TUC_MOKT_438 verwenden.

Fehlerfälle	• 1: Wenn TUC_MOKT_202 in Schritt 1 mit einem Fehler endet, MUSS der Mini-AK TUC_MOKT_438 mit diesem Fehler beenden. • 2: Wenn TUC_PKI_002 in Schritt 2 mit dem Fehler CERT_READ_ERROR endet, MUSS der Mini-AK TUC_MOKT_438 mit diesem Fehler beenden. • 2: Wenn TUC_PKI_002 in Schritt 2 mit dem Fehler CERTIFICATE_NOT_VALID_TIME (das Zertifikat ist nicht gültig) endet, MUSS der Mini-AK TUC_MOKT_438 mit Fehler 1088 beenden. • 3: Wenn TUC_PKI_009 in Schritt 3 keine Rolle liefert oder die ermittelte Rolle aus Schritt 3 nicht mit oid_versicherter übereinstimmt, MUSS der Mini-AK TUC_MOKT_438 mit Fehler 1083 beenden.	
Technische Fehlermeldungen	Fehler Code	Bedeutung
	1083	Rolle oid_versicherter stimmt nicht überein
	1088	Zertifikat ist zeitlich nicht gültig
	Siehe auch aufgerufene TUCs: TUC_MOKT_202 readFile TUC_PKI_002 Gültigkeitsprüfung des Zertifikats TUC_PKI_009 Rollenermittlung	
Weitere Anforderungen	keine	
Anmerkungen, Bemerkungen	keine	
Offene Punkte		
Referenzen	Pic_MOKT_016 Aktivitätsdiagramm zu TUC_MOKT_438 checkEGKAuthCertificate	

10.1.17 TUC_MOKT_470 encryptData

TIP1-A_3783 - Mobiles KT: "TUC_MOKT_470 encryptData"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_470 encryptData" gemäß Tab_MOKT_118 umsetzen.
[<=]

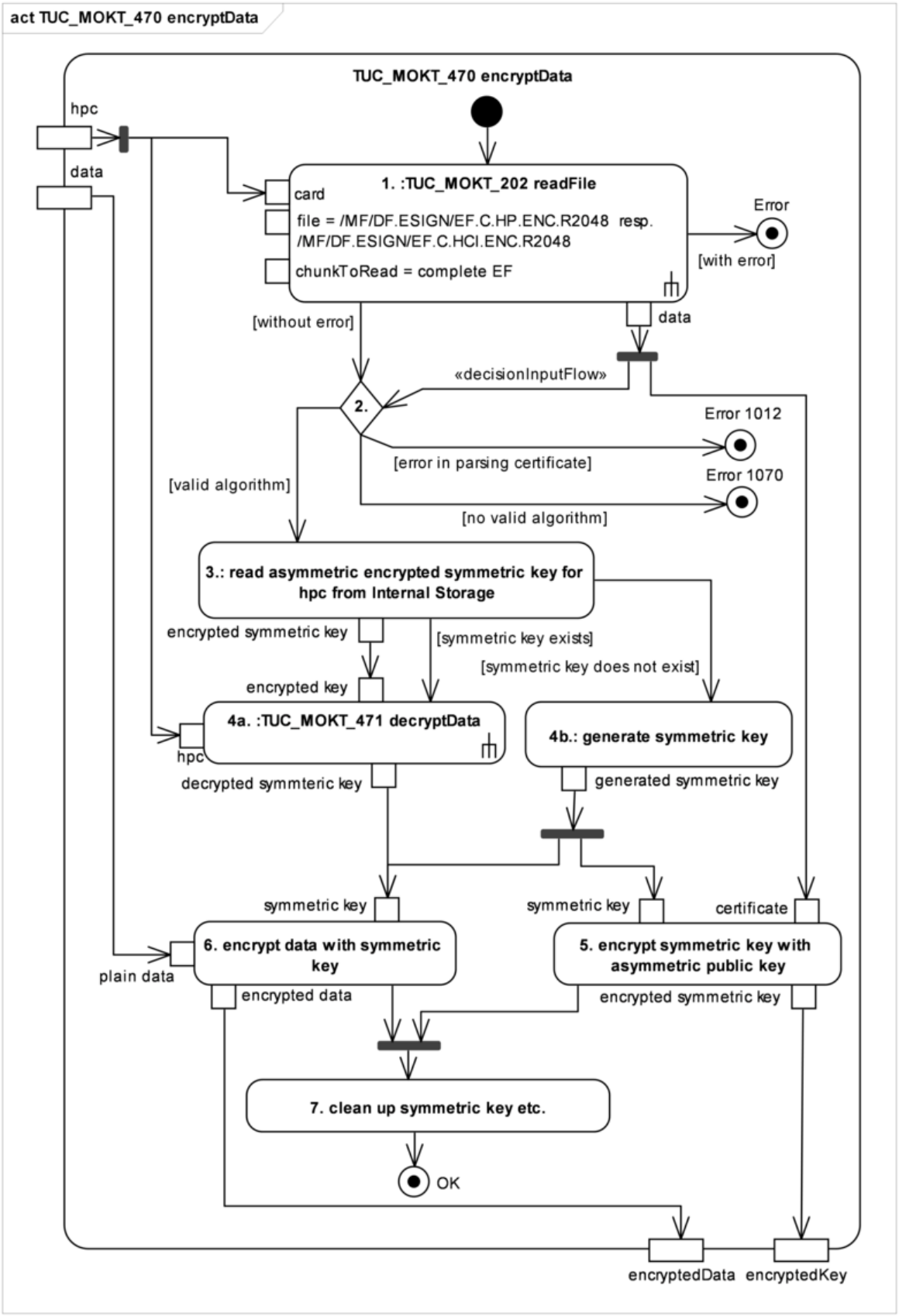


Abbildung 21: Pic_MOKT_018 Aktivitätsdiagramm zu TUC_MOKT_470 encryptData

Tabelle 31: Tab_MOKT_118 - TUC_MOKT_470 encryptData

TUC_MOKT_470 encryptData	
Beschreibung	TUC_MOKT_470 verschlüsselt Daten für eine Karte. Die Verschlüsselung erfolgt zweistufig, d. h. die Daten werden symmetrisch mit einem generierten Schlüssel und anschließend dieser Schlüssel mit einem asymmetrischen Verfahren verschlüsselt. Der verschlüsselte Schlüssel (Encrypted Key) und die verschlüsselten Daten können gespeichert und später mit der entsprechenden Karte entschlüsselt werden. Das Format des erzeugten verschlüsselten Dokuments und der verschlüsselten symmetrischen Schlüssel werden nicht festgelegt.
Anwendungsumfeld	Zwischenspeichern von Daten im MobKT.
Initiierender Akteur	MobKT
Weitere Akteure	HPC (HBA oder SMC-B)
Auslöser	TUC_MOKT_010 writeToInternalStorage
Vorbedingungen	• hpc ist eine Karte vom Typ HBA oder SMC-B mit einer vom Mini-AK unterstützten Version.
Nachbedingungen	
Eingangsdaten	• hpc: berechtigte Karte mit dem Verschlüsselungszertifikat • data: zu verschlüsselnde Daten
Ausgangsdaten	• encryptedKey: verschlüsselter symmetrischer Schlüssel • encryptedData: verschlüsselte Daten
Weitere Informationsobjekte	• Asymmetrically encrypted symmetric key of hpc: pro berechtigter Karte existiert ein symmetrischer Schlüssel, der asymmetrisch verschlüsselt gespeichert wird. Ist ein solcher symmetrischer Schlüssel für eine berechtigte Karte bereits vorhanden, wird dieser vor dem Schreiben eines neuen Datensatzes mit dem asymmetrischen Schlüssel der berechtigten Karte entschlüsselt und bei der Verschlüsselung der Daten im Zwischenspeicher verwendet.

Standardablauf	1. Der Mini-AK MUSS das Zertifikat mit dem öffentlichen Schlüssel gemäß TUC_MOKT_202 mit a. card = hpc, b. file = /MF/DF.ESIGN/EF.C.HP.ENC.R2048 bzw. /MF/DF.ESIGN/EF.C.HCI.ENCR2048 c. chunkToRead = ganze Datei lesen. 2. Wenn TUC_MOKT_202 ohne Fehler endet, MUSS der Mini-AK den öffentlichen Schlüssel im Zertifikat darauf hin überprüfen, ob er einen zulässigen Verschlüsselungsalgorithmus mit zulässigen Parametern unterstützt. 3. Ist der Schlüssel für einen zulässigen Verschlüsselungsalgorithmus mit zulässigen Parametern anwendbar, MUSS der Mini-AK prüfen, ob bereits ein symmetrischer Schlüssel zur berechtigten Karte existiert. 4. a. Existiert ein symmetrischer Schlüssel, MUSS der Mini-AK den symmetrischen Schlüssel mit dem asymmetrischen öffentlichen Schlüssel der berechtigten Karte gemäß TUC_MOKT_471 decryptData mit a) card = hpc b) encryptedKey = asymmetrically encrypted symmetric key of hpc entschlüsseln. b. Existiert kein symmetrischer Schlüssel zur berechtigten Karte, MUSS der Mini-AK einen symmetrischen Schlüssel generieren. 5. Der Mini-AK MUSS den symmetrischen Schlüssel aus Schritt 4 asymmetrisch mit dem öffentlichen Schlüssel aus dem Zertifikat aus Schritt 1 verschlüsseln, wenn dieser in Schritt 4 neu generiert wurde. 6. Der Mini-AK MUSS mit dem symmetrischen Schlüssel aus Schritt 4 die Daten symmetrisch verschlüsseln. 7. Der Mini-AK MUSS nach beiden Verschlüsselungsoperationen in Schritt 5 und 6 den unverschlüsselten symmetrischen Schlüssel löschen und TUC_MOKT_470 mit OK beenden.
Varianten/Alternativen	• Wenn das Zertifikat für die Entschlüsselung bereits im Mini-AK vorliegt, KANN der Mini-AK Schritt 1 auslassen.

Fehlerfälle	• 1: Wenn TUC_MOKT_202 in Schritt 1 mit einem Fehler endet, MUSS der Mini-AK TUC_MOKT_470 mit diesem Fehler beenden. • 2: Wenn beim Auswerten des Zertifikats ein Fehler auftritt, MUSS der Mini-AK TUC_MOKT_470 mit dem Fehler 1012 beenden. • 2: Wenn der öffentliche Schlüssel oder seine Parameter nicht für einen zulässigen Verschlüsselungsalgorithmus geeignet sind, MUSS der Mini-AK TUC_MOKT_470 mit Fehler 1070 beenden.	
Technische Fehlermeldungen	**Fehler Code**	**Bedeutung**
	1012	Korruptes Datenformat auf der Karte
	1070	Kryptographischer Algorithmus nicht unterstützt
	Siehe auch aufgerufene TUCs: TUC_MOKT_202 readFile	
Weitere Anforderungen	• Der Mini-AK MUSS bei der Erzeugung des symmetrischen Schlüssels in Schritt 3 die Anforderungen aus [gemSpec_Krypt] berücksichtigen • Der Mini-AK MUSS für die Erzeugung des symmetrischen Schlüssels in Schritt 3 und die symmetrische Verschlüsselung in Schritt 5 die Anforderungen an die Algorithmen aus [gemSpec_Krypt] umsetzen. • Der Mini-AK MUSS für die asymmetrische Verschlüsselung in Schritt 5 die Anforderungen an die Algorithmen aus [gemSpec_Krypt] umsetzen.	
Anmerkungen, Bemerkungen	keine	
Offene Punkte		
Referenzen	Pic_MOKT_018 Aktivitätsdiagramm zu TUC_MOKT_470 encryptData	

10.1.18 TUC_MOKT_471 decryptData

TIP1-A_3784 - Mobiles KT: "TUC_MOKT_471 decryptData"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_471 decryptData" gemäß Tab_MOKT_119 umsetzen.
[<=]

