Elektronische Gesundheitskarte und Telematikinfrastruktur

Errata zu Release 3.1.1 Online-Produktivbetrieb (Stufe 3)

führt zu

Release 3.1.1-1

Version:	1.0.0
Stand:	27.08.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemErrata_R3.1.1-1]

Betroffene Produkttypen	Neue Produkttypversion
gemProdT_COS	4.5.0-0

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_6969	gemSpec_COS	Kap. 14.2.7	**Ergänzung zur Selektion von Kartenanwendungen** Kartenanwendungen lassen sich derzeit mittels diverserser Use Cases selektieren. Dabei werden nicht alle in ISO/IEC 7816-4 genannten Möglichkeiten normativ gefordert. Apples iOS 13 verlangt derzeit eine SELECT-Variante, die nicht normativ gefordert wird. Deshalb ist die Wahrscheinlichkeit, dass ein von der gematik zugelassenes COS von Apple iOS 13 unterstützt wird gering.	Es wird ein neuer Use Case eingeführt: Select per AID, first, Antwortdaten mit File Control Information siehe C_6969_Anlage	gemSpec_COS gemProdT_COS

1 Einleitung

Entsprechend den Regelungen im „Gesetz für schnellere Termine und bessere Versorgung (Terminservice- und Versorgungsgesetz TSVG)“ sollen ab dem 01.12.2019 durch Krankenkassen elektronische Gesundheitskarten ausgegeben werden, die mit einer kontaktlosen Schnittstelle (NFC) ausgestattet sind. Die NFC-Schnittstelle soll geeignet sein, um mit gängigen mobilen Geräten genutzt zu werden. Insbesondere soll die NFC-Schnittstelle im Rahmen der elektronischen Patientenakten durch Versicherte im ePA-Frontend des Versicherten eingesetzt werden. Mit der derzeitigen beta-Version von iOS/iPadOS 13 existieren Interoperabilitätsprobleme, die mit dieser COS-Änderung behoben werden sollen.

2 Änderungen an [gemSpec_COS]

Die SELECT-Variante mit P2=00 (so wie sie momentan von Apple verwendet wird) gehört derzeit nicht zum normativen Umfang in [gemSpec_COS]. Gemäß [ISO/IEC 7816–4#Tab.8] bestehen die File Control Information (FCI) aus File Control Parameters (FCP) und File Management Data (FMD). Die von Apple verwendete SELECT-Variante ist unter anderem in [GPC_SPE_034#11.9] spezifiziert, weshalb sich der folgende Vorschlag daran orientiert:

2.1 Änderung 1: Neuer Use Case SELECT per AID, Antwort mit FCI

In [gemSpec_COS] wird nach 14.2.6.14 ein neues Unterkapitel mit der Überschrift
"14.2.6.15 Use Case Selektieren per AID, first, Antwortdaten mit FCI"
und folgendem Inhalt eingefügt:

In dieser Variante enthält die APDU des SELECT-Kommandos fünf Parameter:

(N047.350) K_externeWelt {K_Karte}
Der Parameter selectionMode bestimmt die Art der Suche. Für diesen Use Case MUSS selectionMode = '04' gewählt werden.

(N047.352) K_externeWelt {K_Karte}
Der Parameter fileOccurrence bestimmt, welches File aus einer Liste von passenden Files gefunden wird. Für diesen Use Case MUSS fileOccurrence = '0' gewählt werden.

(N047.354) K_externeWelt {K_Karte}
Der Parameter aid MUSS einen Oktettstring gemäß (N010.200) oder dessen Anfang enthalten. Im Objektsystem wird nach einem Ordner mit dazu passendem Attribut applicationIdentifier gesucht.

(N047.356) K_externeWelt {K_Karte}
Der Parameter responseType bestimmt die Art der Antwortdaten. Für diesen Use Case MUSS responseType = '00' gewählt werden.

(N047.358) K_externeWelt {K_Karte}
Der Parameter length bestimmt die Länge der erwarteten Antwortdaten. Der Wert von length MUSS gleich WildCardShort sein.<=

(N047.360) K_externeWelt {K_Karte}
Es MUSS eine Case 4S Kommando-APDU gemäß 11.7.4.1 über die Schnittstelle "Interpreter" in Abbildung 1 geschickt werden. Für die Konstruktion dieser Case 4 Kommando-APDU MÜSSEN die Angaben aus Tabelle CosT_812 verwendet werden.

