SRQ - Specification Related Question

SRQ-ID: 0773

Betrifft (wird vom FLS (optional vom Erfasser) ausgefüllt):

Themenkreis	Dezentrale Komponenten
Schlagwort	mobiles Kartenterminal, Ausbaustufe 1, CT-API, Übertragungsprotokoll
zu Dokument / Datei	[gemSpec_MobKT]
Version	1.1.0
Bezug (Kap., Abschnitt, Tab., Abb.)	gesamt

Stichwort: mobiles Kartenterminal, Ausbaustufe 1, CT-API, Übertragungsprotokoll

Frage:

Welche Korrekturen sind an der Spezifikation 1.1.0 vorgenommen worden, um vorhandene Unschärfen oder Fehler zu beheben?

Betrifft (wird vom PB ausgefüllt):

Gültig ab Release	0.5.2	Verbindlichkeit	
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	☐ erfasst ☐ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☐ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Es ergeben sich folgende Korrekturen:

5.1 Zulassungsverfahren, Zertifikat

~~*Das Dokument „Einführung der Gesundheitskarte -Zulassung von dezentralen IT-Komponenten in der Telematikinfrastruktur (mobiles Kartenterminal Ausbaustufe 1)“ ist noch nicht verfügbar und befindet sich in der Entstehung.*~~

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 ~~und anschließend Interoperabilitätstests durchführt~~. Details zur Zulassung sind im Dokument „Zulassung von dezentralen IT-Komponenten in der Telematikinfrastruktur (Mobile Kartenterminals)“ [gemZul_MobKT] beschrieben.

5.2 Zulassungsanforderungen

~~*Die Zulassungsanforderungen bezüglich der Sicherheit sind noch offen. Sie orientieren sich jedoch an denen des KVT mobil Lesegerätes, da in der Ausbaustufe 1 keine zusätzlichen Sicherheitsanforderungen entstehen. Die Evaluationsstufe der zugrunde liegenden [KVT-Mobil] war E2 mit der Mindeststärke der Mechanismen: niedrig. Ein äquivalentes Sicherheitsniveau ist für die Ausbaustufe 1 ausreichend. In der Ausbaustufe 2 wird das Sicherheitsniveau aller Voraussicht nach höher liegen.*~~

5.3.1 Anschlussarten

~~Die beiden Komponenten MÜSSEN sich jedoch gegenseitig authentifizieren bevor Daten an der internen Schnittstelle übertragen werden dürfen um sicherzustellen, dass nur dafür vorgesehene Komponenten miteinander kommunizieren.~~

5.3.4 Anzeige der Versichertenstammdaten

Verfügt das mobile Kartenterminal über ein Display, so MUSS das Kartenterminal die während der Datenerfassung zuletzt gelesenen VSD anzeigen, hierbei ist die jeweils aktuell verbindlich festgelegte VSD-Schemaversion zu unterstützen [A_02097]. Die Anzeige der ausgelesenen VSD erfolgt hierbei zusätzlich zum Zwischenspeichern der Daten. Zu Kontrollzwecken MUSS, bei vorhandenem Display, das mobile Kartenterminal zwischengespeicherte Daten zur Anzeige bringen können [A_02098]. Das mobile Kartenterminal MUSS, wenn es zwischengespeicherte Daten anzeigen kann, dem Benutzer eine Möglichkeit bereitstellen, durch die Datensätze zu navigieren [A_02099]. Das mobile Kartenterminal MUSS, bei vorhandenem Display, die VSD einer Karte auch direkt zur Anzeige bringen, z. B. falls es keinen Platz mehr hat, die Daten zwischenzuspeichern [A_02100].

5.3.5 Übertragung

~~Als übertragen markierte VSD eines abgelaufenen Quartals MÜSSEN zum Ende des Quartals automatisch durch das mobile Kartenterminal gelöscht werden [A_02108].~~

5.3.16 Firmwareupdate

Das mobile Kartenterminal MUSS über einen Mechanismus zum sicheren Firmwareupdate verfügen [A_02135]. Jede Firmware Version MUSS über eine

Versionsnummer verfügen [A_02136]. Eine neuere Version MUSS eine höhere Versionsnummer haben, als eine ältere [A_02137]. Beim Einspielen einer neuen Firmware MUSS sichergestellt sein, dass das Update nur auf die gleiche oder eine neuere Version als installiert möglich ist [A_02138]. Ist eine Regression auf eine ältere Firmwareversion erforderlich, so MUSS diese mit einer neuen Versionsnummer versehen werden [A_02139]. ~~Ein neuerliches Einspielen der bereits installierten Version KANN möglich sein. Es MUSS zuvor sichergestellt sein, dass die installierte Software korrekt installiert ist. Es DARF NICHT dazu verwendet werden, fehlerhafte Installationen zu korrigieren [A_02140].~~

5.4.1.2 Kontaktiereinheiten

Das mobile Kartenterminal KANN anzeigen, wenn sich eine Chipkarte korrekt in der Kontaktiereinheit befindet und diese mit Strom versorgt ist (z. B. leuchtende LED) [A_02157].

