

## Elektronische Gesundheitskarte und Telematikinfrastruktur

# Spezifikation Basis- und KTR-Consumer

Version: [1.23.0 CC](#)  
Revision: [241913266650](#)  
Stand: [30.0605.08.2020](#)  
Status: [zur Abstimmung](#) freigegeben  
Klassifizierung: Öffentlich [Entwurf](#)  
Referenzierung: gemSpec\_Basis\_KTR\_Consumer

## 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	15.05.19		initiale Erstellung des Dokuments	gematik
1.1.0	28.06.19		Einarbeitung P19.1	gematik
1.2.0	30.06. <del>2020</del> <u>20</u>		Einarbeitung P22.1	gematik
<u>1.3.0 CC</u>	<u>05.08.20</u>		<u>Einarbeitung P22.3</u>	<u>gematik</u>

36

## Inhaltsverzeichnis

37	<b>1 Einordnung des Dokumentes .....</b>	<b>7</b>
38	<b>1.1 Zielsetzung .....</b>	<b>7</b>
39	<b>1.2 Zielgruppe .....</b>	<b>7</b>
40	<b>1.3 Geltungsbereich .....</b>	<b>7</b>
41	<b>1.4 Abgrenzungen .....</b>	<b>7</b>
42	<b>1.5 Methodik .....</b>	<b>8</b>
43	<b>2 Systemüberblick .....</b>	<b>9</b>
44	<b>3 Systemkontext .....</b>	<b>10</b>
45	<b>4 Zerlegung der Produkttypen .....</b>	<b>11</b>
46	<b>4.1 Basisfunktionen .....</b>	<b>11</b>
47	<b>4.2 LDAP Proxy .....</b>	<b>11</b>
48	<b>4.3 Clientmodul KOM-LE .....</b>	<b>11</b>
49	<b>5 Übergreifende Festlegungen .....</b>	<b>13</b>
50	<b>5.1 Anschluss an die TI .....</b>	<b>13</b>
51	5.1.1 Anbindung per LAN/WAN .....	13
52	5.1.1.1 Funktionsmerkmalweite Aspekte .....	13
53	5.1.1.1.1 Netzwerksegmentierung .....	13
54	5.1.1.2 Durch Ereignisse ausgelöste Reaktionen .....	16
55	5.1.2 Zeitdienst .....	17
56	5.1.3 Namensdienst und Dienstlokalisierung .....	17
57	5.1.3.1 Funktionsmerkmalweite Aspekte .....	17
58	5.1.3.2 Interne TUCs, auch durch Fachmodule nutzbar .....	18
59	5.1.3.2.1 TUC_CON_362 „Liste der Dienste abrufen“ .....	18
60	5.1.3.3 Operationen an der Außenschnittstelle .....	19
61	5.1.3.4 Betriebsaspekte .....	19
62	<b>5.2 Sicherheit .....</b>	<b>20</b>
63	<b>5.3 Identitäten .....</b>	<b>20</b>
64	<b>5.4 Schnittstellen .....</b>	<b>22</b>
65	<b>6 Funktionsmerkmale .....</b>	<b>23</b>
66	<b>6.1 Verschlüsselungsdienst .....</b>	<b>23</b>
67	6.1.1 Durch Module nutzbare TUCs .....	23
68	6.1.2 Operationen an der Clientschnittstelle .....	23
69	6.1.2.1 EncryptDocument .....	24
70	6.1.2.2 DecryptDocument .....	27
71	<b>6.2 Signaturdienst .....</b>	<b>29</b>
72	6.2.1 Durch Module nutzbare TUCs .....	29

73	6.2.2 Operationen an der Clientschnittstelle.....	30
74	6.2.2.1 SignDocument .....	30
75	6.2.2.2 VerifyDocument .....	36
76	6.2.2.3 ExternalAuthenticate .....	40
77	<b>6.3 Zertifikatsdienst .....</b>	<b>43</b>
78	6.3.1 Durch Module nutzbare TUCs .....	43
79	6.3.2 Operationen an der Clientschnittstelle.....	43
80	6.3.2.1 VerifyCertificate .....	43
81	<b>6.4 LDAP-Proxy .....</b>	<b>46</b>
82	6.4.1 Durch Module nutzbare TUCs .....	46
83	6.4.2 Unterstützte LDAPv3-Operationen an der Clientschnittstelle .....	47
84	<b>6.5 Clientmodul KOM-LE .....</b>	<b>47</b>
85	6.5.1 Allgemeine Anforderungen .....	47
86	6.5.2 Senden von Nachrichten .....	48
87	6.5.3 Empfangen von Nachrichten .....	50
88	<b>6.6 Realisierung der Leistungen der TI-Plattform .....</b>	<b>52</b>
89	6.6.1 Transportschnittstelle für Kartenkommandos .....	52
90	6.6.2 Schnittstelle für PIN-Operationen und Anbindung der Karten der TI .....	53
91	<b>7 Anhang A – Verzeichnisse .....</b>	<b>55</b>
92	7.1 Abkürzungen .....	55
93	7.2 Glossar .....	56
94	7.3 Abbildungsverzeichnis .....	56
95	7.4 Tabellenverzeichnis .....	56
96	7.5 Referenzierte Dokumente .....	58
97	7.5.1 Dokumente der gematik .....	58
98	7.5.2 Weitere Dokumente .....	58
99	<b>8 Anhang B – Übersicht über die verwendeten Versionen .....</b>	<b>61</b>
100	<b>9 Anhang C – Übersicht der genutzten Systemprozesse .....</b>	<b>62</b>
101	<b>1 Einordnung des Dokumentes .....</b>	<b>7</b>
102	1.1 Zielsetzung .....	7
103	1.2 Zielgruppe .....	7
104	1.3 Geltungsbereich .....	7
105	1.4 Abgrenzungen .....	7
106	1.5 Methodik .....	8
107	<b>2 Systemüberblick .....</b>	<b>9</b>
108	<b>3 Systemkontext .....</b>	<b>10</b>
109	<b>4 Zerlegung der Produkttypen .....</b>	<b>11</b>
110	4.1 Basisfunktionen .....	11

111	<b>4.2 LDAP-Proxy .....</b>	<b>11</b>
112	<b>4.3 Clientmodul KOM-LE .....</b>	<b>11</b>
113	<b>5 Übergreifende Festlegungen .....</b>	<b>13</b>
114	<b>5.1 Anschluss an die TI .....</b>	<b>13</b>
115	5.1.1 Anbindung per LAN/WAN .....	13
116	5.1.1.1 Funktionsmerkmalweite Aspekte .....	13
117	5.1.1.1.1 Netzwerksegmentierung .....	13
118	5.1.1.2 Durch Ereignisse ausgelöste Reaktionen .....	16
119	5.1.2 Zeitdienst .....	17
120	5.1.3 Namensdienst und Dienstlokalisierung .....	17
121	5.1.3.1 Funktionsmerkmalweite Aspekte .....	17
122	5.1.3.2 Interne TUCs, auch durch Fachmodule nutzbar .....	18
123	5.1.3.2.1 TUC CON 362 „Liste der Dienste abrufen“ .....	18
124	5.1.3.3 Operationen an der Außenschnittstelle .....	19
125	5.1.3.4 Betriebsaspekte .....	19
126	<b>5.2 Sicherheit .....</b>	<b>20</b>
127	<b>5.3 Identitäten .....</b>	<b>20</b>
128	<b>5.4 Schnittstellen .....</b>	<b>22</b>
129	<b>6 Funktionsmerkmale .....</b>	<b>23</b>
130	<b>6.1 Verschlüsselungsdienst .....</b>	<b>23</b>
131	6.1.1 Durch Module nutzbare TUCs .....	23
132	6.1.2 Operationen an der Clientschnittstelle .....	23
133	6.1.2.1 EncryptDocument .....	24
134	6.1.2.2 DecryptDocument .....	27
135	<b>6.2 Signaturdienst .....</b>	<b>29</b>
136	6.2.1 Durch Module nutzbare TUCs .....	29
137	6.2.2 Operationen an der Clientschnittstelle .....	30
138	6.2.2.1 SignDocument .....	30
139	6.2.2.2 VerifyDocument .....	36
140	6.2.2.3 ExternalAuthenticate .....	40
141	<b>6.3 Zertifikatsdienst .....</b>	<b>43</b>
142	6.3.1 Durch Module nutzbare TUCs .....	43
143	6.3.2 Operationen an der Clientschnittstelle .....	43
144	6.3.2.1 VerifyCertificate .....	43
145	<b>6.4 LDAP-Proxy .....</b>	<b>46</b>
146	6.4.1 Durch Module nutzbare TUCs .....	46
147	6.4.2 Unterstützte LDAPv3-Operationen an der Clientschnittstelle .....	47
148	<b>6.5 Clientmodul KOM-LE .....</b>	<b>47</b>
149	6.5.1 Allgemeine Anforderungen .....	47
150	6.5.2 Senden von Nachrichten .....	48
151	6.5.3 Empfangen von Nachrichten .....	50
152	<b>6.6 Realisierung der Leistungen der TI-Plattform .....</b>	<b>52</b>
153	6.6.1 Transportschnittstelle für Kartenkommandos .....	52
154	6.6.2 Schnittstelle für PIN-Operationen und Anbindung der Karten der TI .....	53

155	<b><u>7 Anhang A - Verzeichnisse .....</u></b>	<b>55</b>
156	<b><u>7.1 Abkürzungen .....</u></b>	<b>55</b>
157	<b><u>7.2 Glossar .....</u></b>	<b>56</b>
158	<b><u>7.3 Abbildungsverzeichnis .....</u></b>	<b>56</b>
159	<b><u>7.4 Tabellenverzeichnis .....</u></b>	<b>56</b>
160	<b><u>7.5 Referenzierte Dokumente .....</u></b>	<b>58</b>
161	7.5.1 Dokumente der gematik.....	58
162	7.5.2 Weitere Dokumente.....	58
163	<b><u>8 Anhang B – Übersicht über die verwendeten Versionen.....</u></b>	<b>61</b>
164	<b><u>9 Anhang C – Übersicht der genutzten Systemprozesse .....</u></b>	<b>62</b>
165		

166

## 1 Einordnung des Dokumentes

### 1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen an Herstellung, Test und Betrieb der beiden Produkttypen Basis-Consumer und KTR-Consumer.

Der Basis-Consumer und der KTR-Consumer sind Produkttypen der TI-Plattform, die in der Rolle eines Consumers mit der Telematikinfrastruktur (TI) interagieren und dabei sowohl Anteile der TI-Plattform als auch Anteile des sicheren Übermittlungsverfahrens KOM-LE enthalten. Der KTR-Consumer enthält darüber hinaus auch Fachmodule, um den Nutzerkreis „Krankenkassen“ die Teilnahme an den für sie vorgesehenen Fachanwendungen der Telematikinfrastruktur zu ermöglichen.

### 1.2 Zielgruppe

Das Dokument ist maßgeblich für Anbieter und Hersteller des Produkttyps Basis- und KTR-Consumer sowie für Anbieter und Hersteller von Produkten, die die Schnittstellen des Produkttyps Basis- und KTR-Consumer nutzen.

### 1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren 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 Abgrenzungen

Spezifiziert werden in dem Dokument die von den Produkttypen Basis- und KTR-Consumer bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang A5).

202 Die vollständige Anforderungslage für die Produkttypen ergibt sich aus weiteren Konzept-  
203 und Spezifikationsdokumenten, diese sind in den Produkttypsteckbriefen des Produkttyps  
204 Basis- bzw. KTR-Consumer verzeichnet.

### 205 **1.5 Methodik**

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

210

211 Sie werden im Dokument wie folgt dargestellt:

212 **<AFO-ID> - <Titel der Afo>**

213 Text / Beschreibung

214 [**<=**]

215

216 Dabei umfasst die Anforderung sämtliche zwischen der ID und der Textmarke  
217 angeführten Inhalte.



218

---

## 2 Systemüberblick

---

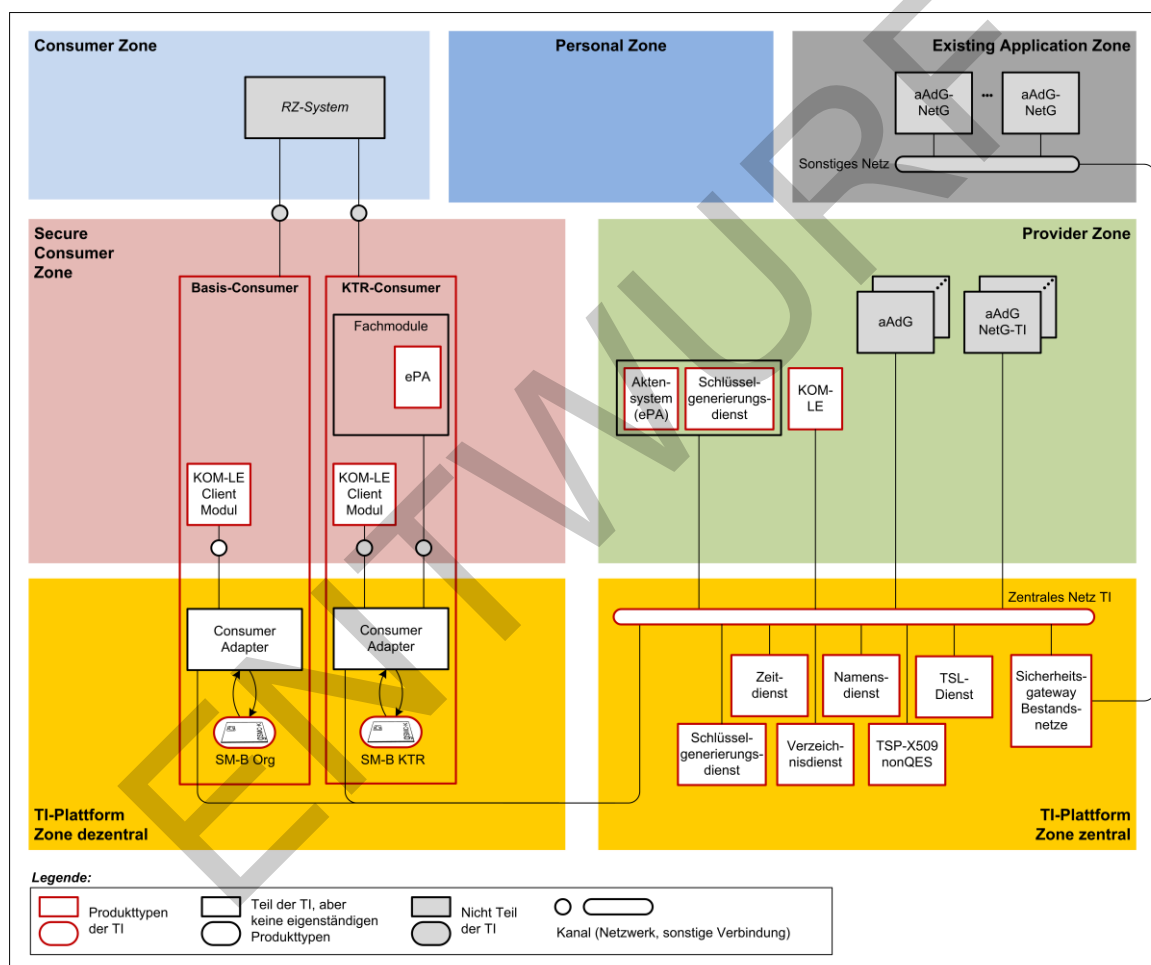
219 Die Produkttypen Basis- und KTR-Consumer sind beides Realisierungen des  
220 konzeptionellen Konstrukts „RZ-Consumer“ aus dem [gemKPT\_Arch\_TIP]. D.h., sie  
221 agieren als Consumer in der Telematikinfrastruktur (TI), nutzen dabei zentrale Dienste,  
222 die Dienste des sicheren Übermittlungsverfahrens und ggf. fachanwendungsspezifische  
223 Dienste und werden in einem Rechenzentrum entsprechend den Vorgaben der TI  
224 betrieben. Beide Produkttypen bieten für externe Clients eine Menge von Basisfunktionen  
225 (z.B. kryptographische Operationen), ermöglichen den Zugriff auf weitere Anwendungen  
226 des Gesundheitswesens und die Nutzung des sicheren Übermittlungsverfahrens KOM-LE.

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

234 Der KTR-Consumer ermöglicht es Krankenkassen, als Nutzer an der TI teilzunehmen.  
235 Genutzt werden können dabei Fachanwendungen, bei der die Krankenkassen als  
236 berechtigte Nutzer festgelegt sind (mit Ausnahme von VSDM), die sicheren  
237 Übermittlungsverfahren und die weiteren Anwendungen des Gesundheitswesens. Dieser  
238 Produkttyp enthält Fachmodule und ein Clientmodul KOM-LE zur Nutzung des sicheren  
239 Übermittlungsverfahrens. Auf technischer Ebene wird die Nutzergruppe durch die  
240 kryptographische Identität der SMC-B KTR identifiziert, die in einem HSM gespeichert  
241 wird.

