Anlage zu C_6978
Diverse technische Änderungen ohne Auswirkungen auf COS-Implementierung

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

1 Farbliche Markierung von Änderungen

Dieses Kapitel erläutert den Farbcode der farblichen Hinterlegung von Änderungen beim Vergleich von [gemSpec_COS] in der Version 3.12.0 vom 15.05.2019 gegenüber der aktuellen Version.

1) **blaue Hinterlegung:** Editorielle Änderungen, die sich weder auf Implementierungen durch Hersteller, noch auf Testimplementierungen auswirken.
2) **gelbe Hinterlegung:** Änderungen, die sich nicht auf die Implementierung durch Hersteller, wohl aber auf gematik Artefakte (Spezifikationen, Testimplementierung, …) auswirken.
3) **orange Hinterlegung:** Änderungen, die sich auf die Implementierung durch Hersteller und / oder die gematik Artefakte auswirken.

Es ergibt sich eine Kritikalität von niedrig=ohne über blau, gelb nach orange. Im Zweifelsfall wird für eine höhere Kritikalität, also eine stärkere Warnfarbe gewählt.

2 Änderungen

1) Ort (N012.200)a
   a) Die obere Intervallgrenze wird geändert:

   (N012.200)a K_Anwendungsspezifikation {K_Karte}
   Ein strukturiertes EF MUSS ein Attribut *recordList* vom Typ Liste mit einer Anzahl der Listenelemente aus dem Intervall [0, ~~254~~ *maximumNumberOfRecords*] und vom Typ Rekord besitzen.

   b) Begründung: Korrektur.

2) Ort CosK_5a6, Anforderungen an linear variable EF
   a) Es werden zwei neue Anforderungen aufgenommen:

   (N013.050) K_Anwendungsspezifikation {K_Karte}
   KEIN *record* in *recordList* DARF mehr als *maximumRecordLength* Oktette besitzen.

   (N013.060) K_Anwendungsspezifikation {K_Karte}
   Die Summe der Längen in Oktett aller Elemente in *recordList* MUSS kleiner gleich *numberOfOctet* sein.

   b) Begründung: Beseitigung einer Spezifikationslücke.

3) Ort (N014.000)b
   a) Eine an das COS gerichtete Afo vom Typ "egal" wurde umgeformt in eine "MUSS" Afo an die externe Welt:

   (N014.000)b K_externeWelt {K_Karte}
   ~~Das Wertfeld KANN eine beliebige Länge besitzen.~~ Die externe Welt MUSS beliebige Längen des DO_Size akzeptieren.

   b) Begründung: Die Erwartungshaltung an die externe Welt wird besser beschrieben.

4) Ort (N014.700)b
   a) Eine an das COS gerichtete Afo vom Typ "egal" wurde umgeformt in eine "MUSS" Afo an die externe Welt:

   (N014.700)b K_externeWelt {K_Karte}
   ~~Das Wertfeld KANN eine beliebige Länge besitzen.~~ Die externe Welt MUSS beliebige Längen des DO_ReadSize akzeptieren.

   b) Begründung: Die Erwartungshaltung an die externe Welt wird besser beschrieben.

5) Ort (N014.900)a

a) Eine an das COS gerichtete Afo vom Typ "egal" wurde umgeformt in eine "MUSS" Afo an die externe Welt:

(N014.900)a K_externeWelt {K_Karte}
~~Für die Reihenfolge der Datenobjekte in DO_FCP gilt: Die Reihenfolge aller Datenobjekte ist herstellerspezifisch.~~ Die externe Welt MUSS jede beliebige Reihenfolge der DO in DO_FCP akzeptieren. <=

b) Begründung: Die Erwartungshaltung an die externe Welt wird besser beschrieben.

6) Ort Einleitung zu CosK_afb
   a) Art: Der Text wird geändert:

8.6 Schlüsselobjekt (normativ)

Dieses Unterkapitel beschreibt Schlüsselobjekte, die im Rahmen kryptographischer Operationen zum Einsatz kommen. Der Terminus Schlüsselobjekt dient in diesem Dokument als Oberbegriff für symmetrische, private und öffentliche Schlüsselobjekte.

Symmetrische Schlüssel werden in diesem Dokument zu folgenden Zwecken eingesetzt:

~~1. Mit persistent gespeichertem Geheimnis (Schlüssel) zur einseitigen Authentisierung (siehe 15.1.1).~~

1. Mit persistent gespeichertem Geheimnis (Schlüssel) zur gegenseitigen Authentisierung bei gleichzeitiger Aushandlung von Sessionkeys (siehe 15.4.1 und 15.4.2).
2. Mit persistent gespeichertem Geheimnis (Schlüssel) zur gegenseitigen Authentisierung bei gleichzeitiger Übertragung von Sessionkeys (siehe 15.5).
3. Als Sessionkey zur Sicherstellung einer vertraulichen Kommunikation.
4. Als Sessionkey zur Sicherstellung einer integren und authentischen Kommunikation.