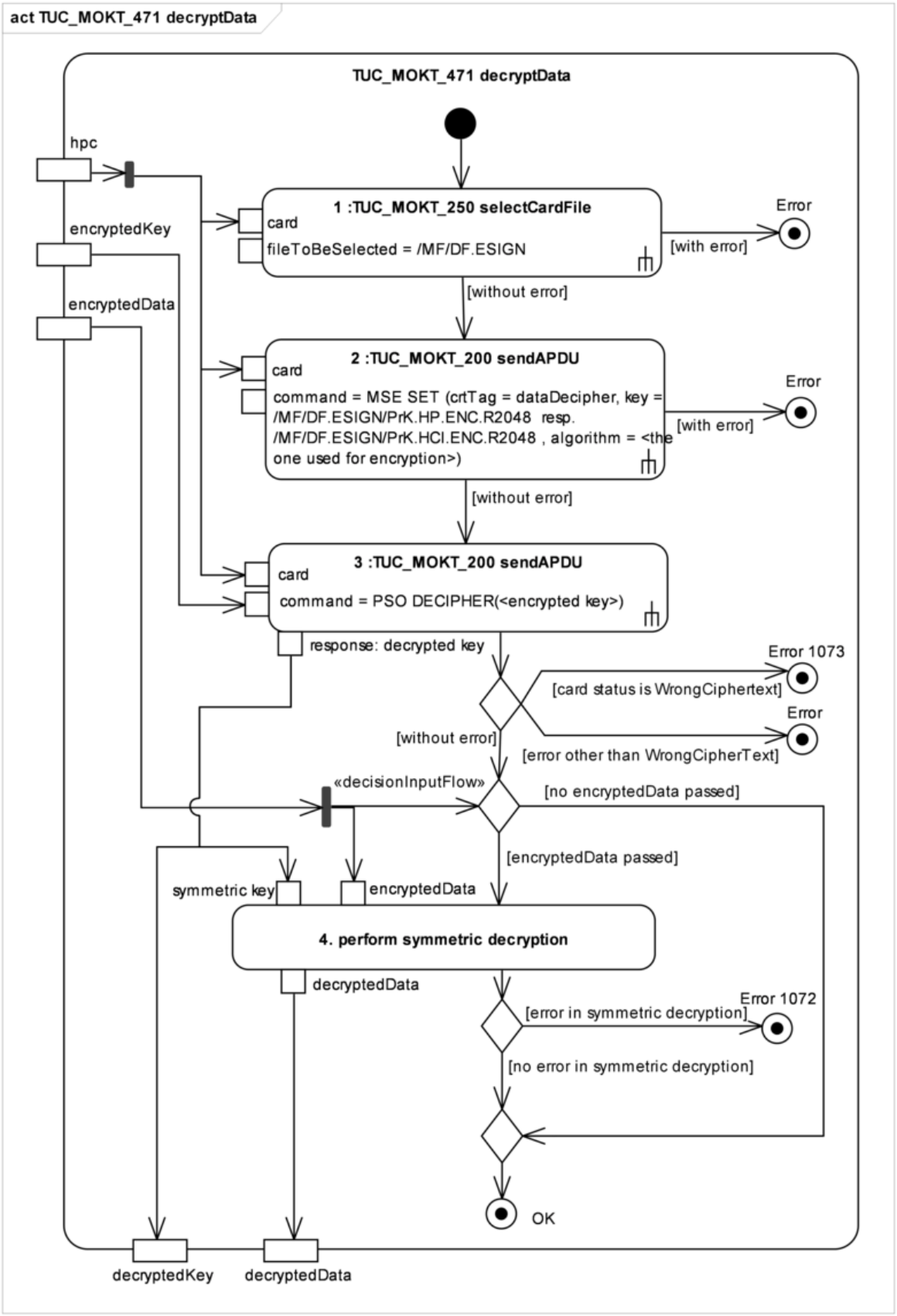


Abbildung 22: Pic_MOKT_019 Aktivitätsdiagramm zu TUC_MOKT_471 decryptData

Tabelle 32: Tab_MOKT_119 - TUC_MOKT_471 decryptData

TUC_MOKT_471 decryptData	
Beschreibung	TUC_MOKT_471 entschlüsselt für einen HBA oder eine SMC-B hybrid verschlüsselte Daten. Das Format des verschlüsselten Dokuments und der verschlüsselten symmetrischen Schlüssel werden in dieser Spezifikation nicht festgelegt.
Anwendungsumfeld	Auslesen von im MobKT zwischengespeicherten Daten
Initiierender Akteur	MobKT
Weitere Akteure	HPC (HBA oder SMC-B)
Auslöser	TUC_MOKT_011 readFromInternalStorage
Vorbedingungen	• hpc ist eine Karte vom Typ HBA oder SMC-B mit einer vom Mini-AK unterstützten Version. • data: symmetrisch verschlüsselte Daten • encryptedKey: mit asymmetrischen Schlüssel von hpc verschlüsselter symmetrischer Schlüssel.
Nachbedingungen	
Eingangsdaten	• encryptedData: zu entschlüsselnde Daten (optional) • hpc: Karte zur Entschlüsselung (HBA oder SMC-B) • encryptedKey: für die Karte asymmetrisch verschlüsselter symmetrischer Schlüssel.
Ausgangsdaten	• decryptedData: entschlüsselte Daten (optional) • decryptedKey: entschlüsselter symmetrischer Schlüssel (optional)
Weitere Informationsobjekte	keine

Standardablauf	1. Der Mini-AK MUSS den Dedicated File, dem der private Schlüssel zugeordnet ist, gemäß TUC_MOKT_250 mit a. card = hpc, b. fileToBeSelected = /MF/DF.ESIGN selektieren. 2. Endet der vorherige Schritt ohne Fehler, MUSS der Mini-AK den privaten Schlüssel und Algorithmus für die Datenentschlüsselung auf der Karte gemäß TUC_MOKT_200 mit a. card = hpc, b. command = MSE SET mit crtTag = dataDecipher, keyReference = /MF/DF.ESIGN/PrK.HP.ENC.R2048 bzw. /MF/DF.ESIGN/PrK.HCI.ENC.R2048 und algorithm entsprechend dem bei der Verschlüsselung eingesetzten Verfahren selektieren. 3. Endet der vorherige Schritt ohne Fehler, MUSS der Mini-AK den verschlüsselten symmetrischen Schlüssel mit der Karte gemäß TUC_MOKT_200 mit a. card = hpc, b. command = PSO DECIPHER entschlüsseln 4. Endet der vorherige Schritt ohne Fehler und wurden verschlüsselte Daten in encryptedData übergeben, MUSS der Mini-AK mit dem symmetrischen Schlüssel encryptedData entschlüsseln. Wurden keine verschlüsselten Daten in encryptedData übergeben, MUSS der Mini-AK den entschlüsselten symmetrischen Schlüssel als Ausgangsdatum zurück geben. Gelingt die Entschlüsselung ohne Fehler oder wurden keine verschlüsselten Daten in encryptedData übergeben, MUSS der Mini-AK TUC_MOKT_471 mit OK beenden.
Varianten/Alternativen	• Ist der Schlüssel auf der Karte bereits selektiert, so KANN der Mini-AK die Schritte 1 und 2 auslassen.

<table>
<tr><td>Fehlerfälle</td><td colspan="2">1: Wenn TUC_MOKT_250 in Schritt 1 mit einem Fehler endet, MUSS der Mini-AK TUC_MOKT_471 mit diesem Fehler beenden.
2: Wenn TUC_MOKT_200 in Schritt 2 mit einem Fehler endet, MUSS der Mini-AK TUC_MOKT_471 mit diesem Fehler beenden.
3: Wenn Schritt 3 mit einem Fehler außer Kartenstatus WrongCipherText endet, MUSS der Mini-AK TUC_MOKT_471 mit diesem Fehler beenden.
3: Wenn Schritt 3 mit dem Kartenstatus WrongCipherText endet, MUSS der Mini-AK TUC_MOKT_471 mit Fehler 1073 beenden.
4: Wenn die symmetrische Entschlüsselung in Schritt 4 fehlschlägt, MUSS der Mini-AK TUC_MOKT_471mit Fehler 1072 beenden</td></tr>
<tr><td rowspan="4">Technische Fehlermeldungen</td><td>Fehler Code</td><td>Bedeutung</td></tr>
<tr><td>1072</td><td>Korruptes Chiffrat bei symmetrischer Entschlüsselung</td></tr>
<tr><td>1073</td><td>Korruptes Chiffrat bei asymmetrischer Entschlüsselung</td></tr>
<tr><td colspan="2">Siehe auch aufgerufene TUCs:
TUC_MOKT_200 sendAPDU
TUC_MOKT_250 selectCardFile</td></tr>
<tr><td>Weitere Anforderungen</td><td colspan="2">keine</td></tr>
<tr><td>Anmerkungen, Bemerkungen</td><td colspan="2">Die Modellierung dieses TUCs geht davon aus, dass der Aufrufende eine korrekte Zuordnung von verschlüsselten Daten zur Karte vorgenommen hat, und beschreibt daher diesbezüglich keine Prüfungen und keine Fehlernummern.
Die Modellierung dieses TUCs geht davon aus, dass die Karte zum Entschlüsseln bereits freigeschaltet ist, und führt daher nicht implizit eine PIN-Verifikation durch.</td></tr>
<tr><td>Offene Punkte</td><td colspan="2"></td></tr>
<tr><td>Referenzen</td><td colspan="2">Pic_MOKT_019 Aktivitätsdiagramm zu TUC_MOKT_471 decryptData</td></tr>
</table>

10.2 Technische Use Cases des Mini-PS

10.2.1 TUC_MOKT_010 writeToInternalStorage

TIP1-A_3795 - Mobiles KT: "TUC_MOKT_010 writeToInternalStorage"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_010 writeToInternalStorage" gemäß Tab_MOKT_200 umsetzen.
[<=]

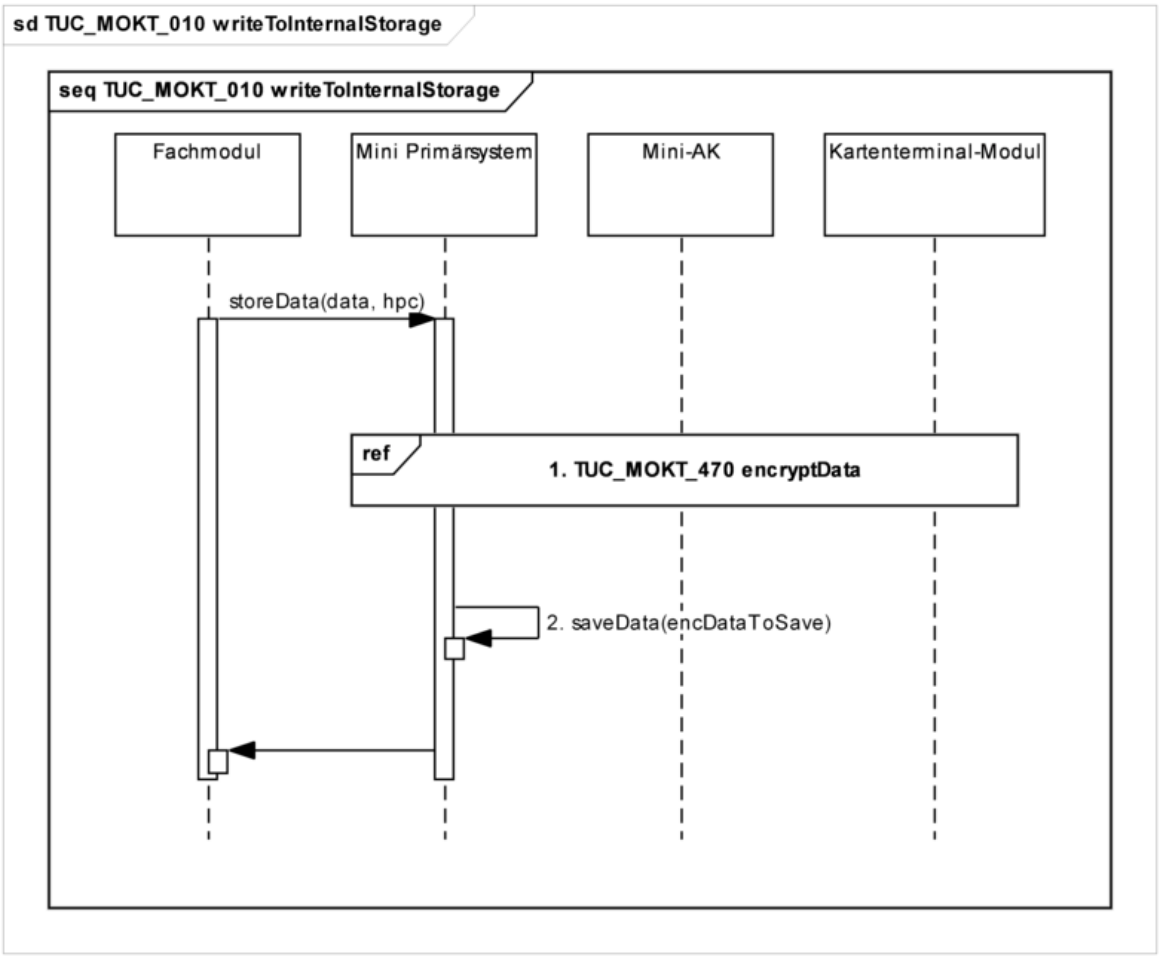


Abbildung 23: Pic_MOKT_021 Sequenzdiagramm zu TUC_MOKT_010 writeToInternalStorage