### 3 Systemkontext

Nachfolgend wird angelehnt an den Systemüberblick aus [gemKPT\_Arch\_TIP] die Einbettung der Produkttypen Basis-Consumer und KTR-Consumer in das System der TI dargestellt. Die Darstellung ist reduziert auf die Produkttypen der TI sowie Clients und Anwendungen außerhalb der TI, mit denen potentiell eine Interaktion stattfindet. Die Festlegungen des vorliegenden Dokuments beziehen sich auf die Produkttypen Basis-Consumer und KTR-Consumer als Ganzes und das logische Konstrukt des Consumer-Adapters aus [gemKPT\_Arch\_TIP], das den Umfang der Basisfunktionen der Produkttypen festlegt.



FMC Block Diagram  
 TI Architektur – KTR-Consumer  
 Project: TI Architekturdarstellung  
 Author: WOC,PTA TEC/TN Date: 26.03.2019

**Abbildung 1: Systemkontext für Basis-/KTR-Consumer**

---

## 4 Zerlegung der Produkttypen

---

Der Produkttyp Basis-Consumer teilt sich in die folgenden Bestandteile auf:

- Basisfunktionen,
- LDAP-Proxy und
- Clientmodul KOM-LE

Der Produkttyp KTR-Consumer teilt sich in die folgenden Bestandteile auf:

- Basisfunktionen,
- LDAP-Proxy und
- Clientmodul KOM-LE
- Fachmodul ePA im KTR-Consumer

Die Festlegungen der vorliegenden Dokuments beziehen sich auf die Produkttypen Basis-Consumer und KTR-Consumer als Ganzes sowie deren oben aufgeführten Bestandteile, mit Ausnahme des Fachmoduls ePA, welches in [gemSpec\_FM\_ePA\_KTR\_Consumer] beschrieben wird. Das logische Konstrukt des Consumer-Adapters aus [gemKPT\_Arch\_TIP], wird durch die Basisfunktionen und den LDAP-Proxy in dem für die Produkttypen benötigten Umfang umgesetzt.

### 4.1 Basisfunktionen

Die Basisfunktionen enthalten:

- den Verschlüsselungsdienst zum Ver- und Entschlüsseln von Dokumenten
- den Signaturdienst zum Signieren und Signaturprüfen
- den Zertifikatsdienst, um Zertifikate zu überprüfen
- netztechnische Anbindung an die Telematikinfrastruktur (Interface, Firewall und DNS)

### 4.2 LDAP-Proxy

Der Basis- und KTR-Consumer ermöglicht es Clientsystemen und Clientmodulen durch Nutzung des LDAP-Proxies Daten aus dem Verzeichnisdienst der TI-Plattform (VZD) abzufragen. Die Kommunikation erfolgt über das LDAPv3-Protokoll.

### 4.3 Clientmodul KOM-LE

Der Basis- und KTR-Consumer enthält ein Clientmodul KOM-LE, um das sichere Übermittlungsverfahren KOM-LE nutzen zu können. Es werden die Anwendungsfälle „Senden und Empfangen von Nachrichten“ unterstützt. Die Spezifikation [gemSpec\_CM\_KOMLE] gilt in großen Teilen auch für den Basis- und KTR-Consumer. Es gibt aber verschiedene Bereiche, in denen eine Anpassung für den Basis- und KTR-Consumer erforderlich ist. Für diese Bereiche werden neue Anforderungen aufgenommen,

288 die statt der bestehenden Anforderungen aus [gemSpec\_CM\_KOMLE] zu verwenden sind.  
289 Die Bereiche sind:

- 290 • Nutzung des Basis- und KTR-Consumer  
291 Die Spezifikation des Clientmoduls [gemSpec\_CM\_KOMLE] schreibt an einigen  
292 Stellen die Nutzung des Konnektors für Signatur/Signaturprüfung und Ver-  
293 /Entschlüsselung vor. Diese Anforderungen werden ersetzt durch Anforderungen,  
294 die die Nutzung der Systemprozesse im Basis-/KTR-Consumer vorschreiben.
- 295 • Client-Schnittstelle des Moduls  
296 Die SMTP/POP3-Schnittstelle des Clientmoduls soll beibehalten werden.  
297 Abweichend von [gemSpec\_CM\_KOMLE] werden die Informationen bzgl. der  
298 Adresse und des Ports des Mail Transfer Agents (MTA, KOM-LE Fachdienst) und  
299 die Informationen des Aufrufkontext nicht beim Aufruf mitgegeben, sondern im  
300 Basis- und KTR-Consumer lokal konfiguriert.

ENTWURF

---

## 5 Übergreifende Festlegungen

---

### 5.1 Anschluss an die TI

#### 5.1.1 Anbindung per LAN/WAN

Unter Anbindung per LAN/WAN werden die Mechanismen beschrieben, mit denen der Basis- und KTR-Consumer auf der einen Seite in das lokale Netz der Einsatzumgebung und auf der anderen Seite in die zentrale TI und die aAdG und aAdG NetG-TI angebunden wird. Diese wesentlichen Aspekte betreffen Routing und Firewall.

##### 5.1.1.1 Funktionsmerkmalweite Aspekte

###### **A\_17396 - Verhalten als IPv4-Router**

Der Basis- und KTR-Consumer MUSS sich nach den in [RFC1812#1.1.3] definierten Rahmenbedingungen als IP-Version-4-(IPv4)-Router verhalten. Die in [RFC2644] geforderten Aktualisierungen zum [RFC1812] MÜSSEN umgesetzt werden. [≤]

###### **A\_17397 - IP-Pakete mit Source Route Option**

Der Basis- und KTR-Consumer DARF NICHT IP-Pakete mit gesetzter Source Route Option gemäß [RFC791] erzeugen oder weiterleiten. [≤]

###### **A\_17400 - NAT-Umsetzung**

Der Basis- und KTR-Consumer MUSS für die Kommunikation mit Adressbereichen der TI und aAdG und aAdG NetG-TI eine Network Address Translation (NAT) gemäß [RFC3022#2.2, 3, 4.1-4.3] vornehmen.

Für die Umsetzung der Private Local Address aus den Adressbereichen der Einsatzumgebung MUSS die verwendete IP-Adresse aus dem vom Anbieter Zentrale Plattform Dienste (AZPD) bereitgestellten Adress-Pool entnommen werden und als Global Address genutzt werden. [≤]

###### **A\_17405 - Nur IPv4. IPv6 nur hardwareseitig vorbereitet**

Der Basis- und KTR-Consumer MUSS die IP Version 4 (IPv4) für alle seine IP-Schnittstellen unterstützen.

Die Hardware des Basis- und KTR-Consumer MUSS für den Einsatz von IPv4 und IPv6 im Dual-Stack-Mode geeignet sein.

Bis zu einer Migration von IPv4 auf IPv6 MUSS der Basis- und KTR-Consumer sämtliche empfangenen IP-Pakete der Version 6 (IPv6) verwerfen. [≤]

Die Anbindung des Basis- und KTR-Consumers an die zentrale TI erfolgt über einen Sicheren Zentralen Zugangspunkt (SZZP), siehe gemSpec\_Net Kapitel 3.1.1. Dieser Produkttyp unterstützt kein dynamisches Routing.

###### **A\_17406 - Kein dynamisches Routing**

Basis- und KTR-Consumer DÜRFEN NICHT Dynamische Routing-Protokolle einsetzen. [≤]

##### 5.1.1.1.1 Netzwerksegmentierung

In Anlehnung an die in der [gemSpec\_Net#2.3.3] definierten Netzwerksegmente werden in der Basis- und KTR-Consumerspezifikation die folgenden Bezeichner verwendet:

341 **Tabelle 1 : Mapping der Netzwerksegmente**

ReferenzID im Basis- und KTR-Consumer	Adressbereich für die TI-Produktivumgebung	Adressbereich für die TI-Testumgebung	Adressbereich für die TI-Referenzumgebung
NET_TI_ZENTRAL	TI_Zentral - Zentrale Dienste	TI_Test_Zentral - Zentrale Dienste	Ist durch den Testbetriebsverantwortlichen zu definieren.
NET_TI_GESICHERTE_FD	TI_Fachdienste - Gesicherte Fachdienste	TI_Test_Fachdienste - Gesicherte Fachdienste	Ist durch den Testbetriebsverantwortlichen zu definieren.
NET_TI_OFFENE_FD	TI_Fachdienste - Offene Fachdienste	TI_Test_Fachdienste - Offene Fachdienste	Ist durch den Testbetriebsverantwortlichen zu definieren.
NET_aAdG_aAdG NetG-TI	aAdG und aAdG NetG-TI	aAdG und aAdG NetG-TI	aAdG und aAdG NetG-TI
NET_CONSUMER	Liste der Netzwerke die in der Einsatzumgebung über den Basis- und KTR-Consumer erreichbar sind. Ein Eintrag der Liste enthält die Netzwerkadresse und den Netzwerkpräfix.		

- 342
- 343 **A\_17411 - Kommunikation mit NET\_TI\_Offene\_FD**
- 344 Der Basis- und KTR-Consumer MUSS sicherstellen, dass IP-Pakete mit dem Ziel
- 345 NET\_TI\_Offene\_FD und NET\_aAdG\_aAdG NetG-TI weitergeleitet werden. [ <= ]
- 346 **A\_17514 - Kommunikation mit NET\_TI\_Gesicherte\_FD**
- 347 Der KTR-Consumer MUSS sicherstellen, dass IP-Pakete mit dem Ziel
- 348 NET\_TI\_Gesicherte\_FD nur durch das im KTR-Consumer vorhandene jeweilige Fachmodul
- 349 in Richtung TI mit dem Ziel NET\_TI\_Gesicherte\_FD weitergeleitet. werden. [ <= ]
- 350 **A\_17415 - Kommunikation mit NET\_TI\_ZENTRAL**
- 351 Der Basis- und KTR-Consumer MUSS sicherstellen, dass IP-Pakete in Richtung
- 352 NET\_TI\_ZENTRAL mit dem Ziel TI-Namens- und Zeitdienst nur vom Basis- und KTR-
- 353 Consumer weitergeleitet werden. [ <= ]
- 354 **A\_17417 - Einschränkung von nicht genehmigten Traffic**
- 355 Der Basis- und KTR-Consumer MUSS nicht genehmigten Traffic blockieren. [ <= ]
- 356 **A\_17418 - Drop statt Reject**
- 357 Der Basis- und KTR-Consumer MUSS alle abgelehnten IP-Pakete verwerfen (DROP), ohne
- 358 ein ICMP-Destination-Unreachable (Type 3) zu schicken. [ <= ]

**A\_17419 - Abwehr von IP-Spoofing, DoS/DDoS-Angriffe und Martian Packets**

Der Basis- und KTR-Consumer MUSS geeignete technische Funktionen zur Abwehr von IP-Spoofing und DoS/DDoS-Angriffen implementieren.

Der Basis- und KTR-Consumer MUSS Martian Packets (Absender- oder Empfängeradressen aus den von der IETF als Special-Purpose definierten Netzbereichen), mindestens jedoch aus folgenden Netzbereichen 0.0.0.0/8, 127.0.0.0/8, 169.254.0.0/16, 192.0.0.0/24, 192.0.2.0/24, 198.18.0.0/15, 198.51.100.0/24, 203.0.113.0/24, 224.0.0.0/4, 240.0.0.0/4, verwerfen. Die in [RFC1918] und [RFC 6598] definierten Netzbereiche sind hiervon ausgenommen. [≤]

**A\_17420 - Eingeschränkte Nutzung von „Ping“**

Der Basis- und KTR-Consumer MUSS TCP-Port-7(Echo)-Pakete verwerfen.

Der Basis- und KTR-Consumer MUSS ICMP-Echo-Request (Typ 8) und ICMP-Echo-Response (Typ 0) ausschließlich für, per Anforderung genehmigten, Traffic weiterleiten. [≤]

**A\_17421 - Einschränkungen der IP-Protokolle**

Der Basis- und KTR-Consumer MUSS alle IP-Protokolle außer 1 (ICMP), 17 (UDP) und 6 (TCP) für alle ein- oder ausgehenden Pakete an allen seinen Adaptern verwerfen. [≤]

**A\_17423 - Firewall Restart**

Der Basis- und KTR-Consumer MUSS gewährleisten, dass unmittelbar nach einer Änderung der Parameter eines Adapters (LAN-Adapter, WAN-Adapter) die Firewall des Basis- und KTR-Consumer neu erstellt und geladen wird. [≤]

Umsetzungshinweis für den Hersteller: Es können zwei getrennten Firewall-Regelsets für den LAN- bzw. für den WAN-Adapter verwendet werden.

**A\_17424 - Firewall-Protokollierung**

Der Basis- und KTR-Consumer MUSS bei Konfigurationsänderungen der Firewall einen Protokolleintrag mit der Schwere „Warning“ und dem Typ „Operations“ sowie mindestens folgenden Informationen generieren:

- Zeitstempel, Aktion (Add/Delete/Change), Details (Beschreibung der Änderung), Auslöser (Prozess/User).

Der Basis- und KTR-Consumer MUSS für alle vom Basis- und KTR-Consumer ausgehenden, nicht zugelassenen Kommunikationsversuche einen Protokolleintrag mit der Schwere „Warning“ und dem Typ „Security“ sowie mindestens folgenden Informationen generieren:

- Zeitstempel, Aktion (Drop, Reject), Absender-IP-Adresse, Empfänger-IP-Adresse, Protokoll, Absender-Port und Empfänger-Port, Interface, über die das Paket empfangen wurde.

Der Basis- und KTR-Consumer MUSS für alle verworfenen IP-Spoofing- und Martian-Packets einen Protokolleintrag mit der Schwere „Warning“ und dem Typ „Security“ sowie mindestens folgenden Informationen generieren:

- Zeitstempel, Aktion (Drop, Reject), Absender-IP-Adresse, Empfänger-IP-Adresse, Protokoll, Absender-Port und Empfänger-Port, Interface über das das Paket empfangen wurde.

Der Basis- und KTR-Consumer MUSS für alle weiteren von der Firewall verworfenen IP-Pakete einen Protokolleintrag mit der Schwere „Info“ und dem Typ „Security“ sowie mindestens folgenden Informationen generieren, wobei Layer 3 Broadcasts von der Protokollierung ausgenommen werden können:



- 405 • Zeitstempel, Aktion (Drop, Reject), Absender-IP-Adresse, Empfänger-IP-Adresse,  
406 Protokoll, Absender-Port und Empfänger-Port, Interface über das das Paket  
407 empfangen wurde.

408 [ $\leq$ ]

### 409 5.1.1.2 Durch Ereignisse ausgelöste Reaktionen

#### 410 **A\_17425 - Reagiere auf LAN\_IP\_Changed**

411 Wurde die IP Adresse des LAN Interfaces geändert oder hat, bei aktiven DHCP Client, ein  
412 erfolgreiches DHCP\_RENEW stattgefunden MUSS der Basis- und KTR-Consumer den LAN-  
413 Adapter initialisieren. [ $\leq$ ]

#### 414 **A\_17426 - Reagiere auf WAN\_IP\_Changed**

415 Wurde die IP Adresse des WAN Interfaces geändert oder hat, bei aktiven DHCP Client,  
416 ein erfolgreiches DHCP\_RENEW stattgefunden MUSS der Basis- und KTR-Consumer den  
417 WAN-Adapter initialisieren. [ $\leq$ ]

#### 418 **A\_17430 - Netzwerk-Routen einrichten**

419 Der Basis- und KTR-Consumer MUSS die Konfiguration aller notwendigen Netzwerk-  
420 Routen ermöglichen. [ $\leq$ ]

#### 421 **A\_17474 - Anzeige IP-Routinginformationen**

422 Der Basis- und KTR-Consumer MUSS über die Managementschnittstelle die konfigurierten  
423 IP-Routen und die aktuelle IP-Routingtabelle mit mindestens folgenden Informationen  
424 anzeigen:

- 425 • Forwarding Status
- 426 • Zieladresse/Präfix
- 427 • Gateway (Next-Hop)
- 428 • Routing Typ
- 429 • Routing Preference.