Tabelle CosT_812: SELECT, AID, first occurrence, Antwortdaten mit FCI

	Inhalt	Beschreibung
CLA	'00'	CLA-Byte gemäß [ISO/IEC 7816-4]
INS	'A4'	Instruction Byte gemäß [ISO/IEC 7816-4]
P1	'04'	*selectionMode* = Ordnerselektion mit *applicationIdentifier*
P2	'00'	*fileOccurrence* + *responseType* = first occurrence, Antwortdaten mit FCI
Data	'XX…XX'	*aid*, Oktettstring, Anzahl Oktette aus dem Intervall [1, 16]
Le	'00'	*length*, Anzahl der erwarteten Oktette in den Antwortdaten

2.2 Änderung 2: Zusammenfassung der SELECT-Varianten

In 14.2.6.15 wird für den Parameter P2 die Wert '00' mit der Bedeutung "first occurrence, Antwortdaten mit FCI" ergänzt.

2.3 Änderung 3: Liste der normativ geforderten Varianten

In (N047.500)a wird der Liste der normativ geforderten SELECT-Varianten die Variante aus Änderung 1 hinzugefügt.

2.4 Änderung 4: Kommandobearbeitung

Der Anforderungstext (N048.300)b wird editorisch umgeformt und eine neue Anforderung (N048.300)c wird erstellt. Insgesamt ändert sich (N048.300) damit wie folgt:

(N048.300) K_COS

Für das Datenfeld rspData der Antwortnachricht gilt:

a. Wenn P2 einen Wert aus der Menge {´04´, ´06´} hat, genau dann MUSS das Datenfeld rspData der Antwortnachricht die File Control Parameter gemäß 8.3.3 wie folgt enthalten: Sei FCP ein Oktettstring, der die File Control Parameter gemäß 8.3.3 enthält, dann gilt: Falls OctetLength(FCP)

   1. kleiner Nr gemäß (N027.200): rspData = FCP.
   2. sonst rspData = Extract_MSByte(FCP, Nr).

b. ~~Andernfalls fehlt das Datenfeld der Antwortnachricht.~~
Wenn P2 einen Wert aus der Menge {'0C, '0E'} hat, dann MUSS das Datenfeld rspData der Antwortnachricht fehlen.

c. Wenn P2 einen Wert aus der Menge {'00"} hat, genau dann MUSS das Datenfeld rspData der Antwortnachricht die File Control Information (FCI) wie folgt enthalten:

   1. Die File Control Information (FCI) sind ein DER-codiertes Datenobjekt mit Tag '6F'.
   2. Die Anzahl der Oktette im Datenfeld *rspData* der Antwortnachricht ist kleiner gleich 256 (short length und FCI vollständig in *rspData* enthalten).
   3. Die FCI enthalten mindestens ein DO'84' mit dem Attribut *applicationIdentifier*, dessentwegen dieser Ordner ausgewählt wurde. Es ist zulässig, dass die FCI mehrere DO'84' enthalten.
   4. Die FCI enthalten ein DO'A5', für das gilt:

i. Das DO'A5' enthält ein DO'9F65'. Das Wertfeld des DO'9F65' enthält eine Zahl *maxLc* in zwei Oktetten gemäß I2OS(*maxLc*, 2). Die Zahl *maxLc* ist größer gleich 1024 (vergleiche (N029.890)a.3) und kleiner als die maximal vom COS unterstützte Länge einer geschützten Kommandonachricht.

ii. Es ist zulässig, dass das DO'A5' stets wie folgt codiert wird:
'A5 – 05 – (9F65 – 02 – 0400) '

iii. Es ist zulässig, dass das DO'A5' weitere Datenobjekte enthält.

5. Es ist zulässig, dass FCI weitere Datenobjekte enthält.

3 Literaturstellen

[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS), Elektrische Schnittstelle Version 3.12.0 vom 15.05.2019
[GPC_SPE_034]	GlobalPlatform Technology, Card Specification, Version 2.3.1, Public Release, March 2018
[ISO/IEC 7816–4]	Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange, third edition, 2013