Private Schlüssel werden in diesem Dokument zu folgenden Zwecken eingesetzt:

5. Berechnung elektronischer Signaturen (siehe 14.8.2)
6. Entschlüsselung von Daten (siehe 14.8.3)
7. Nachweis der Authentizität dieser Karte (siehe 15.2)
8. Transportsicherung von Sessionkey Material (siehe 15.5 und (N085.068)b.7.viii ~~(N084.400)c~~)

Öffentliche Schlüssel werden in diesem Dokument zu folgenden Zwecken eingesetzt:

9. Prüfen elektronischer Signaturen beim Import von Zertifikaten (siehe (N095.900))
10. Prüfen von Signaturen im Rahmen von Rollenauthentisierungen (siehe (N084.400))
11. Transportsicherung von Sessionkey Material (siehe 15.5 und (N085.068)b.7.viii ~~(N086.900)d~~)
12. Verschlüsseln von Daten (siehe 14.8.4)

   b) Begründung: Aktualisierung.

7) Ort (N019.900)e.2 und (N019.900)f
   a) Das RFC Wort wird von SOLL auf MUSS geändert.

(N019.900)e.2 K_Anwendungsspezifikation {K_Karte}
Die Anwendungsspezifikation ~~SOLL~~ MUSS eine Anzahl an Listenelementen für *persistentCache* vorgeschreiben, die mindestens zu unterstützen ist. <=

(N019.900)f K_Anwendungsspezifikation {K_Karte}
Die Anwendungsspezifikation ~~SOLL~~ MUSS eine Anzahl an Listenelementen für *persistentPublicKeyList* vorgeschreiben, die mindestens zu unterstützten ist. <=

   b) Begründung: Präzisierung, was genau von einem Prüfling gefordert wird.

8) Dieser Punkt ist absichtlich leer.
9) Ort Kapitel 10.5
   a) Das Kapitel wird ersatzlos gestrichen.
   b) Begründung: Die Anforderungen bilden eine Untermenge der Anforderungen aus der Warp-per-Spezifikation gemSpec_COS-Wrapper und sind deshalb hier überflüssig.
10) Ort (N023.920)f.2
   a) Der Anforderungstext wird umformuliert.

(N023.920)f.2 K_COS
~~Die Deaktivierung KANN auf andere Art erfolgen.~~ Das COS MUSS so robust sein, dass eine Deaktivierung möglich ist, die von den Vorgaben aus [EMV®_Book-1#6.1.5] abweicht (beispielsweise "Karte ziehen"). <=

   b) Begründung: Präzisierung des gewünschten Verhaltens.

11) Ort (N026.910), (N027.010), (N029.874)
   a) Verschärfung des RFC-Wortes

(N026.910) K_externeWelt {K_Karte}
Der Sender einer Kommando-APDU ~~SOLL~~MUSS die Längenbeschränkung durch passende Wahl von Nc einhalten.

(N027.010) K_externeWelt {K_Karte}
Der Sender einer Kommando-APDU ~~SOLL~~MUSS die Längenbeschränkung durch passende Wahl von Ne einhalten.

(N029.874) K_externeWelt {K_Karte}
Die konsekutive Folge einer Command-Chaining-Sequenz ~~SOLL~~DARF an der Schnittstelle "Interface I/O" aus CosA_e09 NICHT
a. durch Kommandos unterbrochen werden, welche nicht zu dieser Sequenz gehören oder
b. durch eine Deaktivierung unterbrochen werden.

b) Begründung: Aus Interoperabilitätssicht und für einen stabilen Regelbetrieb ist eine MUSS Anforderung besser geeignet, die keine Ausnahmen zulässt.

12) Ort (N037.800)b.1
a) Der Text wird geändert:

(N037.800)b.1 K_COS
Wenn *affectedObject* ~~vom Typ Symmetrisches Authentisierungsobjekt oder Passwortobjekt~~ nicht vom Typ Ordner oder Datei ist, dann SOLL vormals von diesem Objekt allokierter Speicher so freigegeben werden, dass er zum Anlegen anderer Objekte verwendbar ist.

b) Begründung: Beseitigung einer Spezifikationslücke, es fehlten öffentliches Schlüsselobjekt und symmetrisches Verbindungsobjekt

13) Ort (N085.041)
a) Die Längenangabe eines TLV-Objektes wird geändert

(N085.041) K_externeWelt {K_Karte}
Es MUSS eine Case 3S Kommando-APDU gemäß CosK_d
Für die Konstruktion dieser Case 3 Kommando-APDU MÜS

Tabelle 245, CosT_45a: GENERAL AUTHENTI

	Inhalt	Beschreibung
CLA	'00'	CLA-Byte gemäß [ISO/IE
INS	'86'	Instruction Byte gemäß [I
P1	'00'	no information given
P2	'00'	no information given
Data	'XX…XX'	'7C – 81F8 – (82 – 81F '7C – 820139 – (82 – 820 '7C – ~~82013B~~ 82017B – (

b) Begründung: Korrektur.

14) Ort (N106.100)
a) Die Referenz auf GET CHALLENGE wird geändert.

(N106.100) K_externeWelt {K_Karte}
Das erste Kommando der Sequenz MUSS GET CHALLENGE gemäß ~~14.9.4.1~~ (N098.625) sein und über Channel_b zum COSb geschickt werden. Die dabei vom COSb erzeugte Zufallszahl wird mit R1 bezeichnet.

b) Begründung: Korrektur, Präzisierung

3 Literaturstellen

[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS), Elektrische Schnittstelle