430 [ $\leq$ ]

431 Zur Bekanntmachung von Änderungen und Neuanschlüssen zu den, an die TI  
432 angeschlossenen, anderen Anwendungen des Gesundheitswesens (aAdG bzw. aAdG  
433 NetG-TI) wird tagesaktuell eine Datei mit dem Namen "Bestandsnetze.xml" bereitgestellt  
434 (siehe dazu gemSpec\_KSR, Kapitel 9 Anhang C). Die Datei liefert für alle  
435 angeschlossenen aAdG bzw. aAdG NetG-TI einen Namen/ID, Netzwerkinformationen (IP-  
436 Adressen) und den für dieses Netz zu verwendenden DNS Server welcher dem DNS  
437 Forwarder des Basis- und KTR-Konsumer übergeben wird.

#### 438 **A\_17576 - KSR lokalisieren**

439 Der Basis- und KTR-Consumer MUSS für die Lokalisierung des Konfigurationsdienstes der  
440 TI (KSR) die Möglichkeit der Lokalisierung des KSR durch DNS-Anfragen an den DNS-  
441 Forwarder DNS\_SERVERS\_TI zur Auflösung der SRV-RR und TXT-RR mit den  
442 Bezeichnern „\_ksrkonfig.\_tcp.ksr.<TOP\_LEVEL\_DOMAIN\_TI>“ vorsehen.  
443 Der Basis- und KTR-Consumer erhält damit URLs der Downloadpunkte des KSR  
444 für Konfigurationsdaten (MGM\_KSR\_KONFIG\_URL). [ $\leq$ ]

#### 445 **A\_17574 - Infrastruktur Konfiguration aktualisieren**

446 Der Basis- und KTR-Consumer MUSS täglich seine Infrastruktur Konfiguration  
447 aktualisieren.

448 Der Basis- und KTR-Consumer MUSS dazu eine TLS-Verbindung zum  
449 Konfigurationsdienst der TI aufbauen. Dabei MUSS er das durch den Server präsentierte  
450 Zertifikat prüfen.



451 Das Herunterladen der Konfigurationsdaten erfolgt mittels  
 452 I\_KSRS\_Download::get\_Ext\_Net\_Config (MGM\_KSR\_KONFIG\_URL,  
 453 „Bestandsnetze.xml“.)[<=]

## 454 5.1.2 Zeitdienst

455 Der Zeitdienst schafft die Grundlage einer gleichen Systemzeit für alle in der TI  
 456 einzusetzenden Produkttypen. Innerhalb des Basis-KTR-Consumers ist dafür ein NTP-  
 457 Client erforderlich, welcher die Zeitangaben des Zeitdienstes der zentralen TI abfragt und  
 458 verwendet. Die in [gemSpec\_Net#6.2.2] „Nutzung“ getroffenen Anforderungen werden  
 459 durch dieses Kapitel erweitert.

### 460 A\_17485 - Maximale Zeitabweichung

461 Der Basis- und KTR-Consumer MUSS sicherstellen, dass der maximale zulässige Fehler  
 462 von +/- 20ppm (part per million) gegenüber einer Referenzuhr nicht überschritten wird.  
 463 Dies entspricht einer maximalen Abweichung im Freilauf von +/- 34,56 Sekunden über  
 464 20 Tage.[<=]

## 465 5.1.3 Namensdienst und Dienstlokalisierung

### 466 5.1.3.1 Funktionsmerkmalweite Aspekte

#### 467 A\_17498 - Grundlagen des Namensdienstes

468 Der Basis- und KTR-Consumer MUSS die Funktion eines Recursive Caching Nameservers  
 469 zur Auflösung von DNS-Anfragen anbieten. (Im Folgenden kurz DNS-Server genannt).  
 470 Der Caching-Nameserver des Basis- und KTR-Consumer MUSS für Clientsysteme aus  
 471 dem lokalen Netzwerk der Einsatzumgebung erreichbar sein.  
 472 Der Caching Nameserver des Basis- und KTR-Consumer MUSS einen sinnvollen Timeout  
 473 für die Bearbeitung von DNS-Abfragen beachten. Konnte eine DNS-Abfrage nicht  
 474 durchgeführt werden, MUSS die Bearbeitung abgebrochen werden. [<=]

#### 475 A\_17499 - DNS-Forwards des DNS-Servers

476 Der DNS-Server des Basis- und KTR-Consumer MUSS die folgenden DNS-Forwards  
 477 durchführen:  
 478

479 **Tabelle 2 : TAB\_CONS\_687 DNS-Forwards des DNS-Servers**

Domain	Forwarders	Bemerkungen
Namensraum TI (*DNS_TOP_LEVEL_DOMAIN_TI)	DNS_SERVERS_TI	DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb des Namensraums der TI.
Namensraum angeschlossene Netze des Gesundheitswesens mit aAdG-NetG (Domainnamen von angeschlossenen Netzen des	DNS_SERVERS_BESTANDSNETZ E (Je Domainnamen eines angeschlossenen Netzes des Gesundheitswesens mit aAdG-NetG alle zugehörigen DNS-Server IP-Adressen gemäß Bestandsnetze.xml)	Je angeschlossenem Netz des Gesundheitswesens mit aAdG-NetG in NLW_AKTIVE_BESTANDSNETZ E wird eine DNS Forward Rule zur Auflösung von DNS-Namen innerhalb dieses Netzes verwendet.

Gesundheitswesens mit aAdG-NetG gemäß Bestandsnetze.xml)		
Namensraum lokale Einsatzumgebung	DNS_SERVERS_CONSUMER	DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb der DNS-Domain im LAN des Consumer

[<=]

### A\_17500 - DNS Stub-Resolver

Der Basis- und KTR-Consumer MUSS von allen internen Diensten zur Namensauflösung genutzt werden.

Der Stub-Resolver im Basis- und KTR-Consumer MUSS immer den Caching Nameserver im Basis- und KTR-Consumer anfragen.[<=]

## 5.1.3.2 Interne TUCs, auch durch Fachmodule nutzbar

### 5.1.3.2.1 TUC\_CON\_362 „Liste der Dienste abrufen“

#### A\_17502 - TUC\_CON\_362 „Liste der Dienste abrufen“

Der Basis- und KTR-Consumer MUSS den technischen Use Case TUC\_CONS\_362 „Liste der Dienste abrufen“ umsetzen.

**Tabelle 3: TAB\_CONS\_648 – TUC\_CONS\_362 „Liste der Dienste abrufen“**

Element	Beschreibung
Name	TUC „Liste der Dienste abrufen“
Beschreibung	Ermittlung aller zu einer DNS-SD-Gruppe gehörenden DNS-Namen.
Auslöser	interne Anfrage (Basisdienst oder Fachmodul)
Vorbedingungen	Die vom Basis- und KTR-Consumer zu verwendenden DNS-Server müssen konfiguriert sein.
Eingangsdaten	FQDN des PTR Resource Records
Komponenten	Basis- und KTR-Consumer
Ausgangsdaten	LIST_OF_SRV_ENTITIES

Standardablauf	Mit dem FQDN wird eine Typ „PTR“ Anfrage an den Stub-Resolver des Basis- und KTR-Consumer gestellt.
----------------	---

[&lt;=]

### 5.1.3.3 Operationen an der Außenschnittstelle

#### A\_17509 - Basisanwendung Namensdienst

Der Basis- und KTR-Consumer MUSS für Clients in der Einsatzumgebung und den Fachmodulen im jeweiligen Consumer eine Basisanwendung Namensdienst, mit der Funktion Namensauflösung und Dienstlokalisierung anbieten.

**Tabelle 4: Basisanwendung Namensdienst**

Name	Namensdienst	
Version	wird im Produktsteckbrief des Basis- und KTR-Consumer definiert	
Namensraum	Keiner	
Namensraum-Kürzel	Keiner	
Operationen	Name	Kurzbeschreibung
	GetIPAddress	Diese Operation ermöglicht die Auflösung von FQDNs in IP-Adressen
WSDL	Keines	
Schema	Keines	

[&lt;=]

### 5.1.3.4 Betriebsaspekte

#### A\_17512 - Initialisierung „Namensdienst und Dienstlokalisierung“

Der Basis- und KTR-Consumer MUSS in der Bootup-Phase zur Initialisierung des Funktionsmerkmals „Namensdienst und Dienstlokalisierung“:

- den autoritativen Nameserver starten
- den Caching-Nameserver starten.

[&lt;=]

#### A\_17513 - Konfigurationsparameter Namensdienst und Dienstlokalisierung

Der Administrator des Basis- und KTR-Consumer MUSS die aufgelisteten Parameter in Tabelle 5 über die Managementschnittstelle konfigurieren und die aufgelisteten Parameter in Tabelle 6 ausschließlich einsehen können.

Nach jeder Änderung MUSS sichergestellt werden, dass die Änderungen sofort am autoritativen bzw. am Caching Nameserver zur Verfügung stehen.

**Tabelle 5: Konfigurationsparameter Namensdienst**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
------------	----------	---

DNS_SERVERS_CONSUMER	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern, die zur Namensauflösung von Namensräumen in der Einsatzumgebung verwendet werden. Der Administrator MUSS die Liste von DNS-Servern, die die DNS_DOMAIN_CONSUMER auflösen, bearbeiten können. Die IP-Adressen der DNS-Server KÖNNEN auf den Adressbereich der ANLW_LAN_IP_ADDRESS eingeschränkt sein.
DNS_DOMAIN_CONSUMER	DNS Domainname	DNS Domainname, der von einem DNS-Server der Einsatzumgebung aufgelöst wird. Der Name DARF NICHT mit einem „.“ beginnen.

518 **Tabelle 6: Einsehbare Konfigurationsparameter Namensdienst**

ReferenzID	Belegung	Bedeutung
DNS_SERVERS_TI	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern, die zur Namensauflösung des Namensraums der TI verwendet werden
DNS_TOP_LEVEL_DOMAIN_TI	DNS Domainname	Top Level Domain des Namensraumes TI

519  
520 [ $\leq$ ]

## 521 5.2 Sicherheit

522 Die Sicherheits- und Datenschutzanforderungen sind abgedeckt durch die übergreifenden  
 523 Sicherheits- und Datenschutzanforderungen an Hersteller und Anbieter  
 524 [gemSpec\_DS\_Hersteller], [gemSpec\_DS\_Anbieter], die spezifischen Sicherheits- und  
 525 Datenschutzanforderungen des Clientmoduls KOM-LE und des Fachmoduls ePA im KTR-  
 526 Consumer [gemSpec\_FM\_ePA\_KTR\_Consumer] sowie die spezifischen Sicherheits- und  
 527 Datenschutzanforderungen der Systemprozesse der dezentralen TI  
 528 [gemSpec\_Systemprozesse\_dezTI].

## 529 5.3 Identitäten

530 *In diesem Dokument werden kryptographische Identitäten entsprechend ihrer Bezeichner im*  
 531 *Objektsystem der SMC-B referenziert. Dies dient der Eindeutigkeit der Referenz und bedeutet*  
 532 *nicht, dass die Strukturen des Objektsystems der SMC-B in einem HSM nachgebildet werden*  
 533 *müssen.*

Im KTR-Consumer werden private Schlüssel der SMC-B, aber auch Schlüsselmaterial des KOM-LE-Clientmoduls 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.

#### **A\_17598 - Qualität des HSM**

Die Basis- und KTR-Consumer MÜSSEN privates Schlüsselmaterial zu Zertifikaten der Telematikinfrastruktur in einem HSM, dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde, integritätsgeschützt und vertraulich speichern. Als Evaluierungsschema kommen dabei Common Criteria oder Federal Information Processing Standard (FIPS) in Frage. Die Prüftiefe MUSS mindestens (a) FIPS 140-2 Level 3, oder (b) Common Criteria EAL 4 entsprechen. [≤]

#### **A\_18195 - Basis-Consumer mit SMC-B**

Der Basis-Consumer KANN privates Schlüsselmaterial einer SMC-B in Kartenform nutzen. [≤]

**Tabelle 7: Tab\_Personalisierung\_HSM – Personalisierung des HSM**

Aspekt	Beschreibung
Schlüsselmaterial der SMC-B	Das Schlüsselmaterial wird sicher im HSM erzeugt. Das private Schlüsselmaterial verlässt das HSM nicht oder nur zum Zwecke eines Backups auf einem Backup-HSM, wobei die Übertragung hinsichtlich Vertraulichkeit geschützt sein muss.
Zertifikatsrequest	Die benötigten Zertifikatsrequests werden im HSM erzeugt und exportiert. Die Zertifikatsrequests werden unter Wahrung der Authentizität und Integrität dem TSP übermittelt.
Zertifikat	Das Zertifikat wird vom TSP zum Betreiber übermittelt.
TLS-Schlüsselmaterial des KOM-LE-Clientmoduls	Der KOM-LE-Anbieter erzeugt die Schlüsselpaare für die Zertifikate des KOM-LE-Clientmoduls und bezieht aus der Komponenten-PKI der TI die C.CM.TLS-CS-Zertifikate. Das Schlüsselpaar muss zur sicheren Speicherung ins HSM eingebracht werden.

#### **A\_17599 - Personalisierung des HSM**

Der Anbieter des Basis- oder KTR-Consumers MUSS einen sicheren Prozess zur Personalisierung des HSMs definieren und etablieren, der die in Tab\_Personalisierung\_HSM genannten Aspekte beinhaltet. [≤]

#### **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. [≤]

## 5.4 Schnittstellen

Für den Basis- und KTR-Consumer werden einheitliche Schnittstellen definiert und im Rahmen des Zulassungstests genutzt. Für eine bessere Integrationsfähigkeit ist es aber erlaubt, dass zusätzlich zu den definierten Schnittstellen auch weitere Schnittstellentechnologien genutzt werden können, über welche die festgelegten Operationen angesprochen werden können.

### **A\_17712 - Zusätzlich alternative Schnittstellentechnologien**

Der Basis- und KTR-Consumer KANN zusätzlich zu den in den Spezifikationen festgelegten Schnittstellen zusätzlich weitere Schnittstellentechnologien anbieten, über welche die festgelegten Operationen angesprochen werden können. [ $\leq$ ]

ENTWURF

## 6 Funktionsmerkmale

### 6.1 Verschlüsselungsdienst

#### 6.1.1 Durch Module nutzbare TUCs

##### **A\_17466 - Systemprozess PL\_TUC\_HYBRID\_ENCIPHER**

Der Basis- und KTR-Consumer MUSS den Systemprozess PL\_TUC\_HYBRID\_ENCIPHER implementieren und bereitstellen. [≤]

##### **A\_17467 - Systemprozess PL\_TUC\_HYBRID\_DECIPHER**

Der Basis- und KTR-Consumer MUSS den Systemprozess PL\_TUC\_HYBRID\_DECIPHER implementieren und bereitstellen. [≤]

#### 6.1.2 Operationen an der Clientschnittstelle

##### **A\_17477 - Basisdienst Verschlüsselungsdienst**

Der Basis- und KTR-Consumer MUSS für Clients einen Basisdienst Verschlüsselungsdienst anbieten.

**Tabelle 8: Tab\_Verschlüsselungsdienst**

Name	EncryptionService	
Version	Siehe Anhang	
Namensraum	Siehe Anhang	
Namensraum-Kürzel	CRYPT für Schema und CRYPTW für WSDL	
Operationen	Name	Kurzbeschreibung
	EncryptDocument	Dokument hybrid verschlüsseln
	DecryptDocument	Dokument hybrid entschlüsseln
WSDL	EncryptionService.wsdl	
Schema	EncryptionService.xsd	

[≤]

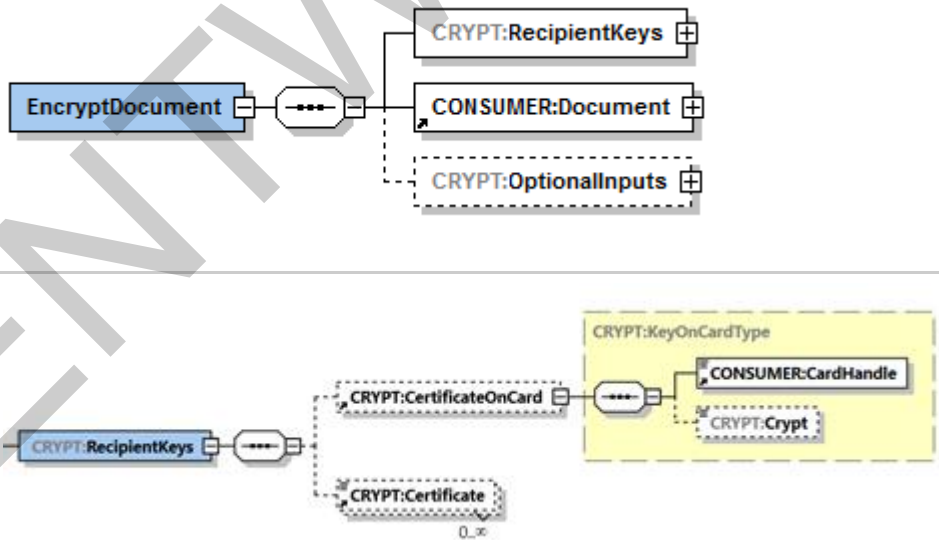
### 6.1.2.1 EncryptDocument

#### A 17510-03A\_17510-02 - Basis- und KTR-Consumer, Operation

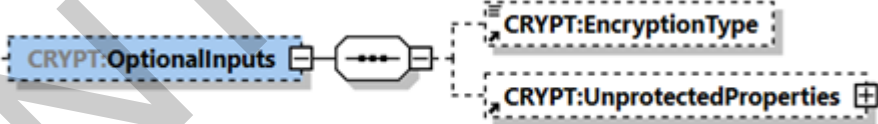
#### EncryptDocument

Der Verschlüsselungsdienst des Basis- und KTR-Consumer MUSS an der Clientschnittstelle eine Operation EncryptDocument anbieten.