Tabelle 33: Tab_MOKT_200 Beschreibung zum Technischen Use Case TUC_MOKT_010 writeToInternalStorage

TUC_MOKT_010 writeToInternalStorage (alias TUC_MOKT_010 writeToInternalStore)	
Beschreibung	TUC_MOKT_010 speichert Daten persistent im Zwischenspeicher des Mini-PS. Die Daten werden verschlüsselt zwischengespeichert, wobei zur Verschlüsselung der öffentliche Schlüssel des Zertifikats einer berechtigten Karte (HBA oder SMC_B) verwendet wird. Es existiert nur ein symmetrischer Schlüssel pro berechtigter Karte. Ist ein solcher symmetrischer Schlüssel für eine berechtigte Karte bereits vorhanden, wird dieser vor dem Schreiben eines neuen Datensatzes mit dem asymmetrischen Schlüssel der berechtigten Karte entschlüsselt und bei der Verschlüsselung der Daten im Zwischenspeicher verwendet (siehe TUC_MOKT_470).
Anwendungsumfeld	Der Use Case wird ausgeführt, wenn der Benutzer Daten persistent abspeichern möchte, um sie zu einem späteren Zeitpunkt an sein Primärsystem zu übertragen.
Initiierender Akteur	MobKT
Weitere Akteure	HBA bzw. SMC-B
Auslöser	Fachmodul
Vorbedingungen	• hpc ist eine Karte vom Typ HBA oder SMC-B
Nachbedingungen	• Die verschlüsselten Daten sind persistent im dafür vorgesehenen Zwischenspeicher des Mini-PS zwischengespeichert.
Eingangsdaten	• data: zu speichernde Daten • hpc: Karte, für deren Identität die Daten verschlüsselt werden sollen
Ausgangsdaten	keine
Weitere Informationsobjekte	

Standardablauf	1. Das Mini-PS MUSS die Fach-Daten gemäß TUC_MOKT_470 mit a. hpc = hpc b. data = Daten verschlüsseln 2. Endet Schritt 1 ohne Fehler, MUSS das Mini-PS den verschlüsselten Datensatz mit encryptedKey und die Protokolldaten im dafür vorgesehenen persistenten Zwischenspeicher speichern.
Varianten/ Alternativen	
Fehlerfälle	• 1: Endet TUC_MOKT_470 in Schritt 1 mit einem Fehler, MUSS das Mini-PS TUC_MOKT_010 mit diesem Fehler beenden. • 2: Ist kein ausreichender Platz für die zwischenzuspeichernden Daten im Zwischenspeicher des Mobilen Kartenterminals verfügbar, bricht der Use Case in Schritt 2 ab. Können die Daten nicht zwischengespeichert werden, DARF das Mini-PS eventuell vorhandene Daten NICHT löschen.
Technische Fehlermeldung	Siehe TUC_MOKT_470 encryptData
Weitere Anforderungen	keine
Anmerkungen, Bemerkungen	keine
Offene Punkte	
Referenzen	Pic_MOKT_021 Sequenzdiagramm zu TUC_MOKT_010 writeToInternalStorage

10.2.2 TUC_MOKT_011 readFromInternalStorage

TIP1-A_3796 - Mobiles KT: "TUC_MOKT_011 readFromInternalStorage"
Das Mobile Kartenterminal MUSS den technischen Use Case "TUC_MOKT_011 readFromInternalStorage" gemäß Tab_MOKT_201 umsetzen.
[<=]

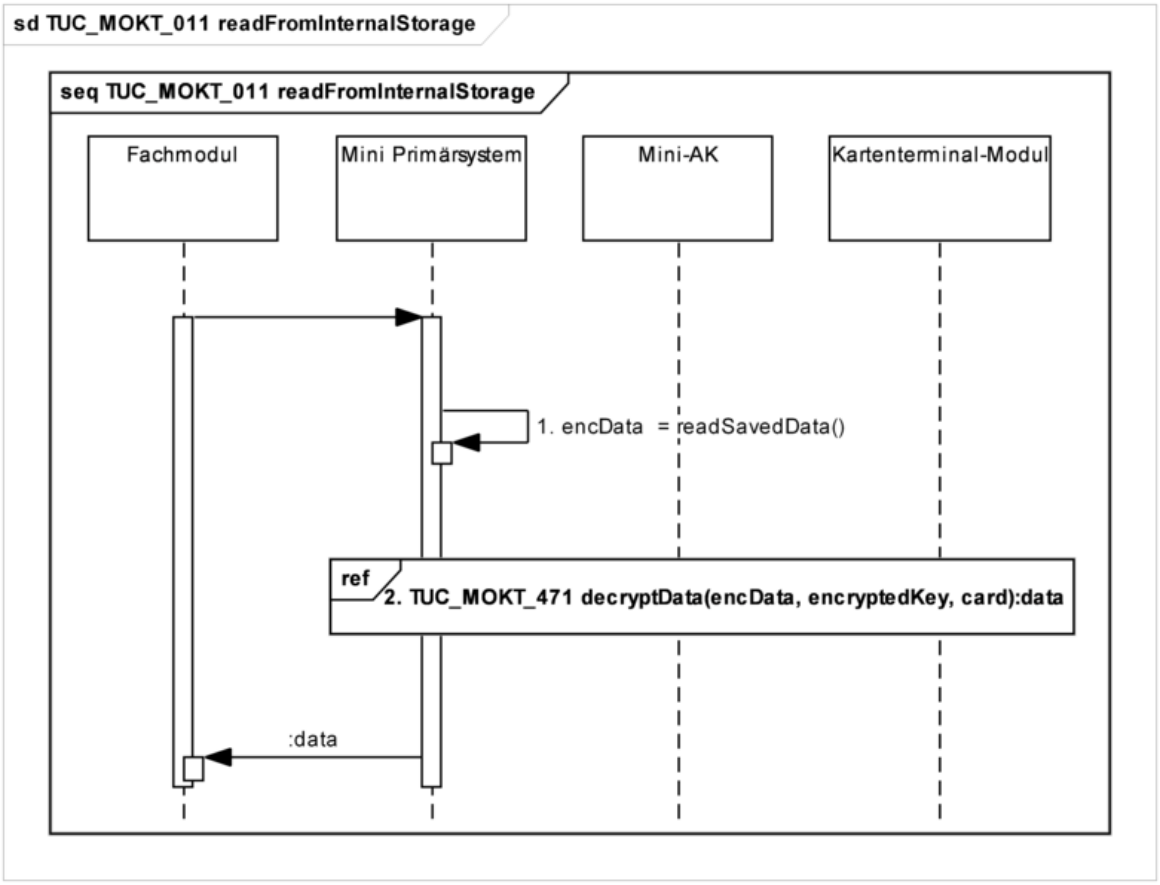


Abbildung 24: Pic_MOKT_022 Sequenzdiagramm zu TUC_MOKT_011 readFromInternalStorage

Tabelle 34: Tab_MOKT_201 Beschreibung zum Technischen Use Case TUC_MOKT_011 readFromInternalStorage

TUC_MOKT_011 readFromInternalStorage (alias TUC_MOKT_011 readFromInternalStore)	
Beschreibung	TUC_MOKT_011 liest zwischengespeicherte VSD. Da die Daten verschlüsselt zwischengespeichert sind, werden sie zur Nutzbarmachung durch den Entschlüsselungsdienst des Mini-AKs entschlüsselt. Es werden nur die VSD, jedoch nicht die Protokolldaten entschlüsselt, da diese nicht verschlüsselt vorliegen.
Anwendungsumfeld	Der Use Case wird ausgeführt, wenn der Benutzer persistent abgespeicherte Daten lesen möchte, z. B. um sie anzuzeigen oder an sein PS zu übertragen.
Initiierender Akteur	MobKT
Weitere Akteure	HBA bzw. SMC-B

Auslöser	Fachliche Anwendungsfälle: Anzeigen zwischengespeicherter VSD Übertragen zwischengespeicherter VSD Anzeigen zwischengespeicherter ungeschützter VSD Übertragen zwischengespeicherter ungeschützter VSD
Vorbedingungen	• hpc ist eine Karte vom Typ HBA oder SMC-B
Nachbedingungen	
Eingangsdaten	• data: Referenz auf die Daten im Zwischenspeicher • hpc: Karte, für die die zwischengespeicherten Daten verschlüsselt sind
Ausgangsdaten	• Daten in entschlüsselter Form
Weitere Informationsobjekte	
Standardablauf	1. Das Mini-PS MUSS die verschlüsselten Daten aus dem Zwischenspeicher lesen. 2. Das Mini-PS MUSS die Daten gemäß TUC_MOKT_471 mit a. hpc = hpc b. encryptedData = gelesene verschlüsselte Daten (VSD) c. encryptedKey = aus den Verwaltungsdaten des Zwischenspeichers entschlüsseln. Wenn TUC_MOKT_471 ohne Fehler endet, MUSS das Mini-PS TUC_MOKT_011 mit OK beenden.
Varianten/Alternativen	
Fehlerfälle	• Wenn TUC_MOKT_471 mit einem Fehler endet, MUSS das Mini-PS TUC_MOKT_011 mit diesem Fehler beenden.
Technische Fehlermeldung	Siehe TUC_MOKT_471 decryptData
Weitere Anforderungen	keine

Anmerkungen, Bemerkungen	Der TUC ist so modelliert, dass davon ausgegangen wird, dass die Daten für die übergebene Karte verschlüsselt sind. Der TUC ist so modelliert, dass die Karte zum Entschlüsseln bereits freigeschaltet ist, d. h. es wir nicht implizit eine PIN-Verifikation durchgeführt.
Offene Punkte	
Referenzen	Pic_MOKT_022 Sequenzdiagramm zu TUC_MOKT_011 readFromInternalStorage

11 Beschreibung der Host-Schnittstelle zur Übertragung zwischen Mobilem Kartenterminal und Primärsystem

Das Mini-PS stellt sich dem Primärsystem während der Übertragung als Kartenterminal dar und emuliert die zwischengespeicherten Datensätze inklusive Protokolldaten als Chipkarten. Hierfür muss das Mobile Kartenterminal für die Übertragung der Daten vom Mobilen Kartenterminal zum Primärsystem die in diesem Kapitel spezifizierten Übertragungsmechanismen nutzen.

TIP1-A_4410 - Mobiles Kartenterminal: Software zur Anbindung
Der Hersteller des Mobilen Kartenterminals MUSS eine Software zur Anbindung des Mini-PS an das Primärsystem gemäß [TIP1-A_3691] zur Verfügung stellen.
[<=]

TIP1-A_4942 - Kommandoaufbau Host-Schnittstelle
Das Mobile Kartenterminal MUSS folgende allgemeine Vorgaben umsetzen:

1. Der generelle Aufbau eines Kommandos entspricht [ISO 7816-4].
2. Die Struktur der 'CardTerminal Control Commands' ist identisch mit der Struktur der 'Interindustry Commands'. Das CLA-Byte (Class-Byte) ist daher entsprechend [ISO 7816-4] codiert:
   a. '20' = Command message structure according to [ISO 7816-4]
3. Das Protokoll basiert auf Kommandos, die zum 'Interindustry Command Set' gehören (siehe [ISO 7816-4]). Das CLA-Byte hat daher bei diesen Kommandos folgende Codierung:
   a. '00' = Command message structure and coding according to [ISO 7816-4].
4. Bei den Kommandos sind nur die speziellen Return-Codes angegeben. Darüber hinaus können noch folgende allgemeine Return-Codes auftreten:
   a. '6700' = Wrong length
   b. '6900' = Command not allowed (at this stage)
   c. '6A00' = Wrong Parameters P1, P2
   d. '6D00' = Wrong instruction

[<=]

TIP1-A_4934 - Mobiles KT: CT-API Versionierung
Der Hersteller des Mobilen Kartenterminals MUSS die zur Anbindung des Mini-PS an einen Host notwendigen Software mit einer eindeutigen Versionsnummer versehen.
[<=]

TIP1-A_4935 - Mobiles KT: CT-API Abfrage Versionsnummer
Der Hersteller des Mobilen Kartenterminals MUSS die in [TIP1-A_4934] geforderte Versionierung so umsetzen, dass die Versionsnummer mit Standardmitteln des jeweiligen Betriebssystems abgefragt werden kann.
[<=]

TIP1-A_6706 - Mobiles KT: Versionen der Betriebssysteme für CT-API
Der Hersteller des Mobilen Kartenterminals MUSS die Angaben zu Versionen der Betriebssysteme veröffentlichen, für die er eine Software zur Anbindung des Mini-PS an das Primärsystem gemäß [TIP1-A_4410] zur Verfügung stellt. Werden zukünftige

Versionen bestimmter Betriebssysteme nicht mehr unterstützt, so MUSS er die Information zu diesen Betriebssystemen und der letzten unterstützten Version veröffentlichen.
[<=]

11.1 Kommandobeschreibung

Dieser Abschnitt beschreibt die Kommandos zur Steuerung des Kartenterminals. Die Kommandos werden nur mit den Funktionen und Codierungen beschrieben, die für den Anwendungsfall relevant sind.

