1 Änderung in gemSpec_Basis_KTR_Consumer

1.1 In Kapitel 2 "Systemüberblick":

Änderung des Freitextes:

...

Der Basis-Consumer ermöglicht es den Gesellschaftern der gematik sowie den durch sie vertretenen Organisationen, als Nutzer an der TI teilzunehmen. Der Zugriff auf Fachanwendungen der TI ist dieser Nutzergruppe nicht gestattet. Der Produkttyp enthält demnach zwar keine Fachmodule, aber ein Clientmodul KOM-LE zur Nutzung des sicheren Übermittlungsverfahrens. Auf technischer Ebene wird die jeweilige Nutzergruppe durch die kryptographische Identität der SMC-B Org oder SMC-B KTR (jeweils auf Basis oid_kostenträger) identifiziert, die in einem HSM ~~oder auf einer Karte~~ gespeichert wird.

...

1.2 In Kapitel 5.3 "Identitäten":

Änderung des Freitextes:

Im Basis- und KTR-Consumer werden private Schlüssel der SMC-B in einem HSM gespeichert.~~Im Basis-Consumer werden private Schlüssel der SMC-B in einem HSM oder auf einer SMC-B in Kartenform gespeichert. Das Schlüsselmaterial des KOM-LE-Clientmoduls hingegen wird auch hier in einem HSM gespeichert.~~

Nachfolgend wird festgelegt, welche Qualitäten dabei erreicht werden müssen und was bei der Personalisierung zu beachten ist.

Die Anforderung A_18195 wird **entfernt**:

A_18195 - Basis-Consumer mit SMC-B
Der Basis-Consumer KANN privates Schlüsselmaterial einer SMC-B in Kartenform nutzen.**[<=]**

Die Anforderung A_18196 wird **entfernt**:

A_18196 - Personalisierung des HSM beim Basis-Consumer
Der Anbieter eines Basis-Consumers, der ausschließlich mit SMC-Bs in Kartenform arbeitet, KANN auf einen Prozess zur Personalisierung der Identitäten der SMC-B im HSM verzichten.**[<=]**

1.3 In Kapitel 6.6 "Realisierung der Leistung der TI-Plattform":

Das gesamte Kapitel mitsamt seinen Unterkapiteln, Anforderungen und Freitexten wird **entfernt**.

Die Anforderung A_18130 wird **entfernt**:

A_18130 - Nutzung von PL_TUC_CARD Systemprozessen
Der Basis-Consumer MUSS für den Zugriff auf Smartcards die in TAB_Systemprozesse mit PL_TUC_CARD_* bezeichneten Systemprozesse benutzen.
[<=]

1.3.1 In Kapitel 6.6.1 "Transportschnittstelle für Kartenkommandos":

Das gesamte Unterkapitel mitsamt seinen Unterkapiteln, Anforderungen und Freitexten wird **entfernt**.

~~Wenn der Basis-Consumer Smartcards unterstützt, muss er eine Schnittstelle zu Karten der TI über ein Kartenterminal herstellen. Diese Schnittstelle muss die von den Plattformprozessen erzeugten, kartenverständlichen APDUs an die Karte übertragen. Neben proprietären Schnittstellentreibern von Kartenterminalherstellern existiert eine Reihe standardisierter Schnittstellen, die auch von verschiedenen Betriebssystemen zur Anbindung handelsüblicher Kartenterminals unterstützt werden.~~

~~Die folgenden Anforderungen betreffen die gemäß [gemSpec_Systemprozesse_dezTI#ENV_TUC_CARD_APDU_TRANSPORT] zu beschreibende Transportschnittstelle.~~

Die Anforderung A_18166 wird **entfernt**:

A_18166 - Vertrauliche und integritätsgeschützte Kommunikation mit KT
Wenn der Basis-Consumer Smartcards unterstützt, MUSS der Basis-Consumer mit dem Kartenterminal ausschließlich über eine vertrauliche, integritätsgeschützte Verbindung kommunizieren.**[<=]**

Die Anforderung A_18097 wird **entfernt**:

A_18097 - Transportschnittstelle für Kartenkommandos
Wenn der Basis-Consumer Smartcards unterstützt, MUSS er eine sichere Transportschnittstelle für die Übertragung von Smartcard-APDUs gemäß [CT-API] implementieren.**[<=]**

Die Anforderung A_18100 wird **entfernt**:

A_18100 - Ergänzende Standards für Transportschnittstelle
Der Basis-Consumer KANN eine Transportschnittstelle für die Übertragung von SmartCard-APDUs auf Basis des SICCT-Protokolls gemäß [CCID] und unter Verwendung der vom Hersteller des Kartenterminals ggf. bereitgestellten Hardwaretreiber implementieren.**[<=]**

Die Anforderung A_18163 wird **entfernt**:

A_18163 - Kartenterminal für Basis-Consumer
Wenn der Basis-Consumer Smartcards unterstützt, MUSS er mindestens ein Kartenterminal enthalten.
[<=]

Die Anforderung A_18102 wird **entfernt**:

A_18102 - PIN-Eingabe nicht speichern
Der Basis-Consumer DARF ein eingegebenes PIN-Geheimnis NICHT speichern.**[<=]**

Die Anforderung A_18103 wird **entfernt**:

A_18103 - PIN-Geheimnis ausschließlich an Karte übermitteln
Der Basis-Consumer MUSS sicherstellen, dass das eingegebene PIN-Geheimnis ausschließlich an die Karte und nicht an andere Adressaten übermittelt wird.
[<=]

1.3.2 In Kapitel 6.6.2 "Schnittstelle für PIN-Operationen und Anbindung der Karten an die TI":

Das gesamte Unterkapitel mitsamt seinen Unterkapiteln, Anforderungen und Freitexten wird **entfernt**.

~~Anwendungsfälle zur PIN-Verwaltung, zur Kartenfreischaltung oder weiterer Fachanwendungen können die Eingabe eines PIN- oder PUK-Geheimnisses erfordern. Der Zugriff auf Karten der TI erfolgt über die Systemprozesse PL_TUC_CARD_*. Der Basis-Consumer als Realisierungsumgebung der Systemprozesse muss seinerseits die von der Plattform geforderten Schnittstellen gemäß [gemSpec_Systemprozesse_dezTI#ENV_TUC_CARD_SECRET_INPUT] implementieren, um die Kommunikation der Plattform mit dem Benutzer zu ermöglichen.~~

~~Die Kommunikationsschnittstelle ist in Kapitel 6.6.1 Transportschnittstelle für Kartenkommandos beschrieben und umfasst das Kartenterminal, Eingabemedium und Hinweistexte an den Benutzer. Diese kann je nach Konfiguration an einem Gerät als Kartenterminal oder auch eine Kombination aus Bildschirmausgabe, Kartenterminal-PIN-Pad und/oder Tastatureingabe erfolgen.~~

Die Anforderung A_18107 wird **entfernt**:

A_18107 - Übergabeschnittstelle PIN/PUK-Geheimnis
Wenn der Basis-Consumer Smartcards unterstützt, MUSS er eine Operation gemäß [gemSpec_Systemprozesse_dezTI#ENV_TUC_CARD_SECRET_INPUT] zur Eingabe eines PIN/PUK-Geheimnisses und Weiterleitung an eine Smartcard mit folgenden Parametern implementieren:
Eingabeparameter:

- Identifikator
- Aktion
- minLength
- maxLength
- commandApduPart

Rückgabewerte

- responseApdu

[<=]

Die Anforderung A_18108 wird **entfernt**:

A_18108 - Umsetzung ENV_TUC_CARD_SECRET_INPUT
Wenn der Basis-Consumer Smartcards unterstützt, MUSS er die Abbildung der Eingabeparameter auf die Rückgabewerte der Operation ENV_TUC_SECRET_INPUT derart umsetzen, dass

- die Eingabeparameter `Identifikator` und `Aktion` für einen Hinweistext an den Benutzer verwendet werden, welche Aktion auf welchem konkreten Kartenobjekt (z.B. Name einer PIN) durchgeführt wird,

- der `commandApduPart` an der Eingabeschnittstelle um das Benutzergeheimnis ergänzt wird,
- der `commandApduPart` über die Transportschnittstelle für Kartenkommandos an die Karte gesendet wird

und die Antwortnachricht der Karte als responseApdu an den Aufrufer zur Auswertung zurückgegeben wird.
[<=]

Die Anforderung A_18109 wird **entfernt**:

A_18109 - Minimalprinzip Karteninteraktion
Der Basis-Consumer DARF ein Kartenkommando NICHT an eine angebundene Karte weiterleiten, wenn dies nicht explizit im Kontext eines Anwendungsfalls (intendierte Kartenoperationen und Erhöhen des Sicherheitszustands der Karte, falls erforderlich) erforderlich ist.**[<=]**

1.4 In Kapitel 7.5.2 "Weitere Dokumente":

Kartenspezifische Einträge in der Tabelle werden entfernt, da nicht mehr relevant.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI-TR-03111]	BSI TR-31111: Elliptic Curve Cryptography, Version 2.10, Juni 2018
[RFC1939]	RFC 1939: Post Office Protocol – Version 3, J. Myers, M. Rose, Mai 1996
[RFC2045]	RFC 2045: Multipurpose Internet Mail Extension (MIME) Part One: Format of Internet Message Bodies, N. Freed, N. Borenstein, November 1996
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner
[RFC4511]	RFC 4511: Lightweight Directory Access Protocol (LDAP), J. Sermersheim, Juni 2006
[RFC4954]	RFC 4954: SMTP Service Extension for Authentication, R. Siemborski, A. Melnikov, März 2007
[RFC5083]	RFC 5083: Authenticated-Enveloped-Data Content Type, R.Housley, November 2007
[RFC5321]	RFC 5321: Simple Mail Transfer Protocol, J. Klensin, Oktober 2008
[RFC5652]	RFC 5652: Cryptographic Message Syntax (CMS), R. Housley, September 2009
[RFC5751]	RFC 5751: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, B. Ramsdell, S. Turner, Januar 2010
[RFC1812]	RFC 1812: Requirements for IP Version 4 Routers, Juni 1995