**Tabelle 9: Tab\_Operation\_EncryptDocument**

Name	EncryptDocument
Beschreibung	<p>Diese Operation verschlüsselt ein übergebenes Dokument hybrid. Der Dokumententyp XML wird gesondert behandelt. Alle anderen Dokumententypen nutzen die binäre Verschlüsselung. Für die hybride Verschlüsselung wird ein asymmetrischer Schlüssel aus einem X.509v3-Zertifikat genutzt. Dieses Zertifikat wird als Parameter übergeben oder auf dem HSM referenziert. Pro Operationsaufruf können mehrere Hybridschlüssel erzeugt werden. Durch das Zertifikat wird festgelegt, ob RSA oder ECC basierte Hybridschlüssel erzeugt werden. Bei Angabe der Zertifikate über CertificateOnCard (Referenz auf HSM) wird das Verschlüsselungsverfahren durch die Angabe in Crypt bestimmt. Es können Hybridschlüssel für RSA oder ECC oder beide Verfahren erzeugt werden. Für alle Dokumententypen wird immer das gesamte Dokument verschlüsselt.</p>
Aufrufparameter	 <p>The diagram illustrates the sequence of parameters for the EncryptDocument operation. The main operation box is 'EncryptDocument'. It receives three inputs: 'CRYPT:RecipientKeys', 'CONSUMER:Document', and 'CRYPT:OptionalInputs'. The output of the operation is a dashed box containing 'CRYPT:CertificateOnCard', 'CRYPT:Certificate', and 'CRYPT:KeyOnCardType'. The 'CRYPT:KeyOnCardType' box is further detailed in a yellow box, showing 'CONSUMER:CardHandle' and 'CRYPT:Crypt'.</p>
RecipientKeys	Identifiziert die Empfänger der zu verschlüsselnden Nachricht über X.509-Zertifikate (öffentliche Schlüssel). Quelle für die Zertifikate kann eine Karte sein, die per CertificateOnCard-Element referenziert wird, oder der Aufrufer, der X.509-Zertifikate im Certificate-Element übergibt.
CardHandle	Identifiziert die zu verwendende Karte mit dem (öffentlichen) Schlüssel.



		Ist das Element nicht vorhanden, so werden nur Zertifikate per Element <code>Certificate</code> übergeben.
	Crypt	Der Wert dieses Parameters ist in Tabelle Tab_KeyReference_für_Encrypt/Decrypt spezifiziert und gibt den Typ von Zertifikaten und dadurch das Verfahren für die Erzeugung der Hybridschlüssel vor. (Default-Wert ist RSA)
	Certificate	<p><code>Certificate</code> ist ein Base64-kodiertes XML-Element, in dem das Zertifikat, das den asymmetrischen Schlüssel enthält (öffentlicher Schlüssel), DER-kodiert übergeben wird.</p> <p>Es kann eine Liste von Zertifikaten übergeben werden.</p> <p>Dieses Element kann leer sein, wenn ausschließlich Zertifikate verwendet werden sollen, die über <code>CertificateOnCard</code> angegeben werden.</p>
	CONSUMER: Document	<p>Dieses entsprechend [OASIS-DSS] Section 2.4.2 spezifizierte Element enthält das zu verschlüsselnde Dokument, wobei das Kindelement <code>dss:Base64Data</code> <del>und</del> <u>oder</u> <code>CONSUMER:Base64XML</code> verwendet wird. <u>Das zugeordnete Verschlüsselungsverfahren ist</u></p> <ul style="list-style-type: none"> <li>• <u>XMLEnc: „http://www.w3.org/TR/xmlenc-core/“ für <code>CONSUMER:Base64XML</code></u></li> <li>• <u>CMS: „urn:ietf:rfc:5652“ für <code>dss:Base64Data</code></u></li> </ul>
		
	CRYPT: Optional Inputs	<p>Enthält <del>eine Auswahl der folgenden unten näher erläuterten (die optionalen) Eingabeparameter:</del> <u>Parameter <code>CRYPT:UnprotectedProperties</code> und <code>CRYPT:EncryptionType</code>.</u></p>
	Encryption Type	<p><del>Zu wählendes</del> <u>Dieses optionale Element bestimmt das Verschlüsselungsverfahren, wobei folgende URI vorgesehen sind:</u></p> <ul style="list-style-type: none"> <li>• <u>Es MUSS das Verfahren XMLEnc: „http://www.w3.org/TR/xmlenc-core/“</u></li> <li>• <u>unterstützt werden, wenn das Dokument in <code>CONSUMER:Base64XML</code> übergeben wird und CMS: „urn:ietf:rfc:5652“</u></li> </ul>

		<p><u>Im Fall XMLEnc wird ein Base64-codiertes XML-„ wenn das Dokument in CONSUMER:Document/CONSUMER:Base64XML übergeben. Im Fall CMS wird ein Base64-codiertes Binär- Dokument im Element CONSUMER:Document/dss:Base64Data übergeben- Ist wird.</u></p> <p><u>Die Verwendung dieses Elements ist aufgrund der Parameter EncryptionTypeimpliziten Zuordnung der Verschlüsselungsverfahren zur Methode der Dokumentübergabe nicht gesetzt, wird anhand des für die Übergabe des Dokuments verwendeten Elements (CONSUMER:Base64XML oder dss:Base64data) das Verfahren XMLEnc, bzw. CMS angewendet erforderlich.</u></p>
	CRYPT: Unprotected Properties	<p>Dieses optionale Element wird <u>innur für das Verschlüsselungsverfahren CMS-Fall (EncryptionType = urn:ietf:rfc:5652) ausgewertet. (zu verschlüsselndes Dokument ist in dss:Base64Data vorhanden).</u></p> <p>Die Elemente ./UnprotectedProperties/Property/Value/CMSAtt ribute müssen base64/DER-kodiert ein vollständiges ASN.1-Attribute enthalten, definiert in [CMS# 9.1.AuthenticatedData Type]. Es muss bei der Erstellung des CMS-Containers unter "unauthAttrs" aufgenommen werden. Das zugehörige Element ./UnprotectedProperties/Property/Identifier wird nicht ausgewertet.</p>
<b>Rückgabe</b>		
	Status	Enthält den Ausführungsstatus der Operation.
	Document	<p>Enthält das verschlüsselte Dokument in Base64-codierter Form, wenn die Verschlüsselung erfolgreich durchgeführt wurde.</p> <p>Im Fall XMLEnc wird das verschlüsselte XML-Dokument in CONSUMER:Document/CONSUMER:Base64XML zurückgegeben.</p>

		Im Fall CMS wird das verschlüsselte Dokument in <code>CONSUMER:Document/dss:Base64data</code> zurückgegeben.
<b>Vorbedingungen</b>	Keine	
<b>Nachbedingungen</b>	Keine	

Vor der Verwendung für die Verschlüsselung MÜSSEN Zertifikate durch den Aufruf von `PL_TUC_PKI_VERIFY_CERTIFICATE` auf ihre Gültigkeit geprüft werden. Abgelaufene oder gesperrte Zertifikate MÜSSEN von der Verwendung ausgeschlossen werden.

Das Verschlüsseln erfolgt durch Aufruf von `PL_TUC_HYBRID_ENCIPHER` {  
`Doc, das zu verschlüsselnde Dokument = CONSUMER:Document;`  
`{Cert(i)}, „Menge der Empfänger-/Ziel-Zertifikate“ = RecipientKeys;`  
`Attribute, optionale, zusätzliche Attribute = UnprotectedProperties;`  
`}`

Wird ein Zertifikat per `CertificateOnCard`-Element referenziert, ist dieses vorher durch den HSMProxy zu extrahieren

[<=]

### 6.1.2.2 DecryptDocument

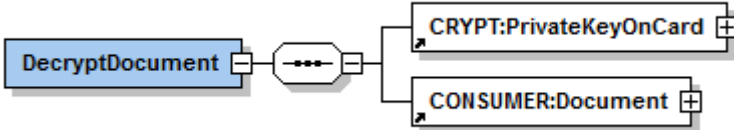
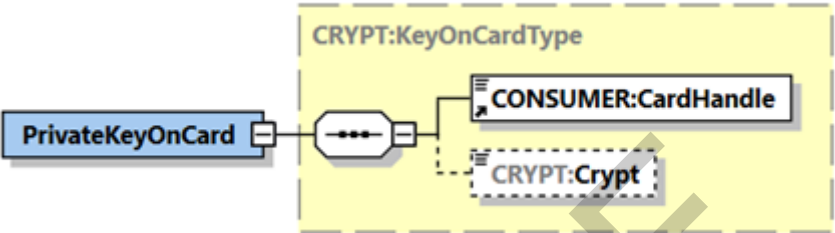
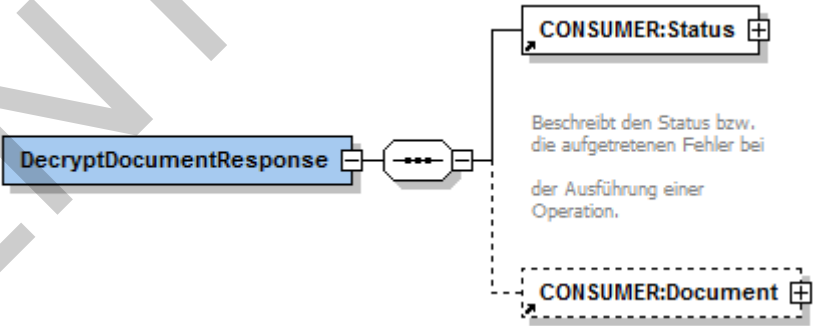
#### A 17515-02A-17515-01 - Basis- und KTR-Consumer, Operation

#### **DecryptDocument**

Der Verschlüsselungsdienst des Basis- und KTR-Consumer MUSS an der Clientschnittstelle eine Operation `DecryptDocument` anbieten.

**Tabelle 10: Tab\_Operation\_DecryptDocument**

Name	DecryptDocument
<b>Beschreibung</b>	<p>Diese Operation entschlüsselt ein hybrid verschlüsseltes Dokument.</p> <p>Es werden die Dokumententypen XML und Andere (Binär) unterstützt.</p> <p>Für die Entschlüsselung wird ein asymmetrischer Schlüssel zu einem X.509v3-Zertifikat genutzt.</p> <p>Das Kryptoverfahren (RSA oder ECC) wird durch den Hybridschlüssel des verschlüsselten Dokuments bestimmt. Liegt eine Verschlüsselung sowohl für RSA, als auch ECC vor, erfolgt vorrangig eine Entschlüsselung mittels des ECC-Schlüssels. <del>Ist dieses nicht erfolgreich oder nicht anwendbar, erfolgt die Entschlüsselung mittels des RSA-Schlüssels.</del></p>

<b>Aufrufparameter</b>		
		
	PrivateKeyOnCard	Identifiziert die zu verwendende Karte mit dem (privaten) Schlüssel.
	CardHandle	Identifiziert die Karte.
	Crypt	Wird nicht verwendet. Die Auswahl des Kryptoverfahrens erfolgt anhand des Hybridschlüssels des verschlüsselten Dokuments..
<b>Rückgabe</b>		
	Status	Enthält den Ausführungsstatus der Operation.
	Document	Enthält das entschlüsselte Dokument in Base64-codierter Form. Im Fall der Verschlüsselung mit XMLEnc wird das entschlüsselte XML-Dokument in CONSUMER:Document/CONSUMER:Base64XML zurückgegeben. Im Fall der Verschlüsselung mit CMS wird das entschlüsselte Dokument in

		CONSUMER:Document/dss:Base64data zurückgegeben.
<b>Vorbedingungen</b>	Keine	
<b>Nachbedingungen</b>	Keine	

Das Entschlüsseln erfolgt durch Aufruf von PL\_TUC\_HYBRID\_DECIPHER {  
 D, "das verschlüsselte Dokument =CONSUMER:Document;  
 Id, "(Identität des) Empfänger" =PrivateKeyOnCard;  
 }  
 [<=]

Tabelle 11: Tab\_KeyReference\_für\_Encrypt/Decrypt

Karte	Crypt (Wert)	KeyReference (Encrypt)	KeyReference (Decrypt)
		In DF.ESIGN	In DF.ESIGN
SM-B (HSM)	RSA	EF.C.HCI.ENC.R2048	PrK.HCI.ENC.R2048
	ECC	EF.C.HCI.ENC.E256	PrK.HP.ENC.E256
	RSA_ECC	EF.C.HCI.ENC.R2048 EF.C.HCI.ENC.E256	PrK.HCI.ENC.R2048 PrK.HP.ENC.E256

## 6.2 Signaturdienst

### 6.2.1 Durch Module nutzbare TUCs

#### A\_17517 - Systemprozess PL\_TUC\_SIGN\_DOCUMENT\_nonQES

Der Basis- und KTR-Consumer MUSS den Systemprozess  
 PL\_TUC\_SIGN\_DOCUMENT\_nonQES implementieren und bereitstellen.[<=]

#### A\_17518 - Systemprozess PL\_TUC\_SIGN\_HASH\_nonQES

Der Basis- und KTR-Consumer MUSS den Systemprozess PL\_TUC\_SIGN\_HASH\_nonQES  
 implementieren und bereitstellen.[<=]

**A\_17577 - Systemprozess PL\_TUC\_VERIFY\_DOCUMENT\_nonQES**

Der Basis- und KTR-Consumer MUSS den Systemprozess  
PL\_TUC\_VERIFY\_DOCUMENT\_nonQES implementieren und bereitstellen.  
[<=]

**6.2.2 Operationen an der Clientschnittstelle****A\_17523 - Basisdienst Signaturdienst**

Der Basis- und KTR-Consumer MUSS Clientsystemen einen Basisdienst Signaturdienst  
(nonQES) anbieten.

**Tabelle 12: Tab\_Signaturdienst**

<b>Name</b>	<b>SignatureService</b>	
<b>Version</b>	Siehe Anhang	
<b>Namensraum</b>	Siehe Anhang	
<b>Namensraum-Kürzel</b>	SIG für Schema und SIGW für WSDL	
<b>Operationen</b>	<b>Name</b>	<b>Kurzbeschreibung</b>
	SignDocument	Dokument signieren
	VerifyDocument	Signatur verifizieren
	ExternalAuthenticate	Binärstring signieren
<b>WSDL</b>	SignatureService.wsdl	
<b>Schema</b>	SignatureService.xsd	

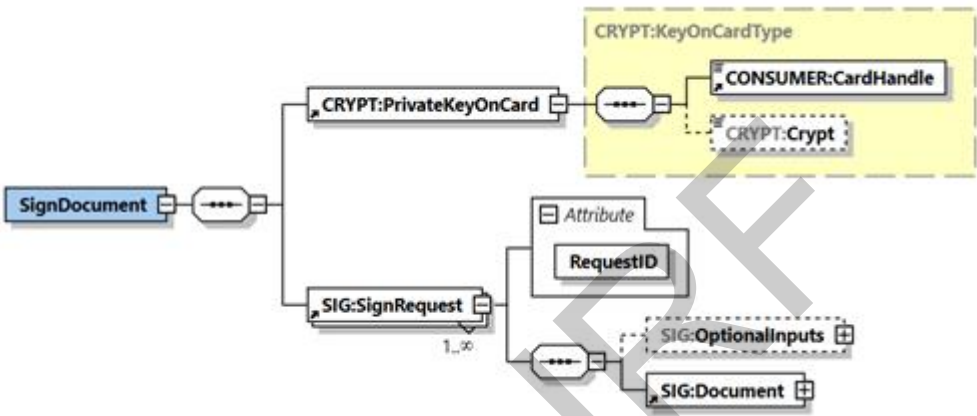
[&lt;=]

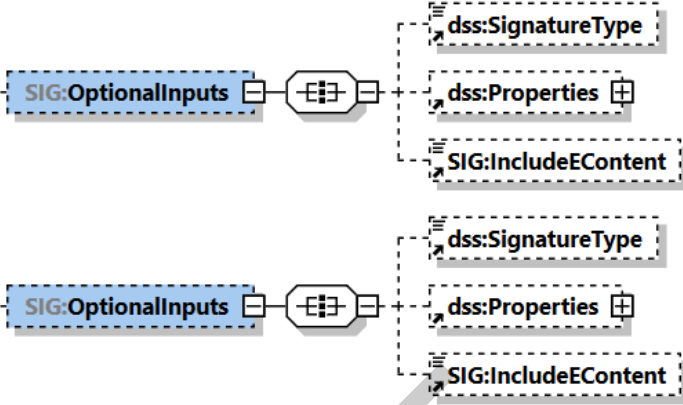
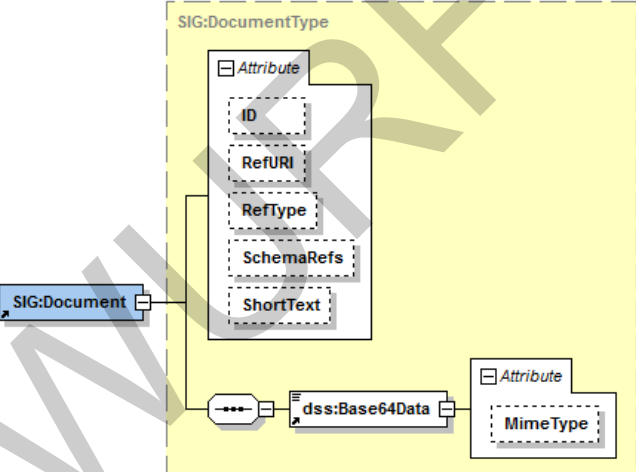
**6.2.2.1 SignDocument****A\_17525-02A\_17525-01 - Basis- und KTR-Consumer, Operation SignDocument**

Der Signaturdienst des Basis- und KTR-Consumer MUSS an der Clientschnittstelle eine an  
[OASIS-DSS] angelehnte Operation *SignDocument* wie in Tabelle  
Tab\_Operation\_SignDocument beschrieben anbieten.