Bei den Kommandos sind nur die speziellen Return-Codes angegeben.

TIP1-A_4943 - Ergänzung allgemeiner Fehlercode
Das Mobile Kartenterminal MUSS ergänzend zu [TIP1-A_4942] den allgemeinen Return-Code „‚6E00' = Class not supported" zurücksenden, wenn das CLA Byte als Codierung weder '20' noch '00' enthält.
[<=]

11.1.1 RESET CT

Dieses Kommando emuliert ein Kartenterminal-Reset. Aus der Antwort SW = ‚9501' kann das Primärsystem erkennen das es mit einem Mini-PS kommuniziert.

TIP1-A_4417 - Mobiles KT: Reset CT
Das Mini-PS des mobilen Kartenterminal MUSS das Kommando RESET CT gemäß "Tab_mobKT_005 - Command RESET CT" und "Tab_mobKT_006 - Response RESET CT" für die Host-Schnittstelle umsetzen.
[<=]

Tabelle 35: Tab_mobKT_005 - Command RESET CT

Command				
CLA	INS	P1	P2	Le
20	11	00	00	00

Tabelle 36: Tab_mobKT_006 - Response RESET CT

Response		**Bedeutung**
SW1	SW2	-
95	01	Reset successful (Version of mobCT belongs to Online Rollout)
64	00	Reset not successful
6A	00	Wrong parameters P1, P2

67	00	Wrong length Le

11.1.2 REQUEST ICC

Dieses Kommando emuliert die Aufforderung zum Einlegen der Chipkarte. Im hier betrachteten Kontext wird damit abgefragt ob zwischengespeicherte Daten vorliegen. Für den Timer Parameter T ist als Default-Wert ‚01' (= 1 Sekunde) zu setzen.

Sind im mobilen Kartenterminal Daten zwischengespeichert, es wurde jedoch keine berechtigte Karte gesteckt oder diese nicht freigeschaltet, hängt es von der Speicherorganisation des mobilen Kartenterminals ab, ob das mobile Kartenterminal erkennen kann, dass zwischengespeicherte Daten vorliegen.

TIP1-A_4418 - Mobiles KT: Request ICC
Das Mini-PS des mobilen Kartenterminals MUSS das Kommando REQUEST ICC gemäß "Tab_mobKT_007 - Command REQUEST ICC" und "Tab_mobKT_008 - Response REQUEST ICC" für die Host-Schnittstelle umsetzen.
[<=]

TIP1-A_4944 - Mobiles KT: Timer Request ICC
Das Mobile Kartenterminal MUSS im Fall, dass das Kommando Request ICC gemäß [TIP1-A_4418] ohne Lc und ohne Daten gesendet wird, den Timer auf 1 Sekunde setzen.
[<=]

Tabelle 37: Tab_mobKT_007 - Command REQUEST ICC

Command					
CLA	INS	P1	P2	Lc	Data
20	12	01	00	01	01
20	12	01	00	-	-

Tabelle 38: Tab_mobKT_008 - Response REQUEST ICC

Response		**Bedeutung**
SW1	SW2	-
90	00	The stored data is of type KVK
90	01	The stored data is of type eGK
62	00	No buffered VSD available for transmission.
64	00	Reset not successful or Error in Data (Data <> 01)
6A	00	Wrong parameters P1, P2

67	00	Wrong length Lc or Le

11.1.3 EJECT ICC

Dieses Kommando emuliert einen Kartenauswurf. Für den Timer T ist als Default-Wert ‚01' (= 1 Sekunde) zu setzen.

TIP1-A_4419 - Mobiles KT: Eject ICC
Das Mini-PS des mobilen Kartenterminal MUSS das Kommando EJECT ICC gemäß "Tab_mobKT_009 - Command EJECT ICC" und "Tab_mobKT_010 - Response EJECT ICC" für die Host-Schnittstelle umsetzen.
[<=]

TIP1-A_4945 - Mobiles KT: Timer Eject ICC
Das Mobile Kartenterminal MUSS im Fall, dass das Kommando Eject ICC gemäß [TIP1-A_4419] ohne Lc und ohne Daten gesendet wird, den Timer auf 1 Sekunde setzen.
[<=]

Tabelle 39: Tab_mobKT_009 - Command EJECT ICC

Command					
CLA	INS	P1	P2	Lc	Data
20	15	01	00	01	01
20	15	01	00	-	-

Tabelle 40: Tab_mobKT_010 - Response EJECT ICC

Response		**Bedeutung**
SW1	SW2	-
90	00	command successful
67	00	Wrong length Lc (e.g. Data present but Data <> 01 or Lc present but Lc <> 01)
6A	00	Wrong parameters P1, P2

11.1.4 SELECT FILE

Das Kommando SELECT FILE emuliert die Selektion einer Anwendung auf der Karte und dient im hier betrachteten Kontext dazu, die Art der zwischengespeicherten Daten auszuwählen: Entweder Daten der KVK oder Daten der eGK.

Im Fall der KVK ist der aid auf der Chipkarte entweder ‚D27600000101' oder ‚D28000000101'. Im Fall der eGK ist der aid ‚D27600000102'

TIP1-A_4420 - Mobiles KT: SELECT FILE
Das Mini-PS des mobilen Kartenterminal MUSS das Kommando SELECT FILE gemäß "Tab_mobKT_011 - Command SELECT FILE" und "Tab_mobKT_012 - Response SELECT FILE" für die Host-Schnittstelle umsetzen.
[<=]

TIP1-A_5008 - Mobiles KT: Ausschluss Prüfung auf Freischaltung bei SELECT FILE
Das Mini-PS des Mobilen Kartenterminals DARF beim Kommando SELECT FILE NICHT mit der Response ‚69 00' antworten, wenn der Benutzer den nach [TIP1-A_4270] geforderten Authentifizierungsstatus nicht erreicht hat.
[<=]

Tabelle 41: Tab_mobKT_011 - Command SELECT FILE

Command					
CLA	INS	P1	P2	Lc	Data
00	A4	04	00	06	KVK AID = ‚D2 76 00 00 01 01' oder ‚D2 80 00 00 01 01'.
00	A4	04	0C	06	eGK AID = ‚D2 76 00 00 01 02'

Tabelle 42: Tab_mobKT_012 - Response SELECT FILE

Response		**Bedeutung**
SW1	SW2	-
6A	82	File not Found (e.g. wrong AID)
90	00	Command successful
69	00	Command not allowed at this stage
6A	00	Wrong parameters P1, P2
67	00	Wrong length Lc or Le

Liegen gespeicherte Daten des gewünschten Formats nicht vor, so wird der Fehlercode ‚6A82' zurückgegeben. In diesem Fall liefert ein nachfolgendes READ BINARY ebenfalls einen Fehlercode zurück.

11.1.5 READ BINARY

Das Kommando READ BINARY dient der Übertragung eines gespeicherten Datensatzes. Die Indizierung eines bestimmten Datensatzes ist nicht möglich, d. h. es kann nur jeweils der aktuellste, noch nicht gelöschte Datensatz gelesen werden. Das Lesen des nächsten Datensatzes ist erst nach Löschen (siehe EREASE BINARY) des zuletzt gelesenen Datensatzes möglich.

TIP1-A_4950 - Mobiles KT: READ BINARY
Das Mini-PS des mobilen Kartenterminals MUSS das Kommando READ BINARY gemäß "Tab_mobKT_013 - Command READ BINARY KVK", "Tab_mobKT_014 - Response READ BINARY KVK", "Tab_mobKT_015 - Command READ BINARY eGK" und "Tab_mobKT_016 - Response READ BINARY eGK" für die Host-Schnittstelle umsetzen.

[<=]

11.1.5.1 READ BINARY KVK

Das Kommando dient im Fall der KVK zum Lesen des VersichertenDatenTemplates und der Zusatzfelder (EinleseDatum, ZulassungsNummer und PrüfSummeZusatz). Sobald das Kartenterminal mit der Übertragung der Versichertendaten und der Zusatzfelder beginnt, markiert es die Daten als übertragen. Das Kartenterminal stellt sicher, dass der zuletzt übertragene Datensatz mittels ERASE BINARY durch das Primärsystem gelöscht wurde, bevor es die Übertragung des nächsten zwischengespeicherten Datensatzes zulässt.

Eine vollständige und korrekte Übertragung muss das Host-System nach dem Lesen durch das Kommando ERASE BINARY anzeigen.

Als Offset sollte im READ BINARY-Kommando ‚0000' angeben werden, d. h. es soll ab logischer Adresse ‚0000' (= Anfangsadresse der Anwendungsdaten) gelesen werden. Es soll der komplette zur Anwendung gehörende Datenbereich gelesen werden. Im Fall der KVK ist dies das gesamte VD-Template, beginnend mit Tag ‚60' und endend mit dem XOR-Prüfbyte des ASN.1-Elements ‚Prüfsumme' und die zusätzlichen Datenobjekte. Die Länge der gesamten Daten und damit das logische Ende (EOF) des zur Anwendung gehörenden Datenbereichs, ergibt sich aus der Länge des VD-Templates (Längenbyte nach Tag ‚60') und der Länge der zusätzlichen Datenfelder (+ 47 Bytes). Im Falle der eGK ist es jeweils der gesamte, zuvor mittels SELECT FILE selektierte Datenblock, wobei die Statusblöcke (siehe Kapitel 11.3) jeweils um die zusätzlichen Datenobjekte erweitert werden. Die Daten und die Zusatzfelder werden in einem Block übertragen und mit den Status-Bytes ‚9000' abgeschlossen. Das Kommando kann auch mit variablem Offset angegeben (MMMM) in P1 und P2, wobei die Daten in diesem Fall ab dem angebenden Offset gelesen werden. Das Kommando kann auch mit Le > 0 ausgeführt werden, wobei der Wert in Le in diesem Fall die Anzahl der zu lesenden Bytes (N) angibt und in diesem Fall werden, sofern im gelesenen File vorhanden, Le Bytes zurückgeliefert.

Entspricht die Struktur der Daten nicht den Vorgaben, werden nur die Status-Bytes mit der Codierung ‚6501' (= Memory failure or data corrupted) zurückgegeben. Tritt ein Übertragungsfehler auf, sodass die Daten während der Übertragung geändert wurden wird das Status-Byte ‚6F00' zurückgegeben. Nur bei der Angabe von Le > 0 kann im Response der Status-Code ‚6282' auftreten, wenn die Länge der zurück gelieferten Daten kleiner als Le ist. Bei Le = ‚00' (WildcardShort) wird unabhängig von der Länge der zurückgegebenen Daten der Status ‚9000' im Response verwendet. Zur Behandlung von WildcardShort siehe auch [gemSpec_COS#(N052.300)] und [gemSpec_COS-#(N067.000)].

Tabelle 43: Tab_mobKT_013 - Command READ BINARY KVK

Command				
CLA	INS	P1	P2	Le
00	B0	00	00	00 /(/ bedeutet „oder“) 00 00 00
00	B0	MM	MM	N

Tabelle 44: Tab_mobKT_014 - Response READ BINARY KVK

Response			**Bedeutung**
Daten	SW1	SW2	
KVK-Daten	90	00	Command Successful
-	65	01	Memory Failure or data corrupt
-	6B	00	Wrong offset
-	69	00	Command not allowed: memory access denied
-	6F	00	Error during communication (i. e. checksum error)
-	62	82	Warning, end of file reached before reading Le bytes
-	67	00	Wrong length Le

Die KVK Daten werden je nach Benutzereinstellung im ASN.1 oder im Festformat gesendet.