5.4.1.3 Bauformen und Ausprägungen

Die Dockingstation DARF die NFD bzw. VSD NICHT an andere Systeme, als das PS weitergeben oder dauerhaft speichern [A_02162]. Nachdem ein Datensatz übertragen wurde, MÜSSEN diese aus dem Zwischenspeicher der Dockingstation gelöscht werden [Tmp_A_20000].

5.4.7 Belastbarkeit

~~Das mobile Kartenterminal MUSS den Belastungen, die bei normaler Benutzung auftreten, widerstehen können [A_02178].~~

Im mobilen Einsatz ist das mobile Kartenterminal höheren Belastungen ausgesetzt als vergleichbare stationäre Komponenten. Im Folgenden werden die Anforderungen an die Belastbarkeit des mobilen Kartenterminals beschrieben.

5.4.7.1 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 [A_03647]. Bei sachgemäßer Handhabung oder bei gestörtem Betrieb DARF ein gefährlicher Zustand NICHT eintreten können [A_02179].

Das mobile Kartenterminal unterliegt den Anforderungen aus dem Geräte- und Produktsicherheitsgesetz (GPSG) [GPSG] und das Einhalten der Anforderungen aus dem GPSG ist Bestandteil der Betriebszulassung durch die gematik. Darüber hinaus KANN die Betriebssicherheit einer Komponente durch ein Prüfzeichen (z. B. GS) nachgewiesen werden.

5.4.7.4 Klima

Mobile Kartenterminals MÜSSEN mindestens bei einer Lagertemperatur von -20°C bis 60°C und einer relativen Luftfeuchtigkeit von 5% bis 95% funktionsfähig sein [A_03650].

Die Funktionsfähigkeit MUSS mindestens im Bereich der Raumtemperatur von 0°C bis 40°C liegen [A_03651].

5.4.8 Transportierbarkeit

Um dem Leistungserbringer Mobilität zu ermöglichen MÜSSEN mobile Kartenterminals weniger als 0,7 Kilo wiegen und ein Volumen kleiner als 1 dm^3 aufweisen [A_03653].

5.5.1 Authentifikationsmechanismus

Der Authentifikationsstatus ~~MUSS nach maximal 24 Stunden zurückgesetzt werden und~~ MUSS zurückgesetzt werden, wenn das Entnehmen der zuletzt gesteckten KVK oder eGK maximal 15 Minuten zurück liegt und in dieser Zeit keine weitere KVK oder eGK gesteckt wurde [A_02189].

5.5.5 Kartenzugriff

Es DARF NICHT möglich sein, über interne oder externe Schnittstellen schreibend auf eine KVK zuzugreifen [A_02203]. Es MUSS im Hinblick auf die Migration zur Ausbaustufe 2 möglich sein, schreibend auf den Logging-Container der eGK zuzugreifen [A_02204]. Dies wird für die Ausbaustufe 1 noch nicht benötigt. Schreibzugriffe auf die eGK außerhalb des Logging-Containers DARF das mobile Kartenterminal allerdings NICHT zulassen [A_02205].

~~Ein direkter Zugriff auf eine gesteckte Karte bei Anschluss an das Primärsystem DARF NICHT möglich sein [A_02206].~~

6.2 Sequenzdiagramme

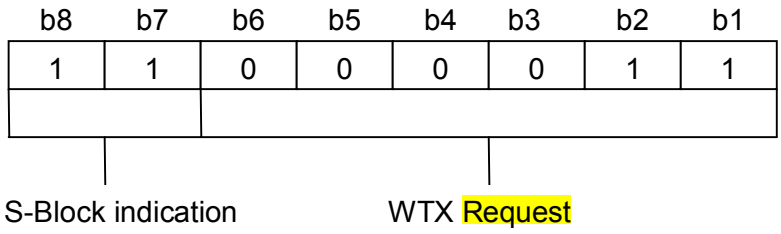
Technischer Use Case TUC_MOKT_001 „Daten erfassen“