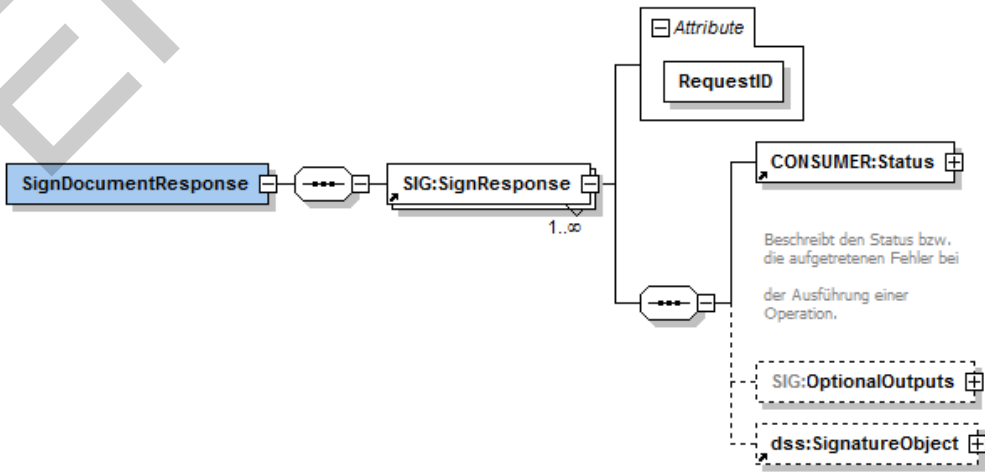
**Tabelle 13: Tab\_Operation\_SignDocument**

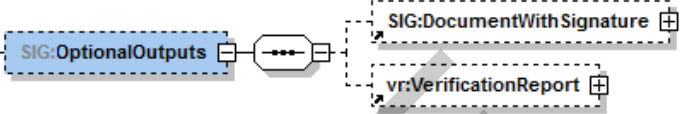
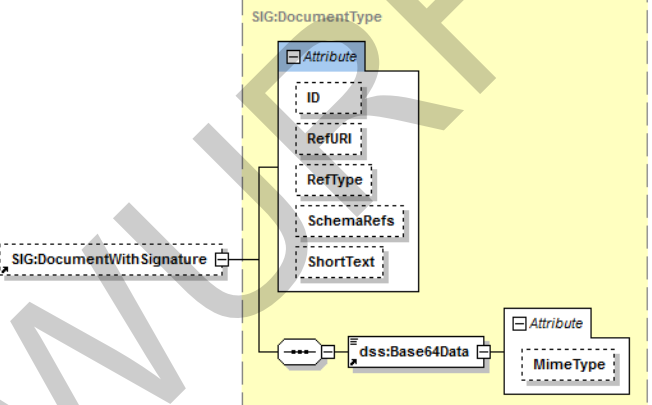
<b>Name</b>	<b>SignDocument</b>
-------------	---------------------

<b>Beschreibung</b>	<p>Diese Operation lehnt sich an [OASIS-DSS] an. Sie enthält voneinander unabhängige SignRequests. Jeder SignRequest erzeugt eine Signatur für ein Dokument.</p> <p>Zur Signaturerzeugung werden Schlüssel und Zertifikate eines HSM benutzt. Es wird ausschließlich der Signatortyp "CMS-Signatur" verwendet gemäß <a href="#">[RFC 5652]</a> (<a href="#">URIn:ietf:rfc:5652</a>) und das Profil CADES-BES gemäß <a href="#">[CADES]</a> verwendet.</p>	
<b>Aufrufparameter</b>		
PrivateKeyOnCard	Identifiziert die zu verwendende Karte mit dem (privaten) Schlüssel.	
CardHandle	Identifiziert die zu verwendende Signaturkarte.	
Crypt	<p>Dieser Parameter steuert die Auswahl der Zertifikate und Schlüssel für die Signaturerstellung. Die Werte sind in der Tabelle Tab_Zertifikate_für_Sign/VerifyDocument vorgegeben.</p> <p>(Default-Wert ist RSA)</p>	
SIG:SignRequest	<p>Ein SignRequest kapselt den Signaturauftrag für ein Dokument.</p> <p>Das verpflichtende XML-Attribut RequestID identifiziert einen SignRequest innerhalb eines Stapels von SignRequests eindeutig. Es dient der Zuordnung der SignResponse zum jeweiligen SignRequest.</p>	
SIG:OptionalInputs	Enthält optionale Eingangsparameter (angelehnt an dss:OptionalInputs gemäß [OASIS-DSS] Section 2.7):	

		
SIG:Document		 <p>Dieses an das <code>dss:Document</code> Element aus [OASIS-DSS] Section 2.4.2 angelehnte Element enthält das zu signierende Dokument, <u>wobei das Kindelement in <code>dss:Base64Data</code> auftreten kann.</u></p>
<code>dss:SignatureType</code>		<p>Durch dieses in [OASIS-DSS] (Abschnitt 3.5.1) beschriebene Element kann der generelle Typ der zu erzeugenden Signaturen <u>spezifiziert angegeben</u> werden. <u>Hierbei MUSS folgender Es muss der Signaturtyp unterstützt werden:</u></p> <p><b>CMS-Signatur</b></p> <p><u>Durch Übergabe der URI <code>urn:ietf:rfc:5652</code> wird eine CMS-Signatur gemäß [RFC5652] angestoßen. Das zu verwendende Profil ist CAdES-BES ({CAdES}).</u>  <u>Die Signatur wird als <code>dss:Base64Signature</code> mit der oben genannten URI als Type zurückgeliefert.</u></p> <p><u>(Siehe Tabelle Tab_Default_Signaturverfahren)</u></p>



		<p><a href="#">unterstützt werden.</a></p> <p>Fehlt dieses Element, so <del>wird dieses</del><a href="#">muss der Signaturtyp CMS-Signatur (URI urn:ietf:rfc:5652) implizit verwendet werden.</a></p>
	dss:Properties	<p>Durch dieses in [OASIS-DSS] (Abschnitt 3.5.5) definierte Element können zusätzliche signierte und unsignierte Eigenschaften (Properties) bzw. Attribute in die Signatur eingefügt werden</p> <p>Es dürfen genau die folgenden Attribute</p> <p><code>./SignedProperties/Property/Value/CMSAttribute</code> und <code>./UnsignedProperties/Property/Value/CMSAttribute</code> enthalten sein.</p> <p>Ein solches XML-Element <code>CMSAttribute</code> muss ein vollständiges, base64/DER-kodiertes ASN.1-Attribute enthalten, definiert in [CMS#5.3.SignerInfo Type]. Es muss bei der Erstellung des CMS-Containers unverändert unter <code>SignedAttributes</code> bzw. <code>UnsignedAttributes</code> aufgenommen werden.</p>
	SIG:IncludeContent	<p>Durch dieses in [OASIS-DSS] (Abschnitt 3.5.7), definierte Element kann bei einer CMS-basierten Signatur das Einfügen des signierten Dokumentes in die Signatur angefordert werden.</p> <p><a href="#">Fehlt dieses Element oder ist der Wert = "'false', wird die Signaturvariante "detached" verwendet, ansonsten "enveloping".</a></p>
<b>Rückgabe</b> 		
	SIG:SignResponse	<p>Eine <code>SignResponse</code> kapselt den ausgeführten Signaturauftrag pro Dokument. Die Zuordnung</p>

		zwischen SignRequest und SignResponse erfolgt über die RequestID.
	CONSUMER:Status	Enthält den Status der ausgeführten Operation pro SignRequest.
	SIG:OptionalOutputs	<p>Enthält <del>(angelehnt an dss:OptionalOutputs)</del> optionale Ausgangsparameter.</p> <p><u>Dieses Element wird durch den Basis- und KTR-Consumer nicht befüllt.</u></p> 
	SIG:DocumentWithSignature	 <p><u>Pro SignResponse wird ein Element SIG:DocumentWithSignature gemäß [OASIS-DSS] (Abschnitt 3.5.8) zurückgeliefert, in dem das Dokument mit Signatur enthalten ist. Dabei werden die XML-Attribute des Elements SIG:Document auf dem zugehörigen SignRequest übernommen.</u></p> <p><u>Ist die Signatur nicht im Dokument enthalten, wird ein leeres Element Base64Data zurückgegeben. Die Signatur wird dann im Element dss:SignatureObject abgelegt.</u></p> <p><u>Wenn die Signatur im Dokument enthalten ist, wird das signierte Dokument im Feld Base64Data zurückgeliefert. In diesem Fall MUSS die dss:SignaturePtr-Alternative in dss:SignatureObject (vgl. [OASIS-DSS] Abschnitt 2.5) dazu genutzt werden, auf die in den Dokumenten enthaltenen Signaturen zu verweisen. Dieses Element wird durch den Basis- und KTR-Consumer nicht befüllt.</u></p>
	vr:VerificationReport	<u>Vom</u> <u>Dieses Element wird durch den</u> Basis- und KTR-Consumer nicht befüllt.

	dss:SignatureObject	<p>Enthält im Erfolgsfall die erzeugte Signatur in Form eines dss:SignatureObject-Elements gemäß [OASIS-DSS] (Abschnitt 3.2). Der Signaturwert wird im XML-Element dss:SignatureObject/dss:Base64Signature übergeben. Der Signatur-Typ (CMS Signatur) in dss:SignatureObject/dss:Base64Signature/@Type</p> <p>Die XML-Elemente dss:SignatureObject/ds:Signature dss:SignatureObject/dss:Timestamp dss:SignatureObject/dss:SignaturePtr dss:SignatureObject/dss:Other werden nicht verwendet.</p>
<b>Vorbedingungen</b>	Keine	
<b>Nachbedingungen</b>	Keine	

Tabelle 14: Tab\_Default\_Signaturverfahren

Dokument-Format	Signaturverfahren (und -variante)			
	Signaturverfahren	Signaturvariante	WAS wird signiert?	WO wird die Signatur abgelegt?
Alle	CAES	detached	gesamtes Binärdokument	außerhalb des Dokuments in der SignResponse

Das Signieren erfolgt durch Aufruf von PL\_TUC\_SIGN\_DOCUMENT\_nonQES {  
IDENTIFIKATOR = PrivateKeyOnCard;  
DOKUMENT = SIG:Document;  
DOKUMENTTYPE = dss:SignatureType;  
}

Die folgende Tabelle führt die zulässigen Zertifikate und Schlüssel für die nonQES auf:

Tabelle 14: Tab\_Zertifikate\_für\_Sign/VerifyDocument(nonQES)

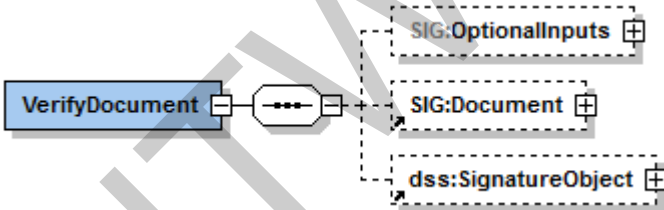
Karte	Crypt (Wert)	KeyReference (Verify)	KeyReference (Sign)
		in DF.ESIGN	in DF.ESIGN
	RSA	EF.C.HCI.OSIG.R2048	PrK.HCI.OSIG.R2048

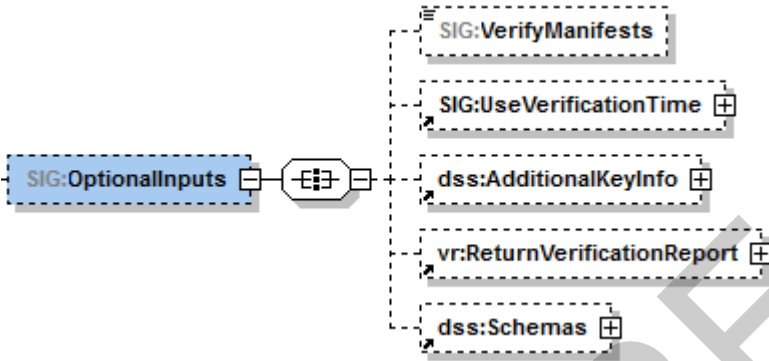
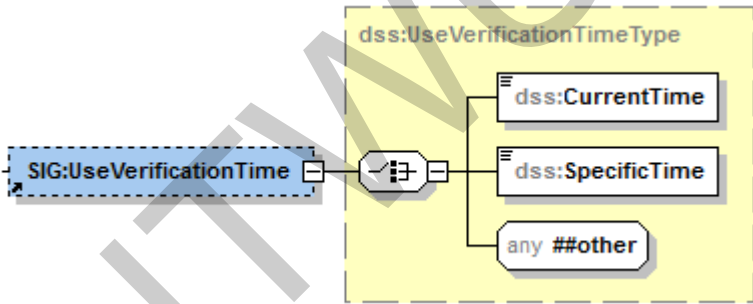
SM-B (KTR/Org) (HSM)	ECC	EF.C.HCI.OSIG.E256	PrK.HCI.OSIG.E256
	RSA_ECC	EF.C.HCI.OSIG.R2048 EF.C.HCI.OSIG.E256	PrK.HCI.OSIG.R2048 PrK.HCI.OSIG.E256

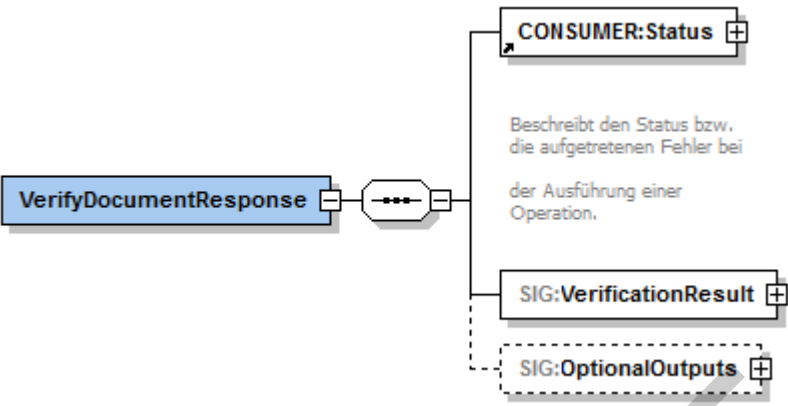
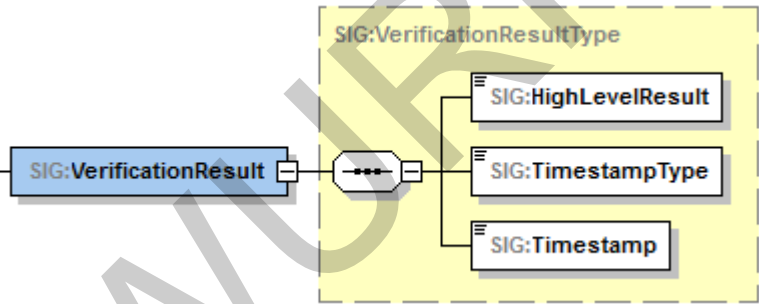
663 [ $\leq$ ]664 **6.2.2.2 VerifyDocument**665 **[A\\_17526-02A\\_17526-01](#) - Basis- und KTR-Consumer, Operation VerifyDocument**

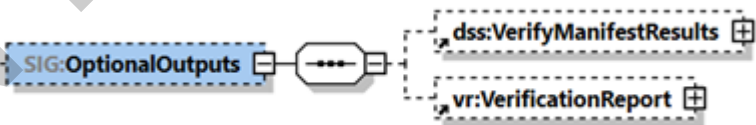
666 Der Signaturdienst des Basis- und KTR-Consumer MUSS an der Clientschnittstelle eine  
 667 Operation `VerifyDocument` wie in Tabelle `Tab_Operation_VerifyDocument` beschrieben  
 668 anbieten.