11.1.5.2 READ BINARY eGK

Das Kommando READ BINARY wird wie folgt ergänzt, um die zwischengespeicherten Daten einer eGK zu lesen. Der Parameter P1 dient der Indizierung des zu liefernden Teils des gespeicherten Datensatzes.

Tabelle 45: Tab_mobKT_015 - Command READ BINARY eGK

Command				
CLA	INS	P1	P2	Le

00	B0	8C	00	00 /(/ bedeutet „oder“) 00 00 00
00	B0	81	00	00 00 00
00	B0	82	00	00 00 00
00	B0	83	00	00 00 00

Der Parameter P1 hat folgende Bedeutung:

- 8C = Protokolldaten der VSD (siehe Tabelle „Tab_MOKT_005 Erweiterung der Datentypen READ BINARY VSD eGK“)
- 81 = Persönliche Versichertendaten
- 82 = Allgemeine Versichertendaten
- 83 = Geschützte Versichertenstammdaten

Tabelle 46: Tab_mobKT_016 - Response READ BINARY eGK

Response			**Bedeutung**
Daten	SW1	SW2	
eGK-Daten gemäß Wert in P1	90	00	-
-	65	01	Memory Failure or data corrupt
-	6B	00	Wrong offset
-	69	00	Command not allowed: memory access denied
-	6F	00	Error during communication (i. e. checksum error)
-	62	82	Warning, end of file reached before reading Le bytes
-	67	00	Wrong length Le
-	6A	00	Wrong parameters P1, P2
-	6A	82	File not found (e.g. no GVD stored)

Die Statusdaten werden mit den Verwaltungsdaten (Erfassungszeitpunkt und Zulassungsnummer) wie im KVK-Fall ergänzt siehe 11.3.

Die Daten werden im vorliegenden Format (gezippte XML-Datei) an das Primärsystem übertragen. Eine Prüfung der Daten findet nicht statt.

11.1.6 ERASE BINARY

Das Kommando dient zum Löschen des letzten (ummittelbar zuvor) übertragenen Datensatzes inklusive der zusätzlichen Datenobjekte im portablen Lesegerät durch das Primärsystem.

Es wird immer der komplette Datensatz gelöscht, auch wenn im Fall der eGK-Daten eventuell noch nicht alle zum Lesen nötigen READ BINARY Kommandos geschickt wurden.

TIP1-A_4421 - Mobiles KT: ERASE BINARY
Das Mini-PS des mobilen Kartenterminal MUSS das Kommando ERASE BINARY gemäß "Tab_mobKT_017 - Command ERASE BINARY" und "Tab_mobKT_018 - Response ERASE BINARY" für die Host-Schnittstelle umsetzen.
[<=]

Tabelle 47: Tab_mobKT_017 - Command ERASE BINARY

Command			
CLA	INS	P1	P2
00	0E	00	00

Tabelle 48: Tab_mobKT_018 - Response ERASE BINARY

Response		**Bedeutung**
SW1	SW2	
90	00	command successful
69	86	No data selected for deletion (e.g. data set already deleted)
65	00	Erasure failed
6B	00	Wrong parameter / Wrong Offset
69	00	Command not allowed: memory access denied
67	00	Wrong length Falls das Kommando ERASE BINARY den Parameter Lc oder Le enthält

11.1.7 GET STATUS

Dieses Kommando dient zur Abfrage der Produktidentifikation.

TIP1-A_4422 - Mobiles KT: GET STATUS
Das Mini-PS des mobilen Kartenterminals MUSS das Kommando GET STATUS gemäß "Tab_mobKT_019 - Command GET STATUS", "Tab_mobKT_020 - Response GET STATUS", "Tab_mobKT_021 - CardTerminal Manufacturer Data Object Definition (CTM DO)" und "Tab_mobKT_022 - Discretionary Data Data Object Definition" für die Host-Schnittstelle umsetzen.

[<=]

Tabelle 49: Tab_mobKT_019 - Command GET STATUS

Command				
CLA	INS	P1	P2	Le
20	13	00	46	00

Tabelle 50: Tab_mobKT_020 - Response GET STATUS

Response			**Bedeutung**
Daten	SW1	SW2	
CTM DO	90	00	Command Successful

Tabelle 51: Tab_mobKT_021 – CardTerminal Manufacturer Data Object Definition (CTM DO)

CardTerminal Manufacturer Data Object (CTM DO)				
TAG	‘46’	One byte tag according ISO 7816-6: Application Label		
		Tag coding according ASN.1 BER see SICCT 5.5.10.3		
		BER-Coding : private, primitive, Tag-Number = 82 (‘52’)		
LEN	LEN coding see SICCT 5.5.10.3			
	71 <=LEN<=127			
VALUE	DO name		length	Description
	CTM	man	5	Cardterminal Manufacturer as issued by the gematik

	CTT	man	5	Cardterminal Type
	CTSV	man	5	Cardterminal Software Version
	Discretionary Data	man	56<=LEN<=112	Discretionary Data Data Object

Tabelle 52: Tab_mobKT_022 - Discretionary Data Data Object Definition

Discretionary Data Data Object (DD DO)				
TAG	'D7'	One byte tag according ISO 7816-6: Application Label		
		Tag coding according ASN.1 BER see SICCT 5.5.10.3		
		BER-Coding : private, primitive, Tag-Number = 23 ('17')		
LEN	LEN coding see SICCT 5.5.10.3			
	54 <=LEN<=110			
VALUE	DO name		length	Description
	VER	man	9	MOBCT-Interface version reflecting the conformance to specific versions of applicable gematik interface specifications.
	PT	man	5	Producttype
	PTV	man	9	Producttype Version
	MODN	man	8	Model Name of Cardterminal
	FWV	man	9	Firmware Version
	HWV	man	9	Hardware Version
	FWG	man	5	Version of Firmware Group
	VEN	opt	0..56	Vendor specific information

Tabelle 53: Tab_mobKT_023 - Discretionary Data Data Object Type Definition

Data	Len		Description
VER	9	man	The version of the interface 1.0.0 yields the ASCII encoded string: '202031202030202030' 9 Byte ASCII String of form [XXX][YYY][ZZZ] The values are defined as follows (see also [gemSpec_OM#2.1.2]) XXX Major Version number left-padded with space '20' YYY Minor version number left-padded with space '20' ZZZ Revision number left-padded with space '20'
PT	5	man	Producttype 'MOBKT' 5 Byte ASCII String with the following content: The name of the producttyp (MOBKT) yields the ASCII encoded string: '4D4F424B54'
PTV	9	man	Producttype Version 9 Byte ASCII String of form [XXX][YYY][ZZZ] XXX Major Version number left-padded with space '20' YYY Minor version number left-padded with space '20' ZZZ Revision number left-padded with space '20' Example: The producttype version 2.61.242 (2 Major, 61 Minor, 242 Revision) yields the ASCII encoded string: '202032203631323432'
MODN	8	man	8 Byte ASCII String- left-padded with Space ('20') Named as "Produktkürzel" in [gemSpec_OM] Vendor specific
FWV	9	man	Firmware Version 9 Byte ASCII String of form [XXX][YYY][ZZZ] XXX Major Version number left-padded with space '20' YYY Minor version number left-padded with space '20' ZZZ Revision number left-padded with space '20' Example: The firmware version 2.61.242 (2 Major, 61 Minor, 242 Revision) yields the ASCII encoded string: '202032203631323432'

HWV	9	man	Hardware Version 9 Byte ASCII String of form [XXX][YYY][ZZZ] XXX Major Version number left-padded with space '20' YYY Minor version number left-padded with space '20' ZZZ Revision number left-padded with space '20' Example: The hardware version 2.61.242 (2 Major, 61 Minor, 242 Revision) yields the ASCII encoded string: '202032203631323432'
FWG	5	man	Firmware Group Version 5 Byte ASCII String Format defined in [gemSpec_KSR]
VEN	0..56	opt.	Optional, vendor specific coded string.

11.2 Kommandosequenz des externen Primärsystems

Die im Folgenden beschriebenen Kommandozyklen (Schritt 0 bis Schritt 5 im Fall der KVK bzw. Schritt 0 bis Schritt 7 im Fall der eGK) können je nach Bedarf wiederholt werden. Das RESET CT-Kommando wird nur dann gegeben, wenn sich bei der Kommunikation mit dem Kartenterminal auf Anwendungsebene eine Situation eingestellt hat, die ein RESET CT-Kommando erfordert bzw. mit dem Kommando(s) READ BINARY ein Datensatz nicht fehlerfrei übertragen werden konnte.

11.2.1 Vorbereitung

Vor dem Start der Kommandosequenz muss ein RESET CT gesendet werden, um das Mobile Kartenterminal zu initialisieren. Optional kann nach einem RESET CT ein GET STATUS versendet werden, um die aktuelle Versionsnummer der Schnittstelle abzufragen. Die Versionsnummer der Schnittstelle ist dem Data Object VER im Discretionary Data Data Object des CardTerminal Manufacturer Data Object (CTM DO) zu entnehmen (siehe Kapitel 11.1.7).

Tabelle 54: Kommandosequenz Vorbereitung zum Lesen eines VSD Datensatzes

Schritt	Kommando	APDU	Bemerkung
0	RESET CT	20 11 00 00 00	Antwort 95 01 d. h. es handelt sich um ein Mobiles Kartenterminal
1	GET STATUS	20 13 00 46 00	Optionaler Schritt zur Abfrage der aktuellen Schnittstellenversion
2	REQUEST ICC	20 12 01 00 01 00	Chipkarte anfordern ohne Wartezeit

Anhand der Antwort auf das REQUEST ICC Kommando kann das Host-System entscheiden, ob eine KVK oder eine eGK vorliegt (SW1SW2=9000 entspricht KVK, SW1SW2=9001 entspricht eGK).

11.2.2 Lesen der KVK (bei REQUEST ICC: SW1SW2=9000)

Der weitere Ablauf für das Auslesen der KVK-Daten ist wie folgt:

Tabelle 55: Kommandosequenz zum Lesen eines VSD Datensatzes von KVK

Schritt	Kommando	APDU	Bemerkung
3	SELECT FILE (KVK)	00 a4 04 00 06 d2 76 00 00 01 01	KVK-Anwendung selektieren
4	READ BINARY	00 b0 00 00 00 oder 00 b0 00 00 00 00 00	Krankenversichertendaten und zugehörige Erfassungsdaten lesen
5	ERASE BINARY	00 0e 00 00	unmittelbar zuvor übertragenen Datensatz löschen
6	EJECT ICC	20 15 01 00 01 01	Beenden des Auslesevorganges (emulierter Kartenauswurf)

11.2.3 Lesen der VSD der eGK (bei REQUEST ICC: SW1SW2=9001)

Im Falle einer eGK muss die weitere Kommandosequenz für das Auslesen der VSD wie folgt implementiert werden.

Tabelle 56: Kommandosequenz zum Lesen eines VSD-Datensatzes von eGK

Schritt	Kommando	APDU	Bemerkung
3	SELECT FILE (HCA)	00 a4 04 0c 06 d2 76 00 00 01 02	eGK-Anwendung selektieren
4	READ BINARY EF.StatusVD	00 b0 8c 00 00 oder 00 b0 8c 00 00 00 00	Statusdaten, Erfassungsdatum und Zulassungsnummer lesen

5	READ BINARY EF.PD	00 b0 81 00 00 00 00	Personendaten lesen
6	READ BINARY EF.VD	00 b0 82 00 00 00 00	Allgemeine Versicherungsdaten lesen
7	READ BINARY EF.GVD	00 b0 83 00 00 00 00	Geschützte Versicherungsdaten lesen
8	ERASE BINARY	00 0e 00 00	unmittelbar zuvor übertragenen Datensatz (StatusVD, Personal Data, Insurance Data) löschen
9	EJECT ICC	20 15 01 00 01 01	Beenden des Auslesevorganges (emulierter Kartenauswurf)

Das Kommando READ BINARY wird mit erweiterter Längenangabe (extended Length) gesendet. Die Methode ein READ BINARY mehrfach mit fortschreitendem Offset zu senden, wird nicht unterstützt. Das Lesen des StatusVD kann auch mit einfacher Länge erfolgen, da die Antwort geeignet kurz ist.