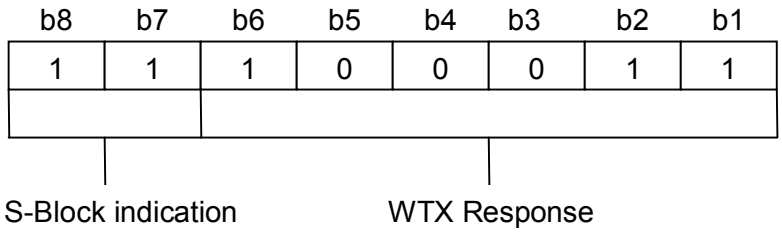
Tabelle 1 Beschreibung des Sequenzdiagramms „Daten erfassen“

Schritt	Beschreibung
1	Das Kartenterminal führt ein Reset der Karte durch und liefert daraufhin den ATR (Answer-To-Reset) der Karte zurück.
2	Der Kartentyp wird bestimmt.
3a.	(optionaler Schritt) EF.ATR wird ausgelesen (enthält Details über die „extended length“-Unterstützung der Karte). *EF.ATR ist nicht zu verwechseln mit dem eigentlichen ATR der Karte, welches nach dem Reset geliefert wird!*
4a.	(optionaler Schritt) EF.GDO wird ausgelesen (enthält die ICSSN).
5a.	(optionaler Schritt) EF.DIR wird ausgelesen (enthält die Applikationen, die auf der eGK gespeichert sind). Die optionalen Schritte 3a – 5a dienen zur Bestimmung des Kartentyps. Es ist jedoch zulässig diese Schritte auszulassen und davon auszugehen, dass es sich bei gesteckten Karten um eGKs bzw. KVKs handelt.
6a.	Der Status der VD (EF.StatusVD) wird gelesen und zu den zu speichernden Versicherungsdaten (daten) hinzugefügt.
7a.	Anhand des StatusVD wird die Integrität der Daten geprüft. Sind die Daten nicht integer, wird der Vorgang abgebrochen.

Schritt	Beschreibung
8a.	Die Persönlichen Daten (EF.PD) werden gelesen und zu den zu speichernden Versicherungsdaten (daten) hinzugefügt.
9a.	Die ungeschützten Versichertendaten (EF.VD) werden gelesen und zu den zu speichernden Versicherungsdaten (daten) hinzugefügt.
3b.	Die Versichertendaten auf der KVK werden gelesen.
4b.	Die Versichertendaten werden auf Integrität geprüft. Sind die Daten nicht integer, wird der Vorgang abgebrochen.
10.	Das aktuelle Datum wird erfasst.
11.	Das mobile Kartenterminal speichert die gelesenen Versichertendaten samt Erfassungsdatum (daten) im persistenten Zwischenspeicher ab.

7.1.2.2.3 Antwortzeit-Verlängerung





7.2.2.2 REQUEST ICC

Mit diesem Kommando wird die Chipkarte angefordert. Nach Einführung der Chipkarte wird automatisch ein Reset durchgeführt. Der Timer T ist auf ‚01' (=1 Sekunde) zu setzen. Im L-Byte ist dann ebenfalls ‚01' (Length = 1 Byte) anzugeben. Wird das Kommando ohne Lc und ohne Daten gesendet ist der Timer per default 1 Sekunde.

Command

Command für KVK und eGK					
CLA	INS	P1	P2	Lc	Data
20	12	01	00	01	T
20	12	01	00	-	-

7.2.2.3 EJECT ICC

Das Kommando steuert die Kontaktiereinheit und ggf. vorhandene Signalgeber. Der Timer T ist auf ‚01' (=1 Sekunde) zu setzen. Im L-Byte ist dann ebenfalls ‚01' (Length = 1 Byte) anzugeben. Gesetzte Indikatoren (LEDs und/oder akustisches Signal) werden nach Herausnahme der Karte bzw. nach Ablauf des Application Timers, wenn die Karte nicht entnommen wurde, gelöscht. Wird das Kommando ohne Lc und ohne Daten gesendet ist der Timer per default 1 Sekunde.