669 **Tabelle 15: Tab\_Operation\_VerifyDocument**

Name	VerifyDocument	
<b>Beschreibung</b>	<p>Diese Operation verifiziert die Signatur eines Dokumentes. Der Basis- und KTR-Consumer MUSS jede konform zur Clientschnittstelle <code>SignDocument</code> erzeugte Signatur durch <code>VerifyDocument</code> prüfen können. Das Ergebnis der Prüfung wird, wenn gefordert, in Form eines standardisierten Prüfberichts in einer <code>VerificationReport</code>-Struktur gemäß [OASIS-VR] zurückgeliefert.</p>	
<b>Aufrufparameter</b>		
	SIG:OptionalInputs	<p>Enthält optionale Eingabeparameter (angelehnt an <code>dss:OptionalInputs</code> gemäß [OASIS-DSS] Section 2.7): Die zulässigen optionalen Eingabeparameter sind unten erläutert.</p>
	SIG:Document	<p>Enthält im Fall der Prüfung von detached oder enveloped Signaturen das zur Signatur gehörende bzw. das diese umschließende Dokument (siehe [OASIS-DSS] Section 2.4.2 und oben).</p>
	dss:SignatureObject	<p>Enthält die zu prüfende Signatur, wenn sie nicht im Dokument selbst eingebettet ist ([OASIS-DSS] Kapitel 4.1). Die Signatur wird in <code>ss:Base64Signature</code> mit entsprechendem <code>Type</code>-Attribut (siehe <code>SignatureType</code>) übergeben, wobei der nachfolgende Werte unterstützt werden muss:</p>

<ul style="list-style-type: none"> <li>• <b>CMS-Signatur</b> <b>urn:ietf:rfc:5652</b></li> </ul>	
	
SIG: VerifyManifests	Durch das in [OASIS-DSS] (Abschnitt 4.5.1) definierte Element kann die Prüfung eines ggf. vorhandenen Manifests angefordert werden. Dieses Element wird durch den Basis-KTR-Consumer nicht verwendet.
	
SIG: UseVerification Time	Durch das in [OASIS-DSS] (Abschnitt 4.5.2) spezifizierte Element kann die Prüfung der Signatur bezüglich eines durch den Aufrufer bestimmten Zeitpunktes (Benutzerdefinierter_Zeitpunkt) erfolgen.
dss: AdditionalKeyInfo	Durch das in [OASIS-DSS] (Abschnitt 4.5.4) spezifizierte Element kann zusätzliches, für die Prüfung benötigtes, Schlüsselmaterial übergeben werden. Dieses Element wird durch den Basis-KTR-Consumer nicht verwendet.
vr: Return VerificationReport	Durch dieses in [OASIS-VR] spezifizierte Element kann die Erstellung eines ausführlichen Prüfberichtes angefordert werden.
<a href="#">dss:Schemas</a>	<a href="#">Dieses Element wird durch den Basis-KTR-Consumer nicht verwendet.</a>

<b>Rückgabe</b>	 <p>The diagram shows a blue box labeled <b>VerifyDocumentResponse</b> connected to a container box. This container box has three outputs: <b>CONSUMER:Status</b>, <b>SIG:VerificationResult</b>, and <b>SIG:OptionalOutputs</b> (which is dashed). A descriptive text states: "Beschreibt den Status bzw. die aufgetretenen Fehler bei der Ausführung einer Operation."</p>
Status	Enthält den Ausführungsstatus der Operation.
SIG: Verifi cation Result	 <p>The diagram shows a blue box labeled <b>SIG:VerificationResult</b> connected to a container box. This container box has three outputs: <b>SIG:HighLevelResult</b>, <b>SIG:TimestampType</b>, and <b>SIG:Timestamp</b>. The entire structure is enclosed in a yellow dashed box labeled <b>SIG:VerificationResultType</b>. A descriptive text states: "Das Element Sig:VerificationResult enthält das Ergebnis der Prüfung als Ampel, den Typ des zugehörigen angenommenen Signaturzeitpunkts und der angenommene Signaturzeitpunkt selbst."</p>
SIG: High Level Result	<p>Das Ergebnis der Prüfung (Ampelschaltung) mit folgenden Werten:</p> <ul style="list-style-type: none"> <li>• VALID: alle Signaturen sind gültig</li> <li>• INVALID: mindestens eine der Signaturen ist ungültig</li> <li>• INCONCLUSIVE: in allen anderen Fällen</li> </ul>

	SIG: Time stamp Type	<p>Der Typ des angenommenen Signaturzeitpunkts mit folgenden Werten:</p> <ul style="list-style-type: none"> <li>• <b>SIGNATURE_EMBEDDED_TIMESTAMP:</b> in der Signatur eingebetter Zeitpunkt Ermittelter_Signaturzeitpunkt_Eingebettet</li> <li>• <b>QUALIFIED_TIMESTAMP:</b> qualifizierter Zeitstempel über die Signatur Ermittelter_Signaturzeitpunkt_Qualifiziert</li> <li>• <b>SYSTEM_TIMESTAMP:</b> Systemzeit des <u>KonnektorsConsumers</u> bei Signaturprüfung Ermittelter_Signaturzeitpunkt_System</li> <li>• <b>USER_DEFINED_TIMESTAMP:</b> benutzerdefinierter Zeitpunkt Benutzerdefinierter_Zeitpunkt</li> </ul> <p>Als Format darf jedes zum XML-Typ "dateTime" konforme Format verwendet werden (&lt;element name="Timestamp" type="dateTime"/&gt;). Wenn mehrere Signaturen im Dokument vorhanden sind, wird hier der angenommene Signaturzeitpunkt der jüngsten Signatur angegeben.</p>
	SIG: Timestamp	Im Element SIG:Timestamp wird der zu SIG:TimestampType gehörende Zeitstempel zurückgegeben.
	SIG: Optional Outputs	<p>Enthält (angelehnt an dss:OptionalOutputs, wie in Abschnitt 2.7 von [OASIS-DSS] beschrieben) optionale Ausgangselemente:</p> 
	dss: Verify Manifest Results	Dieses in Abschnitt 4.5.1 von [OASIS-DSS] definierte Element enthält Informationen zur Prüfung eines ggf. vorhandenen Signaturmanifests und wird zurückgeliefert, sofern beim Aufruf das dss:VerifyManifest-Element, aber nicht das RequestVerificationReport als optionales Eingabeelement übergeben wurde.
	vr: Verificatio n Report	Dieses in [OASIS-VR] spezifizierte Element wird zurückgeliefert, falls das ReturnVerificationReport-Element als Eingabeparameter verwendet wurde.
<b>Vorbedingungen</b>	Keine	

<b>Nachbendungen</b>	Keine
----------------------	-------

SigningTime ist der zu prüfende Signaturzeitpunkt. Dieser ergibt sich wie folgt:

1. SigningTime = Benutzerdefinierter Zeitpunkt, wenn  
SIG:UseVerificationTime Angaben enthält, sonst
2. SigningTime = Ermittelter Signaturzeitpunkt Eingebettet wenn die Signatur  
einen Signaturzeitpunkt enthält, sonst
3. SigningTime = Ermittelter Signaturzeitpunkt System, die Systemzeit.

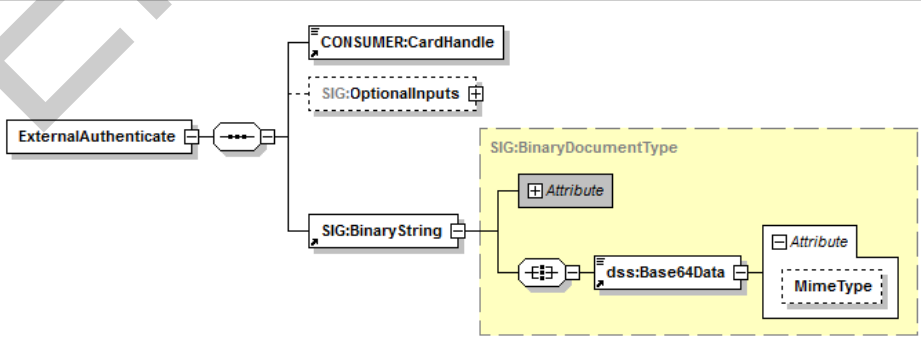
Das Verifizieren erfolgt durch Aufruf von PL\_TUC\_VERIFY\_DOCUMENT\_nonQES {  
 SIGNED\_DOCUMENT = SIG:Document;  
 CERTIFICATE = extrahiert aus SIG:Document;  
 SIGNATURE = dss: SignatureObject ;  
 TIME\_REFERENCE = ~~extrahierte~~ SigningTime ~~aus SIG:Document;~~  
 }.  
 [<=]

### 6.2.2.3 ExternalAuthenticate

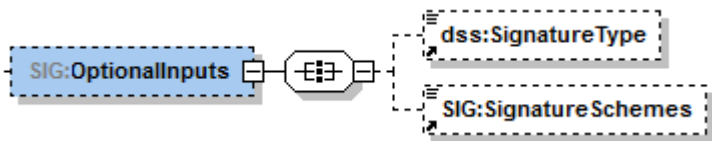
#### A\_17578 - Basis- und KTR-Consumer, Operation ExternalAuthenticate

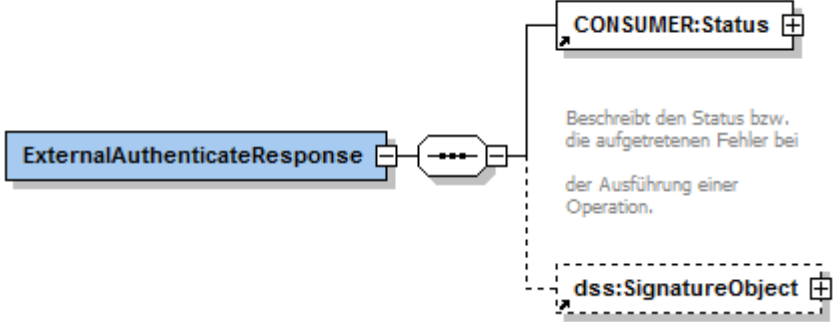
Der Signatordienst des Basis- und KTR-Consumer MUSS an der Clientschnittstelle die Operation ExternalAuthenticate wie in Tabelle Tab\_Operation\_ExternalAuthenticate beschrieben anbieten.

**Tabelle 16: Tab\_Operation\_ExternalAuthenticate**

Name	ExternalAuthenticate	
<b>Beschreibung</b>	Diese Operation versieht einen Binärstring der maximalen Länge 512 Bit mit einer nicht-qualifizierten elektronischen Signatur (nonQES). Dazu wird das Signaturverfahren PKCS#1 oder ECDSA verwendet.	
<b>Aufrufparameter</b>		
	<b>Name</b>	<b>Beschreibung</b>
	CONSUMER: CardHandle	Identifiziert die zu verwendende Signaturkarte.



SIG: Optional Inputs	<p>Enthält optionale Eingangsparameter:</p> 
SIG: Binary String	<p>Dieses Element enthält im Kindelement <code>dss:Base64Data</code> den zu signierenden Binärstring. Das XML Attribut <code>SIG:BinaryString/dss:Base64Data/@MimeType</code> MUSS den Wert "application/octet-stream" haben. Die maximale Länge des Binärstrings beträgt 512 Bit entsprechend der maximal zu erwartenden Hash-Größe.</p>
dss: Signature Type	<p>Durch dieses in [OASIS-DSS] (Abschnitt 3.5.1) beschriebene Element wird der Typ der zu erzeugenden Signatur bestimmt. Als Signatortyp wird unterstützt :</p> <ul style="list-style-type: none"> <li> <b>PKCS#1-Signatur</b> Durch Übergabe der URI <a href="urn:ietf:rfc:3447">urn:ietf:rfc:3447</a> wird eine PKCS#1 (Version 2.1) Signatur gemäß [RFC3447] erzeugt, die als <code>dss:Base64Signature</code> mit der oben genannten URI zurückgeliefert wird. </li> <li> <b>ECDSA-Signatur</b> Durch Übergabe der URI <a href="urn:bsi:tr:03111:ecdsa">urn:bsi:tr:03111:ecdsa</a> wird eine ECDSA Signatur gemäß [BSI-TR-03111]#4.2.1 erzeugt, die als <code>dss:Base64Signature</code> mit der oben genannten URI zurückgeliefert wird. </li> </ul> <p>Andere <code>SignatureType</code>-Angaben führen zu einer Fehlermeldung. Fehlt dieses Element, so wird ebenfalls der Signatortyp PKCS#1-Signatur verwendet.</p>
SIG: Signature Schemes	<p>Durch dieses Element wird für PKCS#1-Signaturen zwischen den folgenden SignatureScheme-Optionen unterschieden:</p> <ul style="list-style-type: none"> <li>RSASSA-PSS</li> <li>RSASSA-PKCS1-v1_5</li> </ul> <p>Fehlt dieses Element, so wird als Default-SignatureScheme RSASSA-PSS gewählt.</p>

Rückgabe		
	CONSUMER: Status	Enthält den Status der ausgeführten Operation.
	dss: Signature Object	<p>Enthält im Erfolgsfall die erzeugte Signatur in Form eines dss:SignatureObject-Elements gemäß [OASIS-DSS] (Abschnitt 3.2). Der Signaturwert wird im XML-Element dss:SignatureObject/dss:Base64Signature übergeben. Das XML-Attribut dss:SignatureObject/dss:Base64Signature/@Type kennzeichnet durch den Wert:</p> <ul style="list-style-type: none"> <li>• <a href="urn:ietf:rfc:3447">urn:ietf:rfc:3447</a> den Signatur-Typ PKCS#1</li> </ul> <p>bzw.</p> <ul style="list-style-type: none"> <li>• <a href="urn:bsi:tr:03111:ecdsa">urn:bsi:tr:03111:ecdsa</a> den Signatur-Typ ECDSA.</li> </ul> <p>Die XML-Elemente  dss:SignatureObject/ds:Signature  dss:SignatureObject/dss:Timestamp  dss:SignatureObject/dss:SignaturePtr  dss:SignatureObject/dss:Other  werden nicht verwendet.</p>
Vorbeding ungen	Keine	
Nachbeding ungen	Keine	

```

692
693 Das Signieren erfolgt durch Aufruf von PL_TUC_SIGN_HASH_nonQES {
694     IDENTIFIKATOR = CardHandle;
695     SIGNATURVERFAHREN = SIG:SignatureSchemes;
696     HASHWERT = SIG:BinaryString;
697 }
698 [<=]

```

## 6.3 Zertifikatsdienst

### 6.3.1 Durch Module nutzbare TUCs

#### A\_17401 - Systemprozess PL\_TUC\_PKI\_VERIFY\_CERTIFICATE

Der Basis- und KTR-Consumer MUSS den Systemprozess

PL\_TUC\_PKI\_VERIFY\_CERTIFICATE implementieren und bereitstellen. [ <= ]

### 6.3.2 Operationen an der Clientschnittstelle

#### A\_17408 - Basisdienst Zertifikatsdienst

Der Basis- und KTR-Consumer MUSS Clientsystemen einen Basisdienst Zertifikatsdienst zur Verfügung stellen.