11.3 Erweiterungen der Datentypen bei der Übertragung

Für die eGK handelt es sich bei den in Schritt 5 READ BINARY (Personal Data) und 6 READ BINARY (Insurance Data) gelesenen Daten um gezippte XML-Dateien wie sie in der eGK-Spezifikation [eGK] definiert sind.

VSDM-A_2881 - Felder hinzufügen
Das Fachmodul VSDM (mobKT) MUSS zur Übertragung der zwischengespeicherten Daten der eGK die Erweiterungen in Tabelle Tab_MOKT_005 anwenden.
[<=]

Tabelle 56: Tab_MOKT_005 Erweiterung der Datentypen READ BINARY VSD eGK

Pos.	Herkunft	Tag	Länge	Inhalt
1	eGK	A0	25	StatusVD, wie aus der eGK ausgelesen.
2	Term.	91	08	Einlesedatum im Format TTMMJJJJ (ASCII)
3	Term.	92	38	Zulassungsnummer (Produktidentifikation) des Mobilen Kartenterminals (ASCII) rechtsseitig mit Leerzeichen (‘20’) gepadded. Format wie beschrieben in [gemSpec_OM]: *Hersteller-ID;ProduktKürzel;Produktversion (=Firmwareversion: Hardwareversion)*

4	Term.	93	01	Prüfsumme XOR über die vollständigen Tags 91 und 92, sowie Tag 93 und dessen Länge „01“.

Das Einlesedatum ist das Datum, welches den Erfassungszeitpunkt des VSD-Datensatzes protokolliert. *TT* steht für den Tag *MM* steht für den Monat und *JJJJ* für das Jahr der Datensatzerfassung.

Als Zulassungsnummer wird die Produktidentifikation wie in [gemSpec_OM] beschrieben verwendet, wobei die einzelnen Einträge Semikolon-separiert sind.

Zur Berechnung der Prüfsumme wird das Datenobjekt des Tags 92, inkl. Tag und Längenangabe, an das Datenobjekt des Tags 91, inkl. Tag und Längenangabe, angehängt. Zudem werden Tag 93 und dessen Länge 01 ebenfalls angehängt und in die Berechung der Prüfsumme miteinbezogen. Anschließend werden die Bytes des zusammengesetzten Arrays byteweise XOR verknüpft. Zu Beginn wird das erste Byte mit dem zweiten Byte XOR verknüpft. Das Ergebnis dieser Operation wird mit dem nächsten (dem dritten) Byte XOR verknüpft und so weiter. Das Ergebnis der letzten Verknüpfung stellt die Prüfsumme dar.

12 Anhang A

12.1 Abkürzungen

Kürzel	Erläuterung
ASV	Ambulante spezialfachärztliche Versorgung
ATR	answer-to-reset
AVS	Apothekenverwaltungssystem
C2C	Card-to-Card
CS	Card Slot
CT-API	Card Terminal Application Programming Interface
eGK	elektronische Gesundheitskarte
GVD	geschützte Versichertenstammdaten
HBA	Heilberufsausweis
KBV	Kassenärztliche Bundesvereinigung
KIS	Krankenhausinformationssystem
KT	Kartenterminal
KVK	Krankenversichertenkarte
LED	Light Emitting Diode
Mini-AK	Mini-Anwendungskonnektor
Mini-PS	Mini-Primärystem
MKT	Multifunktionales Kartenterminal
MTBF	Mean Time Between Failures
OID	Object Identifier
PS	Primärsystem

PVS	Praxisverwaltungssystem
QES	Qualifizierte Elektronische Signatur
RFC	Request For Comments
SICCT	Secure Interoperable ChipCard Terminal
SigG	Signaturgesetz
SigV	Signaturverordnung
SMC	Security Module Card
SRQ	Specification Related Question
TSS	Terminservicestelle
TUC	Technischer Use Case
UI	User Interface
VSD	Versichertenstammdaten

12.2 Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt ([gemGlossar]).

12.3 Abbildungsverzeichnis

Abbildung 1: Komponentenmodell (logische Sicht) 15
Abbildung 2: Pic_MOKT_0023 Verhalten bei PIN-Eingabe mit bekannter Länge 34
Abbildung 3: Anwendungsfälle der Fachanwendung VSDM 58
Abbildung 4: Nicht fachliche Anwendungsfälle 59
Abbildung 5: Pic_MOKT_001 Aktivitätsdiagramm zu TUC_MOKT_200 sendAPDU 79
Abbildung 6: Pic_MOKT_002 Aktivitätsdiagramm zu TUC_MOKT_202 readFile 82
Abbildung 7: Pic_MOKT_003 Aktivitätsdiagramm zu TUC_MOKT_209 readRecord 85
Abbildung 8: Pic_MOKT_004 Aktivitätsdiagramm zu TUC_MOKT_214 appendRecord 88
Abbildung 9: Pic_MOKT_005 Aktivitätsdiagramm zu TUC_MOKT_220 fulfillAccessConditions 91
Abbildung 10: Pic_MOKT_006 Aktivitätsdiagramm zu TUC_MOKT_250 selectCardFile 95

Abbildung 11: Pic_MOKT_008 Aktivitätsdiagramm zu TUC_MOKT_405 authenticateCardToCard 99
Abbildung 12: Pic_MOKT_009 Aktivitätsdiagramm zu TUC_MOKT_406 writeEGKAudit . 104
Abbildung 13: Pic_MOKT_010 Aktivitätsdiagramm zu TUC_MOKT_407 selectKeyForAsymmetricExternalAuthentication 107
Abbildung 14: Pic_MOKT_011 Aktivitätsdiagramm zu TUC_MOKT_412 verifyPIN 113
Abbildung 15: Pic_MOKT_012 Aktivitätsdiagramm zu TUC_MOKT_417 readFromEGK .. 119
Abbildung 16: Pic_MOKT_013 Aktivitätsdiagramm zu TUC_MOKT_418 checkEGK 122
Abbildung 17: Pic_MOKT_014 Aktivitätsdiagramm zu TUC_MOKT_419 changePIN 125
Abbildung 18: Pic_MOKT_015 Aktivitätsdiagramm zu TUC_MOKT_420 showEGKAccessInKTDisplay 128
Abbildung 19: Pic_MOKT_023 – Aktivitätsdiagramm zu TUC_MOKT_421 unblockPIN ... 130
Abbildung 20: Pic_MOKT_016 Aktivitätsdiagramm zu TUC_MOKT_438 checkEGKAuthCertificate 134
Abbildung 21: Pic_MOKT_018 Aktivitätsdiagramm zu TUC_MOKT_470 encryptData 137
Abbildung 22: Pic_MOKT_019 Aktivitätsdiagramm zu TUC_MOKT_471 decryptData 141
Abbildung 23: Pic_MOKT_021 Sequenzdiagramm zu TUC_MOKT_010 writeToInternalStorage 145
Abbildung 24: Pic_MOKT_022 Sequenzdiagramm zu TUC_MOKT_011 readFromInternalStorage 148
Abbildung 25 PIC_MOKT_020 Aufbau der Datenstruktur der KVK..... 178
Abbildung 26: PIC_MOKT_021 Aufbau ATR-Header der KVK..... 178

12.4 Tabellenverzeichnis

Tabelle 1: Tab_MobKT_002 Application Identifier der Kartentypen 42
Tabelle 2: Tab_mobKT_ST2_18 Pflichtfelder zum Anzeigen auf dem Display 46
Tabelle 3 : Tab_mobKT_ST2_10 – VSDM-UC_14 Aktivitäten 50
Tabelle 4 : Tab_mobKT_ST2_11 – Fehlerzustände Technische Nutzbarkeit und Offline-Gültigkeit der eGK prüfen 52
Tabelle 5: Tab_mobKT_ST2_13 – Fehlerzustände VSD Status Container Lesen..... 53
Tabelle 6: Tab_mobKT_ST2_14 – Durch das Fachmodul VSDM (mobKT) zu erzeugende Warnmeldung 53
Tabelle 7: Tab_mobKT_ST2_19 – Durch das Fachmodul VSDM (mobKT) zu erzeugende Warnmeldung 54
Tabelle 8: Tab_mobKT_ST2_15 – Durch das Fachmodul VSDM (mobKT) zu erzeugender Protokolleintrag 54
Tabelle 9: Tab_mobKT_ST2_16 – VSDM-UC_14 Aktivitäten 55
Tabelle 10: Tab_mobKT_ST2_17 – Fehlerzustände Versichertendaten prüfen 56

Tabelle 11: Tab_mobKT_ST2_03 Festformat des VersichertenDatenTemplates der KVK.56
Tabelle 12: Mindestsperrzeiten in Abhängigkeit der Anzahl ungültiger Kennworteingaben 70
Tabelle 13: Tab_MOKT_100 - TUC_MOKT_200 sendAPDU 79
Tabelle 14: Tab_MOKT_101 - TUC_MOKT_202 readFile 82
Tabelle 15: Tab_MOKT_102 - TUC_MOKT_209 readRecord 85
Tabelle 16: Tab_MOKT_103 - TUC_MOKT_214 appendRecord 88
Tabelle 17: Tab_MOKT_104 - TUC_MOKT_220 fulfillAccessConditions 91
Tabelle 18: Tab_MOKT_105 - TUC_MOKT_250 selectCardFile.....95
Tabelle 19: Tab_MOKT_120 - Generalisierte Bezeichnung von Artefakten bei CardToCard-Authentication.....98
Tabelle 20: Tab_MOKT_107 - TUC_MOKT_405 authenticateCardToCard 100
Tabelle 21: Tab_MOKT_108 - TUC_MOKT_406 writeEGKAudit 104
Tabelle 22: Tab_MOKT_109 - TUC_MOKT_407 selectKeyForAsymmetricExternalAuthentication.....108
Tabelle 23: Tab_MOKT_110 - TUC_MOKT_412 verifyPIN 113
Tabelle 24: Tab_MoKT_111 Terminalanzeigen beim Eingeben der PIN am Kartenterminal 116
Tabelle 25: Tab_MOKT_112 - TUC_MOKT_417 readFromEGK 120
Tabelle 26: Tab_MOKT_113 - TUC_MOKT_418 checkEGK 122
Tabelle 27: Tab_MOKT_114 - TUC_MOKT_419 changePIN 125
Tabelle 28: Tab_MOKT_115 - TUC_MOKT_420 showEGKAccessInKTDisplay 128
Tabelle 29: Tab_MOKT_121 - TUC_MOKT_421 unblockPIN 130
Tabelle 30: Tab_MOKT_116 - TUC_MOKT_438 checkEGKAuthCertificate.....134
Tabelle 31: Tab_MOKT_118 - TUC_MOKT_470 encryptData 138
Tabelle 32: Tab_MOKT_119 - TUC_MOKT_471 decryptData 142
Tabelle 33: Tab_MOKT_200 Beschreibung zum Technischen Use Case TUC_MOKT_010 writeToInternalStorage 146
Tabelle 34: Tab_MOKT_201 Beschreibung zum Technischen Use Case TUC_MOKT_011 readFromInternalStorage 148
Tabelle 35: Tab_mobKT_005 - Command RESET CT 152
Tabelle 36: Tab_mobKT_006 - Response RESET CT 152
Tabelle 37: Tab_mobKT_007 - Command REQUEST ICC.....153
Tabelle 38: Tab_mobKT_008 - Response REQUEST ICC.....153
Tabelle 39: Tab_mobKT_009 - Command EJECT ICC.....154
Tabelle 40: Tab_mobKT_010 - Response EJECT ICC 154
Tabelle 41: Tab_mobKT_011 - Command SELECT FILE 155
Tabelle 42: Tab_mobKT_012 - Response SELECT FILE 155