[RFC2644]	RFC 2644: Changing the Default for Directed Broadcasts in Routers, August 1999
[RFC791]	RFC 791: Internet Protocol, September 1981
[RFC3022]	RFC 3022: Traditional IP Network Address Translator (Traditional NAT), Januar 2001
[RFC1918]	RFC 1918: Address Allocation for Private Internets, Februar 1996
[RFC6598]	RFC 6598: IANA-Reserved IPv4 Prefix for Shared Address Spac, April 2012
[OASIS-DSS]	OASIS: Digital Signature Service Core Protocols, Elements, and Bindings, Version 1.0, OASIS Standard, via http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf
[OASIS-SP]	OASIS: Signature Policy Profile of the OASIS Digital Signature Services Version 1.0, Committee Draft 01, 18 May 2009, http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy-cd01.pdf
[OASIS-VR]	OASIS: Profile for comprehensive multi-signature verification reports for OASIS Digital Signature Services Version 1.0, Committee Specification 01, 12 November 2010, http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cs01.pdf
[XMLEnc]	XML Encryption Syntax and Processing W3C Recommendation 11 April 2013 http://www.w3.org/TR/xmlenc-core1/
[XPATH]	W3C Recommendation (14 December 2010) XML Path Language (XPath) 2.0 (Second Edition) http://www.w3.org/TR/2010/REC-xpath20-20101214/
[CMS]	Cryptographic Message Syntax (CMS), September 2009 http://tools.ietf.org/html/rfc5652
[Canon XML1.1]	Canonical XML Version 1.1 http://www.w3.org/TR/2008/REC-xml-c14n11-20080502/
[CAdES]	ETSI: Electronic Signature Formats, Electronic Signatures and Infrastructures (ESI) – Technical Specification, ETSI TS 101 733 V2.2.1, 2008-07, via http://www.etsi.org
~~[CT-API]~~	~~https://www.tuvit.de/de/aktuelles/beitraege-white-paper/card-terminal-application-programing-interface-fuer-chipkartenanwendungen//~~
~~[CCID]~~	~~https://usb.org.10-1-108-210.causewaynow.com/sites/default/files/DWG_Smart-Card_CCID_Rev110.pdf~~

1.5 In TAB_Systemprozesse:

Einträge in der Tabelle mit "PL_TUC_CARD_*" werden entfernt, da nicht mehr relevant.

Tabelle 1: TAB_Systemprozesse – Verwendete Plattformleistungen

Kürzel	Bezeichnung
PL_TUC_HYBRID_DECIPHER	Hybrid entschlüsseln
PL_TUC_HYBRID_ENCIPHER	Hybrid verschlüsseln
PL_TUC_SIGN_DOCUMENT_nonQES	Dokument nonQES signieren
PL_TUC_SIGN_HASH_nonQES	mit Karten-Identität signieren
PL_TUC_VERIFY_DOCUMENT_nonQES	nonQES Dokumentensignatur verifizieren
PL_TUC_PKI_VERIFY_CERTIFICATE	Prüfung eines Zertifikats der TI
PL_TUC_VZD_BIND	Verbindung aufbauen
PL_TUC_VZD_UNBIND	Verbindung trennen
PL_TUC_VZD_SEARCH	Verzeichnis abfragen
PL_TUC_VZD_ABANDON	Verzeichnisabfrage abbrechen
PL_TUC_NET_SYNC_TIME	Zeit synchronisieren
~~PL_TUC_CARD_INFORMATION~~	~~gesammelte Statusinformationen zu einer Karte~~
~~PL_TUC_CARD_RESET~~	~~Rücksetzen einer Karte~~
~~PL_TUC_CARD_CHANGE_PIN~~	~~PIN ändern~~
~~PL_TUC_CARD_ENABLE_PIN~~	~~PIN-Schutz einschalten~~
~~PL_TUC_CARD_DISABLE_PIN~~	~~PIN-Schutz abschalten~~
~~PL_TUC_CARD_VERIFY_PIN~~	~~Benutzer verifizieren~~

~~PL_TUC_CARD_ACTIVATE_APPLICATION~~	~~Anwendung aktivieren~~
~~PL_TUC_CARD_DEACTIVATE_APPLICATION~~	~~Anwendung deaktivieren~~
~~PL_TUC_CARD_GET_CHALLENGE~~	~~Auslesen einer Zufallszahl~~