**Tabelle 17: Tab\_Zertifikatsdienst**

Name	CertificateService	
Version	Siehe Anhang B	
Namensraum	Siehe Anhang B	
Namensraum-Kürzel	CERT für Schema und CERTW für WSDL	
Operationen	Name	Kurzbeschreibung
	VerifyCertificate	Prüfung des Status eines Zertifikats
WSDL	CertificateService.wsdl	
Schema	CertificateService.xsd	

[ <= ]

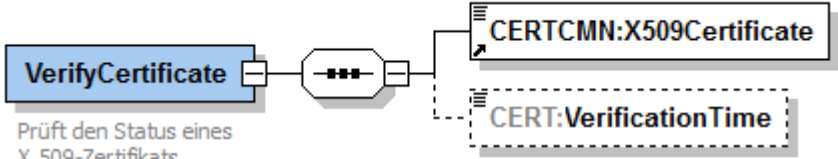
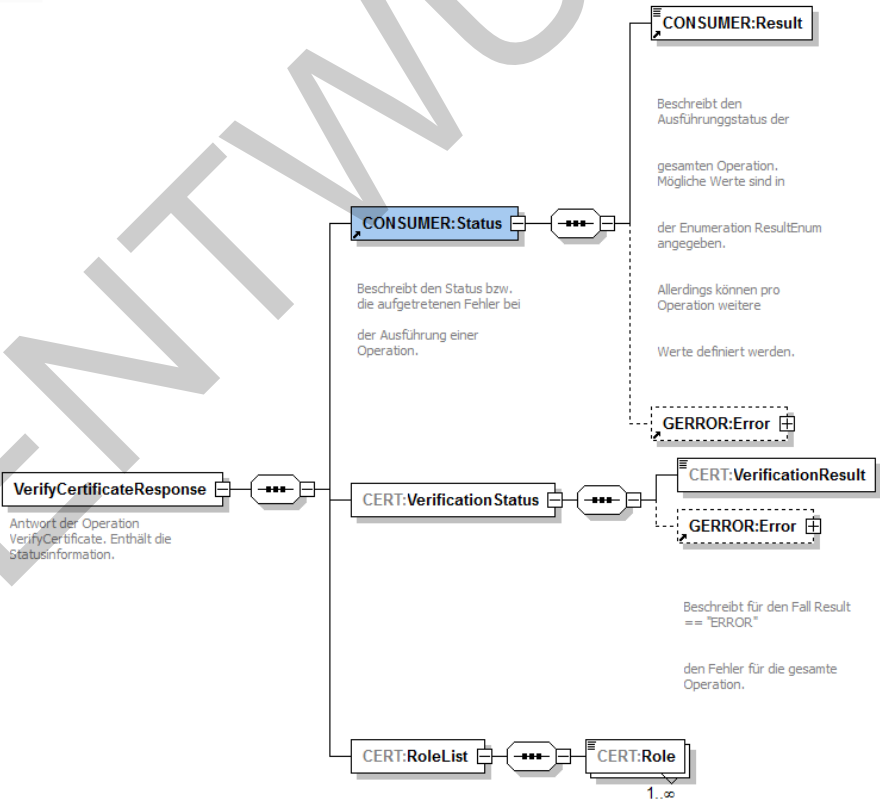
#### 6.3.2.1 VerifyCertificate

##### A\_17429-01 - Basis- und KTR-Consumer, Operation VerifyCertificate

Der Zertifikatsdienst des Basis- und KTR-Consumer MUSS an der Clientschnittstelle eine Operation `VerifyCertificate` wie in Tabelle `Tab_Operation_VerifyCertificate` beschrieben anbieten.

**Tabelle 18: Tab\_Operation\_VerifyCertificate**

Name	VerifyCertificate
Beschreibung	Prüft den Status eines Zertifikats.

<b>Aufruf- parameter</b>	<div data-bbox="432 293 1273 450">  </div> <table border="1"> <thead> <tr> <th>Name</th><th>Beschreibung</th></tr> </thead> <tbody> <tr> <td>CERTCMN: X509Certificate</td><td>Enthält das base64-codierte Zertifikat, dessen Binärstruktur wiederum ASN.1-codiert (gemäß [gemSpec_PKI]) vorliegt.</td></tr> <tr> <td>CERT: VerificationTime</td><td>Der für die Prüfung zu verwendende Referenzzeitpunkt. Falls der Parameter nicht angegeben ist, wird als Referenzzeitpunkt die Systemzeit verwendet.</td></tr> </tbody> </table>	Name	Beschreibung	CERTCMN: X509Certificate	Enthält das base64-codierte Zertifikat, dessen Binärstruktur wiederum ASN.1-codiert (gemäß [gemSpec_PKI]) vorliegt.	CERT: VerificationTime	Der für die Prüfung zu verwendende Referenzzeitpunkt. Falls der Parameter nicht angegeben ist, wird als Referenzzeitpunkt die Systemzeit verwendet.
Name	Beschreibung						
CERTCMN: X509Certificate	Enthält das base64-codierte Zertifikat, dessen Binärstruktur wiederum ASN.1-codiert (gemäß [gemSpec_PKI]) vorliegt.						
CERT: VerificationTime	Der für die Prüfung zu verwendende Referenzzeitpunkt. Falls der Parameter nicht angegeben ist, wird als Referenzzeitpunkt die Systemzeit verwendet.						
<b>Rückgabe</b>	<div data-bbox="432 1003 1315 1800">  </div> <table border="1"> <tbody> <tr> <td>Status</td><td>Enthält den Ausführungsstatus der Operation.</td></tr> </tbody> </table>	Status	Enthält den Ausführungsstatus der Operation.				
Status	Enthält den Ausführungsstatus der Operation.						

	CERT:VerificationStatus	Enthält eines der drei möglichen Prüfungsergebnisse in CERT:VerificationResult <ul style="list-style-type: none"> <li>• VALID</li> <li>• INCONCLUSIVE</li> <li>• INVALID</li> </ul> sowie weiter Details zu den Zuständen „INCONCLUSIVE“ und „INVALID“ in GERROR:Error.
	CERT:RoleList	OIDs der im Zertifikat gespeicherten Rollen.
<b>Vorbedingungen</b>	Keine	
<b>Nachbedingungen</b>	Keine	

718 Der Ablauf der Operation `VerifyCertificate` ist in Tabelle `Tab_Ablauf_VerifyCertificate`  
719 beschrieben:  
720

721 **Tabelle 19: Tab\_Ablauf\_VerifyCertificate**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	PL_TUC_PKI_VERIFY_CERTIFICATE	Die Zertifikatsprüfung erfolgt durch Aufruf von PL_TUC_PKI_VERIFY_CERTIFICATE { Zu prüfendes Zertifikat = CERTCMN:X509Certificate; Referenzzeitpunkt = CERT:VerificationTime; PolicyList = keine Einschränkung; KeyUsage = empty; ExtendedKeyUsage = empty; OCSP-Graceperiod = empty; Offline-Modus = nein; OCSP-Response = empty ; Timeout = empty; TOLERATE_OCSP_FAILURE = ja; }

2.	<p>Wenn der Prüfprozess fehlerhaft war und nicht zu einem Ergebnis im Sinne eines VerificationResult führt, wird eine FaultMessage erzeugt.</p> <p>War der Prüfprozess erfolgreich, wird eine VerifyCertificateResponse mit</p> <ul style="list-style-type: none"> <li>• CONSUMER:Status/CONSUMER:Result=OK,</li> <li>• dem VerificationStatus (als Ergebnis der Zertifikatsprüfung) und</li> <li>• den ermittelten Rollen-OIDs erzeugt.</li> </ul> <p>Ein Prüfergebnis „INCONCLUSIVE“ bzw. „INVALID“ wird in CERT:VerificationStatus/GERROR:Error mit den zugehörigen Fehlermeldungen detailliert (in diesem Fall kann CONSUMER:Status/CONSUMER:Result=OK oder CONSUMER:Status/CONSUMER:Result=Warning gesetzt sein).</p>
----	--

**Tabelle 20: Tab\_Übersicht\_VerificationResult\_VerifyCertificate**

CERT:VerificationResult	Bedeutung
VALID	Wenn Gültigkeit zu Referenzzeitpunkt: "gültig" Mathematische Gültigkeit: "gültig" OCSP-Prüfung: Online gültig
INVALID	Wenn mindestens ein Wert von (Gültigkeit zu Referenzzeitpunkt, Mathematische Gültigkeit, OCSP-Prüfung) „ungültig“, „Prüffehler“ oder „gesperrt“ ist.
INCONCLUSIVE	Wenn OCSP-Prüfung „unbekannt“ und die andere Werte „gültig“ sind.

[&lt;=]

## 6.4 LDAP-Proxy

### 6.4.1 Durch Module nutzbare TUCs

#### A\_17343 - Basis- und KTR-Consumer, LDAPv3 Operationen für interne Module

Der Basis- und KTR-Consumer MUSS für die in Tab\_Ldap\_TUC\_Mapping aufgelisteten Systemprozesse die entsprechenden LDAP-Operationen implementieren und zur Nutzung durch interne Module zur Verfügung stellen.

**Tabelle 21: Tab\_Ldap\_TUC\_Mapping**

LDAPv3-Operation	Systemprozess
------------------	---------------

Bind	PL_TUC_VZD_BIND
Unbind	PL_TUC_VZD_UNBIND
Search	PL_TUC_VZD_SEARCH
Abandon	PL_TUC_VZD_ABANDON

[<=]

## 6.4.2 Unterstützte LDAPv3-Operationen an der Clientschnittstelle

### A\_17341 - Basis- und KTR-Consumer, LDAPv3-Operationen an der Clientschnittstelle

Der Basis- und KTR-Consumer MUSS an der Client-Schnittstelle die folgenden LDAPv3-Operationen für den Zugriff auf den Verzeichnisdienst der TI gemäß [RFC4511] anbieten.

- Bind Operation
- Unbind Operation
- Search Operation
- Abandon Operation

Andere LDAPv3-Operationen MÜSSEN mit dem LDAP-Fehler unwillingToPerform (53) beantwortet werden.

Fehler MÜSSEN gemäß [RFC4511] #Appendix A behandelt werden. [<=]

## 6.5 Clientmodul KOM-LE

### 6.5.1 Allgemeine Anforderungen

#### A\_17298 - Synchronisation mit der Systemzeit der zentralen TI-Plattform

Das KOM-LE-Clientmodul MUSS sich unter Verwendung des Systemprozesses PL\_TUC\_NET\_SYNC\_TIME mit der Systemzeit des Zeitserver der zentralen TI-Plattform synchronisieren. [<=]

#### A\_17299 - Konfigurationsparameter

Das KOM-LE-Clientmodul MUSS die in Tabelle Tab\_Konf\_Param aufgelisteten Parameter über eine Managementoberfläche oder eine Konfigurationsdatei konfigurierbar gestalten und mit einer Standardkonfiguration entsprechend den Defaultwerten ausliefern.

**Tabelle 22: Tab\_Konf\_Param Standardkonfiguration**

Parameter	Beschreibung des Parameters	Defaultwert
ADDRESS_SMTP	URI SMTP-Server	-
ADDRESS_POP3	URI POP3-Server	-

PORT_SMTP	SMTP-Port für Clientsysteme	25
PORT_POP3	POP3-Port für Clientsysteme	995
SMTP_TIMEOUT_SERVER	Timeout für Antworten vom SMTP-Server auf SMTP-Kommandos	5 Minuten
SMTP_TIMEOUT_CLIENT	Timeout für das Warten auf neue SMTP-Kommandos vom Clientsystem	5 Minuten
POP3_TIMEOUT_SERVER	Timeout für Antworten vom POP3-Server auf POP3-Kommandos	5 Minuten
POP3_TIMEOUT_CLIENT	Timeout für das Warten auf neue POP3-Kommandos vom Clientsystem	5 Minuten
TTL_ENC_CERT	Time to Live für gecachte Verschlüsselungs-zertifikate	24 Stunden
TTL_EMAIL_ICCSN	Time to Live für gecachte Zuordnungen von E-Mail-Adressen der Sender bzw. Empfänger zu ICCSNs von deren HBAs/SM-Bs	30 Tage
TTL_PROTS	Time to Live für Protokolldateien.	30 Tage
PROT_PERF	Protokolldatei für Performance	JA

[<=]

### A\_17503 - Prüfung von TLS-Server-Zertifikaten

Das KOM-LE-Clientmodul MUSS für die Prüfung von TLS-Server-Zertifikaten der KOM-LE-Fachdienste den Systemprozess PL\_TUC\_PKI\_VERIFY\_CERTIFICATE des Basis- und KTR-Consumer benutzen.

[<=]

## 6.5.2 Senden von Nachrichten

### A\_17300 - Initialer SMTP-Dialog

Das KOM-LE-Clientmodul MUSS, nachdem die SMTP-Verbindung zwischen dem Clientsystem und dem Clientmodul aufgebaut wird und bis zum Punkt an dem das Clientsystem die Bestätigung des Erfolgs oder Misserfolgs seiner Authentifizierung erwartet, einen SMTP-Dialog entsprechend der Tabelle Tab\_SMTP\_Ant\_Init mit dem Clientsystem führen.



777 **Tabelle 23: Tab\_SMTP\_Ant\_Init Antworten Clientmodul im CONNECT-Zustand**

SMTP-Kommando (Clientsystem -> Clientmodul)	SMTP-Antwortcode (Clientmodul -> Clientsystem)
HELO	"250 OK" Antwortcode
EHLO	"250 OK" Antwortcode mit folgenden EHLO-Kennworten: SIZE <size> AUTH LOGIN PLAIN 8BITMIME ENHANCEDSTATUSCODES DSN und <size> gleich oder größer als 35882577
AUTH	Anmeldungsdaten erhalten und Verbindungsaufbau mit dem MTA beginnen
RSET, NOOP	„250 OK“ Antwortcode
MAIL, RCPT, DATA	„530 5.7.0“ Antwortcode (Authentication required)
QUIT	„221 OK“ Antwortcode senden und die Verbindung mit dem Clientsystem schließen
Andere Meldungen	„502 5.5.1“ Antwortcode (Invalid command)

778  
779  
780 [**<=**]781 **A\_17301 - Verbindungsaufbau mit dem SMTP-Servers**782 Das KOM-LE-Clientmodul MUSS für den Verbindungsaufbau mit dem SMTP-Server die  
783 Werte der Konfigurationsparameter ADDRESS\_SMTP und PORT\_SMTP verwenden. [**<=**]784 **A\_17302 - Authentisierung gegenüber dem SMTP-Server mit Benutzernamen  
785 und Passwort**786 Das KOM-LE-Clientmodul MUSS den Benutzernamen und das Passwort, die es vom  
787 Clientsystem erhalten hat, für die Authentisierung gegenüber dem SMTP-Server  
788 verwenden. [**<=**]789 **A\_17303 - Ergebnis des Verbindungsaufbaus mit dem SMTP-Server**790 Das KOM-LE-Clientmodul MUSS das Clientsystem über das Ergebnis des  
791 Verbindungsaufbaus mit dem MTA mit den in Tabelle Tab\_SMTP\_Verbindung  
792 beschriebenen SMTP-Antwortcodes informieren.793 **Tabelle 24: Tab\_SMTP\_Verbindung SMTP-Antwortcodes für MTA-Verbindungsaufbau**

Bedingung	SMTP-Antwortcode (Clientmodul -> Clientsystem)
Das Clientmodul hat sich erfolgreich gegenüber dem MTA mit den vom Clientsystem erhaltenen Anmeldungsdaten authentifiziert.	235 2.7.0 (Authentication successful)

Das Clientsystem verwendet für die SMTP-Authentifizierung einen anderen Mechanismus als PLAIN oder LOGIN.	504 5.7.4 (Security features not supported)
Die Verbindung zwischen dem Clientmodul und dem MTA kann nicht aufgebaut werden.	454 4.7.0 (Temporary authentication failure)
Die Authentifizierung gegenüber dem MTA schlägt fehl.	535 5.7.8 (Authentication credentials invalid)

794 [**<=**]

795

796 **A\_17305 - Verwenden von PL\_TUC\_SIGN\_DOCUMENT\_nonQES und**

797 **PL\_TUC\_HYBRID\_ENCIPHER**

798 Das KOM-LE-Clientmodul MUSS für das Signieren und Verschlüsseln der Nachrichten

799 entsprechend dem KOM-LE-S/MIME-Profil die

800 Systemprozesse PL\_TUC\_SIGN\_DOCUMENT\_nonQES und PL\_TUC\_HYBRID\_ENCIPHER

801 des Basis- und KTR-Consumers verwenden. [**<=**]

802 **A\_17306 - Vorgehen bei Signatur und Verschlüsselung einer KOM-LE Nachricht**

803 Das KOM-LE-Clientmodul MUSS zur Signatur und Verschlüsselung von KOM-LE

804 Nachrichten das folgende Vorgehen umsetzen:

- 805 1. Unter Verwendung des Systemprozesses PL\_TUC\_SIGN\_DOCUMENT\_nonQES des
- 806 Basis- und KTR-Consumers erzeugt das Clientmodul KOM-LE einen binären Opak-
- 807 signierten CMS-Container entsprechend dem KOM-LE-S/MIME-Profil.
- 808 2. Der binäre CMS-Container mit der signierten Nachricht wird als
- 809 „application/pkcs7-mime“ MIME-Einheit vom smime-type „signed-data“ mit dem
- 810 Content-Transfer-Encoding „binary“ verpackt.
- 811 3. Zur CMS-Verschlüsselung übergibt das KOM-LE-Clientmodul beim Aufruf des
- 812 Systemprozesses PL\_TUC\_HYBRID\_ENCIPHER die in Schritt zwei erzeugte
- 813 Nachricht als binär-Dokument. Als Antwort erhält das KOM-LE-Clientmodul einen
- 814 binären CMS-Container zurück.
- 815 4. Der aus der Verschlüsselung resultierende CMS-Container wird in eine
- 816 „application/pkcs7-mime“ MIME-Einheit vom smime-type „authenticated-
- 817 enveloped-data“ mit dem Content-Transfer-Encoding „base64“ verpackt.