Tabelle 43: Tab_mobKT_013 - Command READ BINARY KVK 157
Tabelle 44: Tab_mobKT_014 - Response READ BINARY KVK 157
Tabelle 45: Tab_mobKT_015 - Command READ BINARY eGK 157
Tabelle 46: Tab_mobKT_016 - Response READ BINARY eGK 158
Tabelle 47: Tab_mobKT_017 - Command ERASE BINARY 159
Tabelle 48: Tab_mobKT_018 - Response ERASE BINARY 159
Tabelle 49: Tab_mobKT_019 - Command GET STATUS 160
Tabelle 50: Tab_mobKT_020 - Response GET STATUS 160
Tabelle 51: Tab_mobKT_021 – CardTerminal Manufacturer Data Object Definition (CTM DO) 160
Tabelle 52: Tab_mobKT_022 - Discretionary Data Data Object Definition 161
Tabelle 53: Tab_mobKT_023 - Discretionary Data Data Object Type Definition 162
Tabelle 54: Kommandosequenz Vorbereitung zum Lesen eines VSD Datensatzes 163
Tabelle 55: Kommandosequenz zum Lesen eines VSD Datensatzes von KVK 164
Tabelle 56: Tab_MOKT_005 Erweiterung der Datentypen READ BINARY VSD eGK 165
Tabelle 57: Tab_MOKT_024 Gültige Werte ATR und Directory 181
Tabelle 58: Tab_MOKT_025 Gültige Tags und Längen des Application-File 182
Tabelle 59: Tab_MOKT_026 Liste der im Rahmen von DIN 66003 zulässigen Sonderzeichen 183
Tabelle 60: Tab_MOKT_027 Gesamtliste der im Rahmen von DIN 66003 zulässigen Zeichen 184

12.5 Referenzierte Dokumente

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 sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

12.5.1 Dokumente der gematik

[Quelle]	Herausgeber (Erscheinungsdatum): Titel

[eGK]	Generation 2 / 2.1: [gemSpec_COS] gematik: Spezifikation COS - Spezifikation der elektrischen Schnittstelle [gemSpec_eGK_ObjSys] gematik: Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem [gemSpec_eGK_OPT] - Spezifikation der elektronischen Gesundheitskarte Äußere Gestaltung
[HBA]	[gemSpec_COS] gematik: Spezifikation COS - Spezifikation der elektrischen Schnittstelle [gemSpec_HBA_ObjSys] gematik: Spezifikation HBA Objektsystem
[SMC-B]	[gemSpec_COS] gematik: Spezifikation COS - Spezifikation der elektrischen Schnittstelle [gemSpec_SMC-B_ObjSys] gematik: Spezifikation SMC-B Objektsystem
[gemeGK_Fach]	gematik: Speicherstrukturen der eGK für Gesundheitsanwendungen
[gemGlossar]	gematik: Glossar
[gemSpec_CVC_Root]	gematik: Spezifikation CVC-Root
[gemSpec_eGK_Fach_VSDM]	gematik: Speicherstrukturen der eGK für die Fachanwendung VSDM
[gemSpec_Karten_Fach_TIP]	gematik: Befüllvorschriften für die Plattformanteile der Karten der TI
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_KSR]	gematik: Spezifikation Konfigurationsdienst
[gemSpec_OID]	gematik: Spezifikation OID
[gemSpec_OM]	gematik: Spezifikation Operations und Maintenance (Fehlermanagement, Versionierung, Monitoring)
[gemSpec_TSL]	gematik: Spezifikation TSL-Dienst
[gemSysL_VSDM]	Gematik: Systemspezifisches Konzept Versichertenstammdatenmanagement (VSDM)

[gemZul_MobKT]	gematik: Zulassungsverfahren Mobile Kartenterminals

12.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI_2005]	BSI (2005): IT-Grundschutz-Kataloge; http://www.bsi.bund.de/gshb/deutsch/index.htm
[BSI-CC-PP-0052]	BSI: Common Criteria Protection Profile Mobile Card Terminal for the German Healthcare System (MobCT), BSI-CC-PP-0052
[CEN ENV]	CEN ENV1375-1 (1994): Identification card systems – Intersector integrated circuit(s) card additional formats – Part 1: ID-000 card size and physical characteristics
[CT-API]	Dt. Telekom AG (B. Kowalski, R. Moos) , Fraunhofer Institut (L. Eckstein, B. Struif), TÜV-IT (J. Atrott), TeleTrust (Prof. Dr.H. Reimer) (7.Juni 2001): CT- API, Version 1.1.1
[BMV-Ä 2014]	Bundesmantelvertrag-Ärzte (BMV-Ä) Anlage 2 - Vereinbarung über die Vordrucke für die vertragsärztliche Versorgung Gültig ab: 1.10.2014
[DAHZ]	DAHZ Hygieneleitfaden Ausgabe 7 (2006): Hygieneleitfaden des Deutschen Arbeitskreises für Hygiene in der Zahnmedizin
[ISO7810]	ISO/IEC 7810 (2003): Identification cards – Physical characteristics
[ISO7816-10]	ISO/IEC 7816-10 (1999): Identification cards – Integrated circuit(s) cards with contacts Part 10 – Electronic signals and answer to reset for synchronous cards
[ISO7816-12]	ISO/IEC 7816-12 (Oktober 2005): Cards with contacts – USB electrical interface and operating procedures

[ISO7816-2]	ISO/IEC 7816-2 (2007): Identification cards – Integrated circuit(s) cards with contacts Part 2 – Dimension and location of the contacts
[ISO7816-3]	ISO/IEC 7816-3 (2005): Identification cards – Integrated circuit(s) cards with contacts Part 3 – Electronic Signals and Transmission Protocols
[KBV_ITA_VGEX_Mapping_KVK]	KBV: Technische Anlage zu Anlage 4a (BMV-Ä/EKV) - Verarbeitung KVK/eGK im Rahmen der vertragsärztlichen Abrechnung im Basis-Rollout In der jeweils aktuellen Version, abrufbar unter: ftp://ftp.kbv.de/ita-update/Abrechnung/KBV_ITA_VGEX_Mapping_KVK.pdf
[KBV_ITA_VGEX_Mapping_KVK_1.06]	KBV: Technische Anlage zu Anlage 4a (BMV-Ä/EKV) - Verarbeitung KVK/eGK im Rahmen der vertragsärztlichen Abrechnung im Basis-Rollout Version 1.06 vom 27.05.2014
[ISO7816-4]	Identification cards — Integrated circuit cards - Part 4: Organization, security and commands for interchange
[KVK]	GKV-Spitzenverband, KBV, KZBV (25.11.2009): Technische Spezifikation der Versichertenkarte, Version 2.08
[MKT_10]	TeleTrust (15.4.1999): Multifunktionale KartenTerminals MKT –Spezifikation – MKT-Version 1.0
[PRODSG]	BGBl. I S. 2179; 2012 I S. 131 (2011): Gesetz über die Bereitstellung von Produkten auf dem Markt (Produktsicherheitsgesetz - ProdSG)
[RFC2119]	RFC 2119 (March1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt
[RKI]	Robert Koch Institut (2004): Anforderungen an die Hygiene bei der Reinigung und Desinfektion von Flächen – Empfehlung der Kommission für Krankenhaushygiene und Infektionsprävention beim Robert Koch-Institut (RKI)
[SGB V]	BGBl. I S.2477 (20.12.1988): Sozialgesetzbuch, Fünftes Buch

[SICCT]	SICCT (17.12.2010): TeleTrusT, SICCT Secure Interoperable ChipCard Terminal, Version 1.21
[TRBA 250]	Ausschuss für Biologische Arbeitsstoffe – ABAS: Technischen Regeln für Biologische Arbeitsstoffe im Gesundheitswesen und in der Wohlfahrtspflege Ausgabe: November 2003 Änderung und Ergänzung Juli 2006 (bundesarbeitsblatt 7-2006, S. 193) Ergänzung April 2007, GMBl Nr. 35 v. 27. Juli 2007, S. 720 Änderung und Ergänzung November 2007, GMBl Nr.4 v. 14.02.2008, S. 83

12.6 Nutzung von Kartenelementen (COS und Objektsysteme)

Die nachfolgende Tabelle enthält die im Rahmen dieser Spezifikation spezifizierten sicherheitsrelevanten Kartenzugriffe auf G2-Karten (Verwendung von Kartenkommandos bzw. Zugriffe auf Kartenobjekte), die eine Sicherheitsleistung im Sinne des [BSI-CC-PP-0052] darstellen.

COS bzw. Kartentyp	**Kartenkommando (COS)**	**Kartenobjekt (Objektsystem)**
COS	Verify	
	Get Pin Status	
	Change Reference Data	
	Reset Retry Counter	
	Manage Security Envrionment	
	Get Random	
	PSO Decipher	
	PSO Encipher	
	PSO Verify Certificate	
	Internal Authenticate	
	External Authenticate	

	Get Challenge	
	Append Record	
	Read Binary	
HBA		/MF/DF.ESIGN/PrK.HP.ENC.R2048
		/MF/ DF.ESIGN/EF.C.HP.ENC.R2048
		/MF/PIN.CH
		/MF/EF.C.CA_HPC.CS.R2048
		/MF/EF.C.CA_HPC.CS.E256
		/MF/EF.C.HPC.AUTR_CVC.R2048
		/MF/EF.C.HPC.AUTR_CVC.E256
		/MF/PrK.HPC.AUTR_CVC.R2048
		/MF/PrK.HPC.AUTR_CVC.E256
		/MF/PuK.RCA.CS.R2048
		/MF/PuK.RCA.CS.E256
		/MF/DF.ESIGN/EF.C.HP.AUT.R2048
SMC-B		/MF/DF.ESIGN/PrK.HCI.ENC.R2048
		/MF/DF.ESIGN/EF.C.HCI.ENC.R2048
		/MF/PIN.SMC
		/MF/EF.C.CA_SMC.CS.R2048
		/MF/EF.C.CA_SMC.CS.E256
		/MF/EF.C.SMC.AUTR_CVC.R2048
		/MF/EF.C.SMC.AUTR_CVC.E256
		/MF/PrK.SMC.AUTR_CVC.R2048
		/MF/PrK.SMC.AUTR_CVC.E256

		/MF/PuK.RCA.CS.R2048
		/MF/PuK.RCA.CS.E256
		/MF/DF.ESIGN/EF.C.HCI.AUT.R2048
eGK		/MF/DF.HCA/EF.Logging
		/MF/EF.C.CA_eGK.CS.E256
		/MF/EF.C.eGK.AUT_CVC.E256
		/MF/PrK.eGK.AUT_CVC.E256
		/MF/PuK.RCA.CS.E256
		/MF/DF.ESIGN/EF.C.CH.AUT.R2048

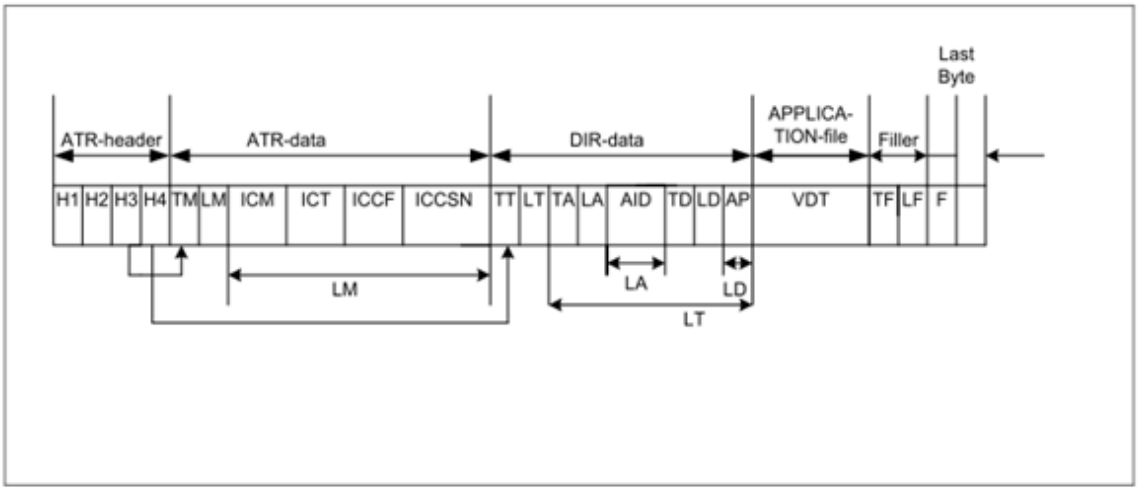
Offener Punkt:

Die Tabelle in Anhang A6 zu den Zugriffen, welche eine Sicherheitsleistung gemäß [BSI-CC-PP-0052] darstellen, befindet sich noch in Abstimmung mit dem BSI.

Das Thema wird daher als offener Punkt geführt.