Command

Command für KVK und eGK					
CLA	INS	P1	P2	Lc	Data
20	15	01	00	01	T
20	15	01	00	-	-

Response

Response bei KVK und eGK		Bedeutung
SW1	SW2	
90	00	command successful
~~90~~	~~01~~	~~command successful, card removed~~
~~62~~	~~00~~	~~No buffered VSD available for ejection.~~

7.2.3.2 READ BINARY

Das Kartenterminal stellt sicher, dass der zuletzt übertragenen Datensatz mittels ERASE BINARY durch das PS gelöscht wurden bevor es die Übertragung des nächsten gespeicherten Datensatzes zulässt.

Als Offset sollte im READ BINARY-Kommando ‚0000' angegeben werden, d. h. es soll ab logischer Adresse ‚0000' (= Anfangsadresse der Anwendungsdaten, beginnend mit dem Tag ‚60') gelesen werden. Als Länge sollte ‚00' angegeben werden, d. h. es soll der komplette zur Anwendung gehörende Datenbereich, also das gesamte VD-Template, beginnend mit Tag ‚60' und endend mit dem XOR-Prüfbyte des ASN.1-Elements ‚Prüfsumme' und die zusätzlichen Datenobjekte, gelesen werden. […] Das Kommando kann auch mit variablem Offset angegeben werden (MMMM) in P1 und P2, wobei die Daten in diesem Fall ab dem angegebenen 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 der Status-Byte ‚6F00' zurückgegeben.

Command

Command im Falle der KVK				
CLA	INS	P1	P2	Le
00	B0	00	00	00
00	B0	MM	MM	N

Response

Im Fall der KVK			Bedeutung
Daten	SW1	SW2	
KVK-Daten	90	00	Command Successful
-	65	01	Memory Failure or data corrupt
-	6B	00	Wrong offset
-	6F	00	Error during communication (i. e. checksum error)

[…]

Response bei eGK

Daten	SW1	SW2
Verwaltungs- und eGK-Daten: Status	90	00

Personendaten Lesen von eGK

CLA	INS	P1	P2	Le
00	B0	81	00	00 00 00

Response bei eGK

Daten	SW1	SW2
eGK-Daten: Persönliche Daten	90	00

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

Allgemeine Versicherungsdaten Lesen von eGK

CLA	INS	P1	P2	Le
00	B0	82	00	00 00 00

Response bei eGK

Daten	SW1	SW2
eGK-Daten: Allgemeine Versicherungsdaten	90	00

7.2.4.3 Lesen der eGK (SW1SW2=9001)

Im Falle einer eGK MUSS die weitere Kommandosequenz für das Auslesen der Daten wie folgt geändert werden.

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 (StatusVD)	00 b0 8c 00 00 oder 00 b0 8c 00 00 00 00	Statusdaten, Erfassungsdatum und Zulassungsnummer lesen
5	READ BINARY (Personal Data)	00 b0 81 00 00 00 00	Personendaten lesen
6	READ BINARY (Insurance Data)	00 b0 82 00 00 00 00	Allgemeine Versicherungsdaten lesen
7	ERASE BINARY	00 0e 00 00	unmittelbar zuvor übertragenen Datensatz (StatusVD, Personal Data und Insurance Data) löschen
8	EJECT ICC	20 15 01 00 01 00	Deaktivieren des elektrischen Interface

7.3 Erweiterungen der Datentypen bei der Übertragung

Die Zulassungsnummer hat die Form ZLS_mobKT_*HST_nnnnnn* wobei die Bezeichner die folgende Bedeutung haben:

- *ZLS:* Der Zulassungsschlüssel (ZLS), der für einen konkreten Firmware-Stand verwendet werden MUSS, wird dem Hersteller von der gematik bei der Anmeldung zur Zulassung bekannt gegeben.
- *HST:* Das dreistellige Herstellerkürzel
- *nnnnnn:* Eine pro Hersteller fortlaufende Nummer inklusive einer Prüfziffer

[…]

Zur Berechnung der Prüfsumme werden die Daten des Tags 92 an die Daten des Tags 91 angehängt. Zudem werden Tag 93 und dessen Länge 01 ebenfalls angehängt und in die Berechung der Prüfsumme miteinbezogen.

8.3.3 Erweitertes Display

Das erweiterte Display MUSS mindestens ein ~~zweifarbiges~~ Grafik-Display ~~mit einer Größe von 256x128 Pixel~~ sein [A_03694]. Das erweiterte Display SOLL bei kleinster Schriftgröße mindestens 8 Zeilen á 16 Zeichen darstellen können [A_03695].