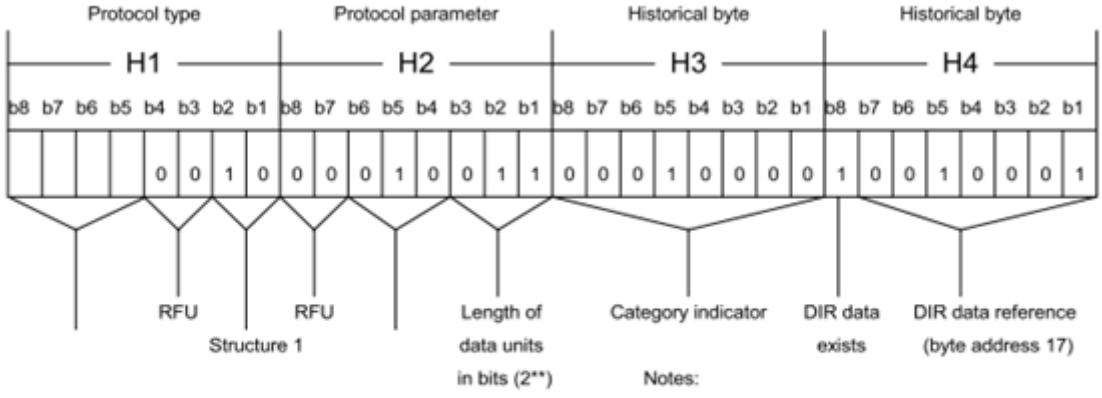
13 Anhang B – Prüfvorgaben KVK

13.1 Aufbau der KVK



AID	= Application Identifier of KVK-Application	ICCF	= IC Card Fabricator Id.	LT	= Length application-templ.
AP	= Application Personal-lizer Identifier	ICCSN	= IC Card Serial Number	TA	= Tag of AID = '4F'
ATR	= Answer-To-Reset	ICM	= IC Manufacturer Id.	TD	= Tag of discretionary data = '53'
DIR	= Directory	ICT	= IC Type	TF	= Tag of filler = 'C0'
F	= Filler	LA	= Length of AID	TM	= Tag of manufacturer data = '46'
H1,H2	= ATR protocol bytes	Last Byte	= Adresse 255 (ggf. + 254)	TT	= Tag of application-template = '61'
H3,H4	= ATR historical bytes	LD	= Length of discretionary data'	VDT	= Versicherten-Daten-Template
		LF	= Length of filler		
		LM	= Length manufacturer data		

Abbildung 25 PIC_MOKT_020 Aufbau der Datenstruktur der KVK



Protokoll type S
'1000' = serial data access protocol (I2Cbus)
'1001' = 3 wire bus protocol
'1010' = 2 wire bus protocol

Number of data units
010 = 256

Notes:
1. b1 is the least significant bit (lsb) and transmitted first
2. Additional ATR-data are to find between H4 an the DIR data section without explicit indication

Abbildung 26: PIC_MOKT_021 Aufbau ATR-Header der KVK

13.2 Prüfvorgaben der KVK

Folgende Prüfungen sind für die von der KVK gelesenen Daten gemäß der technischen Spezifikation der Krankenversichertenkarte [KVK] durchzuführen:

Generelle Prüfungen:	· Tags auf zulässige Werte · Längen auf Werte innerhalb des zulässigen Wertebereichs · Values auf Entsprechung der Längenangabe und des zulässigen eingeschränkten Zeichensatzes
ATR-Header:	· Prüfung auf zulässigen Inhalt gemäß technischer Spezifikation der Krankenversichertenkarte (s. Tabelle 58: Tab_MOKT_024 Gültige Werte ATR und Directory).
ATR-Data, DIR-Data:	· Wenn im ATR-Header das Vorhandensein codiert ist, sind die in der KVK-Spec. (Ziffer 6.2) angegebenen Konstanten auf Wert und Position zu überprüfen. Bei variablen Werten ist zu prüfen, ob diese im zulässigen Zeichensatz definiert sind (s. Tabelle 58: Tab_MOKT_024 Gültige Werte ATR und Directory).
Filler:	· Prüfung auf zulässigen Tag und zulässigen Wert (’20’) auf allen Bytes des value. Zur Längenangabe: Die Adresse des letzten Bytes des Fillers ist 254. Beginnt das Datenobjekt Filler mit der Byte-Adresse 125 und beträgt die Längenangabe 127, so ist die Adresse des letzten Bytes 253.
letzte Bytes:	· Die nicht belegten Bytes nach dem Filler erhalten den hexadezimalen Wert ’00’. Handelt es sich bei dem verwendeten Chip um einen I²C-Bus-Baustein, der das letzte Byte zur Steuerung eines Schreibschutzes verwendet, so ist das letzte Byte so zu belegen, dass kein Schreibschutz besteht. Der Wert kann in diesem Fall hexadezimal ’00’ oder ’FF’ annehmen. Endet der Filler mit dem drittletzten Byte, so ist das vorletzte Byte mit dem gleichen Wert wie das letzte Byte zu belegen.
Datenstruktur des Application-File:	· Zu prüfen sind: Zulässigkeit der Zeichen (Zeichensatz nach DIN 66003). Korrektheit der Werte in den Tags, korrekte Datentypen, Feldlängen in den zulässigen Grenzen. Die Übereinstimmung der angegebenen mit der tatsächlichen Feldlänge ist Tabelle 59: Tab_MOKT_025 Gültige Tags und Längen des Application-File zu entnehmen. In Abweichung zur Spezifikation der Krankenversichertenkarte ist das Feld „Gültigkeitsdatum“ optional zu behandeln. · Datentypen Bei alphanumerischen Daten ist grundsätzlich die Zulässigkeit der Zeichen (eingeschränkter Zeichensatz gem. Tabelle 60: Tab_MOKT_026 Liste der im Rahmen von DIN 66003 zulässigen Sonderzeichen und Tabelle 61: Tab_MOKT_027 Gesamtliste der im

Rahmen von DIN 66003 zulässigen Zeichen) zu prüfen.

Datenobjekt	Datentyp
KrankenKassenName	alphanum.
KrankenKassenNummer	numerisch
VersichertenNummer	numerisch
VKNR /WOP-Kennz. *)	numerisch
VersichertenStatus	numerisch
StatusErgänzung	alphanum.
Titel	alphanum.
VorName	alphanum.
Namenszusatz/Vorsatzwort	alphanum.
FamilienName	alphanum.
Geburtsdatum	Ttmmjjjj 1)
StraßenName&HausNummer	alphanum.
WohnsitzLänderCode	alphanum.
Postleitzahl	alphanum.
OrtsName	alphanum.
GültigkeitsDatum	Mmjj
PrüfSumme	numerisch

1) Im Feld Geburtsdatum ist die Angabe von Tag 00 und Monat 00 zulässig. Im Monat ist 00 nur in Verbindung mit Tag 00 zulässig.

*) Das WOP-Kennzeichen gilt nur für Betriebs- und Innungskrankenkassen, entsprechend dem Kennzeichen gemäß § 2 Abs. 2 der Vereinbarung zur Festsetzung des Durchschnittsbetrages gemäß Artikel 2 § 2 Abs. 2 des Gesetzes zur Einführung des Wohnortprinzipes bei Honorarvereinbarungen für Ärzte und Zahnärzte und zur Krankenversichertenkarte gemäß § 291 Abs. 2 SGB V.

Die Prüfsumme wird über alle Datenobjekte des VersichertenDatenTemplates, incl. Tags und Length gebildet, beginnend mit dem Tag ’60’ bis zur Längenangabe der Prüfsumme

(LPS). Die Daten werden byteweise mit XOR verknüpft. Das Ergebnis dieser Verknüpfung ist der Value der Prüfsumme.

Tabelle 57: Tab_MOKT_024 Gültige Werte ATR und Directory

Adresse	Bereich	Bezeichnung	Zulässige Werte (hexadezimal)
0	ATR-Header	H1	82 (I²C-Bus) 92 (3-wire) A2 (2-wire)
1		H2	13
2		H3	10
3		H4	91
4	ATR-data	TM	46
5		LM	0B
6		ICM	Keine Prüfung
7		ICT	Keine Prüfung
8-12		ICCF	Keine Prüfung
13-16		ICCN	Keine Prüfung
17	DIR-Data	TT	61
18		LT	0B
19		TA	4F
20		LA	06
21		AID	D2
22			80 76
23			00
24			00
25			01
26			01
27		TD	53
28		LD	01
29		AP	Keine Prüfung

Tabelle 58: Tab_MOKT_025 Gültige Tags und Längen des Application-File

Tag	length (min-max)	value
'60'	70-212	VersichertenDatenTemplate
'80'	2-28	KrankenKassenName
'81'	7	KrankenKassenNummer
'8F'	5	VKNR / WOP-Kennzeichen
'82'	6-12	VersichertenNummer
'83'	1 oder 4	VersichertenStatus
'90'	1-3	StatusErgänzung
'84'	2-15	Titel[2)]
'85'	1-28	VorName[2)] (mehrere Vornamen sind durch Bindestrich oder Blank getrennt)
'86'	1-15	NamensZusatz/VorsatzWort[2)] (mehrere Namenszusätze sind durch Blank getrennt)
'87'	2-28	FamilienName
'88'	8	GeburtsDatum (TTMMJJJJ)
'89'	2-28	StraßenName & HausNummer (durch Blank getrennt)
'8A'	1-3	WohnsitzLänderCode[3)] (Datenobjekt entfällt bei Defaultwert = D)
'8B'	4-7	Postleitzahl[3)]
'8C'	2-23	OrtsName[3)] (mehrere Namensbestandteile durch Blank oder Sonderzeichen getrennt)
'8D'	4	GültigkeitsDatum (MMJJ)
'8E'	1	PrüfSumme (XOR) über das gesamte VersichertenDaten-Template

Erläuterung zu Tabelle 59: Tab_MOKT_025 Gültige Tags und Längen des Application-File der Tabelle zur Datenstruktur des Application-File

2) Die Datenobjekte '84' Titel, '85' VorName und '86' NamensZusatz/VorsatzWort können zusammen mit den Blanks, welche die Datenobjekte trennen, im einzeiligen Ausdruck auf den Vordrucken der kassenärztlichen Versorgung nicht mehr als 28 Zeichen annehmen.

Da die Blanks, welche im Ausdruck die Datenobjekte trennen, durch die Druckersteuerung eingeschoben werden, nicht aber im Chip gespeichert sind, ergeben sich für die Summe der value-Felder folgende Maximallängen:

1 Datenobjekt 15 Byte, bei Vorname = 28 Byte

2 Datenobjekte 27 Byte

3 Datenobjekte 26 Byte

3) Die Datenobjekte '8A' Wohnsitz-LänderCode, '8B' Postleitzahl und '8C' Ortsname können zusammen mit den Blanks, welche die Datenobjekte trennen, im einzeiligen Ausdruck auf den Vordrucken der kassenärztlichen Versorgung nicht mehr als 28 Zeichen annehmen.

Da die Blanks, welche im Ausdruck die Datenobjekte trennen, durch die Druckersteuerung eingeschoben werden, nicht aber im Chip gespeichert sind, ergeben sich für die Summe der value-Felder folgende Maximallängen:

2 Datenobjekte 27 Byte

3 Datenobjekte 26 Byte

Tabelle 59: Tab_MOKT_026 Liste der im Rahmen von DIN 66003 zulässigen Sonderzeichen

Zeichen	Bezeichnung	Hex-Code	Zeichen	Bezeichnung	Hex-Code
	Leerzeichen (Space)	'20'	&	kommerzielles Und	'26'
'	Apostroph	'27'	(	Klammer auf	'28'
)	Klammer zu	'29'	+	plus	'2B'
-	Bindestrich	'2D'	.	Punkt	'2E'
/	Schrägstrich	'2F'	_	Unterstreichung	'5F'

Tabelle 60: Tab_MOKT_027 Gesamtliste der im Rahmen von DIN 66003 zulässigen Zeichen

HEX	20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F
NUM	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
ALPHA	SP						&	'	(	)		+		-	.	/
HEX	30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F
NUM	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
ALPHA	0	1	2	3	4	5	6	7	8	9						
HEX	40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F
NUM	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
ALPHA		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
HEX	50	51	52	53	54	55	56	57	58	59	5A	5B	5C	5D	5E	5F
NUM	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
ALPHA	P	Q	R	S	T	U	V	W	X	Y	Z	Ä	Ö	Ü		_
HEX	60	61	62	63	64	65	66	67	68	69	6A	6B	6C	6D	6E	6F
NUM	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
ALPHA		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
HEX	70	71	72	73	74	75	76	77	78	79	7A	7B	7C	7D	7E	7F
NUM	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
ALPHA	p	q	r	s	t	u	v	w	x	y	z	ä	ö	ü	ß	