818

819 [**<=**]

820 **A\_17327 - Signieren der Nachricht mit dem Schlüssel Prk.HCI.OSIG**

821 Das KOM-LE-Clientmodul MUSS für das Signieren einer KOM-LE-Nachricht den privaten

822 Schlüssel Prk.HCI.OSIG.R2048 der SM-B der jeweiligen Organisation (Kostenträger oder

823 Leistungserbringergorganisation) verwenden.

824 [**<=**]

825 **6.5.3 Empfangen von Nachrichten**

826 **A\_17328 - POP3-Dialog zur Authentifizierung**

827 Das KOM-LE-Clientmodul MUSS, nachdem die POP3-Verbindung zwischen dem

828 Clientsystem und dem Clientmodul aufgebaut wurde und bis zu dem Punkt an dem das

829 Clientsystem die Bestätigung des Erfolgs oder Misserfolgs seiner Authentifizierung

830 erwartet, einen POP3-Dialog entsprechend Tabelle Tab\_POP3\_Ant\_Init mit dem  
831 Clientsystem führen.

832 **Tabelle 25: Tab\_POP3\_Ant\_Init Antworten Clientmodul im CONNECT-Zustand**

Clientsystem -> Clientmodul	Clientmodul -> Clientsystem
CAPA	" +OK" Antwortcode mit folgenden CAPA Kennworten: TOP USER SASL PLAIN UIDL
USER, AUTH	Anmeldungsdaten erhalten und Verbindungsaufbau mit dem POP3-Server fortsetzen
QUIT	" + OK" Antwortcode senden und die Verbindung mit dem Clientsystem schließen
Andere Meldungen	" -ERR" Antwortcode

833  
834 [ $\leq$ ]

835 **A\_17329 - Verbindungsaufbau mit dem POP3-Servers**

836 Das KOM-LE-Clientmodul MUSS für den Verbindungsaufbau mit dem POP3-Server die  
837 Werte der Konfigurationsparameter ADDRESS\_POP3 und PORT\_POP3 verwenden. [ $\leq$ ]

838 **A\_17330 - Authentifizierung gegenüber POP3-Server mit Benutzernamen und**  
839 **Passwort**

840 Das KOM-LE-Clientmodul MUSS den Benutzernamen und das Passwort, die es vom  
841 Clientsystem erhalten hat, für die Authentifizierung gegenüber dem POP3-Server  
842 verwenden. [ $\leq$ ]

843 **A\_17331 - Ergebnis des Verbindungsaufbaus mit dem POP3-Server**

844 Das KOM-LE-Clientmodul MUSS das Clientsystem über das Ergebnis des  
845 Verbindungsaufbaus mit dem POP3-Server mit den in der Tabelle Tab\_POP3\_Verbindung  
846 beschriebenen POP3-Antwortcodes informieren.

847 **Tabelle 26: Tab\_POP3\_Verbindung Antwortcodes für POP3-Server-Verbindungsaufbau**

Bedingung	POP3 Antwortcode (Clientmodul -> Clientsystem)
Das Clientsystem hat sich erfolgreich gegenüber dem POP3-Server mit den vom Clientsystem erhaltenen Anmeldungsdaten authentifiziert.	+OK
Das Clientsystem verwendet für die POP3-Authentifizierung einen anderen Mechanismus als USER/PASS oder PLAIN.	-ERR
Die Verbindung zwischen dem Clientmodul und dem POP3-Server kann nicht aufgebaut werden.	-ERR
Die Authentifizierung gegenüber dem MTA schlägt fehl.	-ERR

848  
849

[<=]

850 **A\_17333 - E-Mail-Adresse des den Abholvorgang auslösenden Nutzers**

851 Das KOM-LE-Clientmodul MUSS den vom Clientsystem erhaltenen POP3-Usernamen als  
852 die E-Mail-Adresse des den Abholvorgang auslösenden Nutzers betrachten.[<=]

853 **A\_17504 - Verwenden von PL\_TUC\_VERIFY\_DOCUMENT\_nonQES und**  
854 **PL\_TUC\_HYBRID\_DECIPHER**

855 Das KOM-LE-Clientmodul MUSS für das Entschlüsseln und die Signaturprüfung der  
856 Nachrichten die Systemprozesse PL\_TUC\_VERIFY\_DOCUMENT\_nonQES und  
857 PL\_TUC\_HYBRID\_DECIPHER des Basis- und KTR-Consumers verwenden.

858 [<=]

859 **A\_17337 - Abbrechen des Entschlüsseln, wenn die erforderliche SM-B nicht**  
860 **verfügbar ist**

861 Das KOM-LE-Clientmodul MUSS die Entschlüsselung einer Nachricht abbrechen, wenn die  
862 für die Entschlüsselung erforderliche SM-B nicht verfügbar ist.[<=]

863 **A\_17338 - Abbrechen des Entschlüsseln, wenn Freischaltung der erforderlichen**  
864 **SM-B fehlschlägt**

865 Das KOM-LE-Clientmodul MUSS die Entschlüsselung einer Nachricht abbrechen, wenn die  
866 Freischaltung der für die Entschlüsselung erforderlichen SM-B fehlschlägt.[<=]

867 **6.6 Realisierung der Leistungen der TI-Plattform**

868 **A\_18130 - Nutzung von PL\_TUC\_CARD Systemprozessen**

869 Der Basis-Consumer MUSS für den Zugriff auf Smartcards die in TAB\_Systemprozesse  
870 mit PL\_TUC\_CARD\_\* bezeichneten Systemprozesse benutzen.

871 [<=]

872 **6.6.1 Transportschnittstelle für Kartenkommandos**

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

879 Die folgenden Anforderungen betreffen die gemäß  
880 [gemSpec\_Systemprozesse\_dezTI#ENV\_TUC\_CARD\_APDU\_TRANSPORT] zu  
881 beschreibende Transportschnittstelle.

882 **A\_18166 - Vertrauliche und integritätsgeschützte Kommunikation mit KT**

883 Wenn der Basis-Consumer Smartcards unterstützt, MUSS der Basis-Consumer mit dem  
884 Kartenterminal ausschließlich über eine vertrauliche, integritätsgeschützte Verbindung  
885 kommunizieren.[<=]

886 **A\_18097 - Transportschnittstelle für Kartenkommandos**

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

**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. [≤]

**A\_18163 - Kartenterminal für Basis-Consumer**

Wenn der Basis-Consumer Smartcards unterstützt, MUSS er mindestens ein Kartenterminal enthalten. [≤]

**A\_18102 - PIN-Eingabe nicht speichern**

Der Basis-Consumer DARF ein eingegebenes PIN-Geheimnis NICHT speichern. [≤]

**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. [≤]

**6.6.2 Schnittstelle für PIN-Operationen und Anbindung der Karten der TI**

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.

**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

[≤]

**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.

[<=]

**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. [<=]

953

## 7 Anhang A - Verzeichnisse

### 7.1 Abkürzungen

955 Abkürzungen

Kürzel	Erläuterung
aAdG	Andere Anwendungen des Gesundheitswesens
aAdG NetG-TI	Andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens
AZPD	Anbieter Zentrale Plattform Dienste
CMS	Cryptographic Message Syntax
HSM	Hardware Security Module
IPv4	Internet Protokoll Version 4
IPv6	Internet Protokoll Version 6
KOM-LE	Kommunikation für Leistungserbringer
LDAP	Leightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extensions
MTA	Mail Transfer Agent
POP3	Post Office Protocol Version 3
S/MIME	Secure/Multipurpose Internet Mail Extensions
SM-B	Security Module Typ B
SMTP	Simple Mail Transfer Protocol
TI	Telematikinfrastuktur

## 7.2 Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

## 7.3 Abbildungsverzeichnis

Abbildung 1: Systemkontext für Basis-/KTR-Consumer .....	10
Abbildung 1: Systemkontext für Basis-/KTR-Consumer .....	10

## 7.4 Tabellenverzeichnis

Tabelle 1 : Mapping der Netzwerksegmente .....	14
Tabelle 2 : TAB_CONS_687 DNS Forwards des DNS Servers .....	17
Tabelle 3: TAB_CONS_648 – TUC_CONS_362 „Liste der Dienste abrufen“ .....	18
Tabelle 4: Basisanwendung Namensdienst .....	19
Tabelle 5: Konfigurationsparameter Namensdienst .....	19
Tabelle 6: Einsehbare Konfigurationsparameter Namensdienst .....	20
Tabelle 7: Tab_Personalisierung_HSM – Personalisierung des HSM .....	21
Tabelle 8: Tab_Verschlüsselungsdienst .....	23
Tabelle 9: Tab_Operation_EncryptDocument .....	24
Tabelle 10: Tab_Operation_DecryptDocument .....	27
Tabelle 11: Tab_KeyReference_für_Encrypt/Decrypt .....	29
Tabelle 12: Tab_Signatordienst .....	30
Tabelle 13: Tab_Operation_SignDocument .....	30
Tabelle 14: Tab_Default_Signaturverfahren .....	35
Tabelle 15: Tab_Zertifikate_für_Sign/VerifyDocument(nonQeS) .....	35
Tabelle 16: Tab_Operation_VerifyDocument .....	36
Tabelle 17: Tab_Operation_ExternalAuthenticate .....	40
Tabelle 18: Tab_Zertifikatsdienst .....	43
Tabelle 19: Tab_Operation_VerifyCertificate .....	43
Tabelle 20: Tab_Ablauf_VerifyCertificate .....	45
Tabelle 21: Tab_Übersicht_VerificationResult_VerifyCertificate .....	46



984	<a href="#">Tabelle 22: Tab_Ldap_TUC_Mapping.....</a>	46
985	<a href="#">Tabelle 23: Tab_Konf_Param Standardkonfiguration.....</a>	47
986	<a href="#">Tabelle 24: Tab_SMTP_Ant_Init Antworten Clientmodul im CONNECT-Zustand.....</a>	49
987	<a href="#">Tabelle 25: Tab_SMTP_Verbindung SMTP-Antwortcodes für MTA-Verbindungsaufbau....</a>	49
988	<a href="#">Tabelle 26: Tab_POP3_Ant_Init Antworten Clientmodul im CONNECT-Zustand.....</a>	51
989	<a href="#">Tabelle 27: Tab_POP3_Verbindung Antwortcodes für POP3-Server-Verbindungsaufbau..</a>	51
990	<a href="#">Tabelle 28: Tab_Schema_Versionen Versionen der Schemas aus dem Namensraum des</a>	
991	<a href="#">Basis- und KTR-Consumers.....</a>	61
992	<a href="#">Tabelle 29: TAB_Systemprozesse—Verwendete Plattformleistungen.....</a>	62
993	<a href="#">Tabelle 1 : Mapping der Netzwerksegmente.....</a>	14
994	<a href="#">Tabelle 2 : TAB CONS 687 DNS-Forwards des DNS-Servers.....</a>	17
995	<a href="#">Tabelle 3: TAB CONS 648 – TUC CONS 362 „Liste der Dienste abrufen“.....</a>	18
996	<a href="#">Tabelle 4: Basisanwendung Namensdienst.....</a>	19
997	<a href="#">Tabelle 5: Konfigurationsparameter Namensdienst.....</a>	19
998	<a href="#">Tabelle 6: Einsehbare Konfigurationsparameter Namensdienst.....</a>	20
999	<a href="#">Tabelle 7: Tab Personalisierung HSM – Personalisierung des HSM.....</a>	21
1000	<a href="#">Tabelle 8: Tab Verschlüsselungsdienst.....</a>	23
1001	<a href="#">Tabelle 9: Tab Operation EncryptDocument.....</a>	24
1002	<a href="#">Tabelle 10: Tab Operation DecryptDocument.....</a>	27
1003	<a href="#">Tabelle 11: Tab KeyReference für Encrypt/Decrypt.....</a>	29
1004	<a href="#">Tabelle 12: Tab Signatordienst.....</a>	30
1005	<a href="#">Tabelle 13: Tab Operation SignDocument.....</a>	30
1006	<a href="#">Tabelle 14: Tab Zertifikate für Sign/VerifyDocument(nonQeS).....</a>	35
1007	<a href="#">Tabelle 15: Tab Operation VerifyDocument.....</a>	36
1008	<a href="#">Tabelle 16: Tab Operation ExternalAuthenticate.....</a>	40
1009	<a href="#">Tabelle 17: Tab Zertifikatsdienst.....</a>	43
1010	<a href="#">Tabelle 18: Tab Operation VerifyCertificate.....</a>	43
1011	<a href="#">Tabelle 19: Tab Ablauf VerifyCertificate.....</a>	45
1012	<a href="#">Tabelle 20: Tab Übersicht VerificationResult VerifyCertificate.....</a>	46
1013	<a href="#">Tabelle 21: Tab Ldap TUC Mapping.....</a>	46
1014	<a href="#">Tabelle 22: Tab Konf Param Standardkonfiguration.....</a>	47
1015	<a href="#">Tabelle 23: Tab SMTP Ant Init Antworten Clientmodul im CONNECT-Zustand.....</a>	49
1016	<a href="#">Tabelle 24: Tab SMTP Verbindung SMTP-Antwortcodes für MTA-Verbindungsaufbau....</a>	49
1017	<a href="#">Tabelle 25: Tab POP3 Ant Init Antworten Clientmodul im CONNECT-Zustand.....</a>	51
1018	<a href="#">Tabelle 26: Tab POP3 Verbindung Antwortcodes für POP3-Server-Verbindungsaufbau..</a>	51
1019	<a href="#">Tabelle 27: Tab Schema Versionen Versionen der Schemas aus dem Namensraum des</a>	
1020	<a href="#">Basis- und KTR-Consumers.....</a>	61

1021 [Tabelle 28: TAB Systemprozesse – Verwendete Plattformleistungen.....](#)62

1022 |

## 1023 7.5 Referenzierte Dokumente

### 1024 7.5.1 Dokumente der gematik

1025 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument  
 1026 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der  
 1027 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und  
 1028 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und  
 1029 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht  
 1030 aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in  
 1031 der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der  
 1032 die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemSMIME_KOMLE]	gematik: S/MIME-Profil Kommunikation Leistungserbringer(KOM-LE)
[gemSpec_CM_KOMLE]	gematik: Spezifikation KOM-LE-Clientmodul
[gemSpec_Systemprozesse_dezTI]	gematik: Spezifikation der Systemprozesse der dezentralen TI
[gemSpec_VZD]	gematik: Spezifikation Verzeichnisdienst
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemSpec_FM_ePA_KTR_Consumer]	gematik: Spezifikation Fachmodul ePA im KTR-Consumer
[gemSpec_PKI]	gematik: Übergreifende Spezifikation PKI

### 1033 7.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[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
<del>[RFC3275]</del>	<del>D. Eastlake, J. Reagle, D. Solo: (Extensible Markup Language) XML Signature Syntax and Processing, IETF RFC 3275, via <a href="http://www.ietf.org/rfc/rfc3275.txt">http://www.ietf.org/rfc/rfc3275.txt</a></del>
[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
[OASIS-DSS]	OASIS: Digital Signature Service Core Protocols, Elements, and Bindings, Version 1.0, OASIS Standard, via <a href="http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf">http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf</a>
[OASIS-SP]	OASIS: Signature Policy Profile of the OASIS Digital Signature Services Version 1.0, Committee Draft 01, 18 May 2009, <a href="http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy-cd01.pdf">http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy-cd01.pdf</a>
[OASIS-VR]	OASIS: Profile for comprehensive multi-signature verification reports for OASIS Digital Signature Services Version 1.0, Committee Specification 01, 12 November 2010, <a href="http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-VR-CS01.pdf">http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-VR-CS01.pdf</a>
<del>[XAdES]</del>	<del>European Telecommunications Standards Institute (ETSI): Technical Specification XML Advanced Electronic Signatures (XAdES). ETSI Technical Specification TS 101 903, Version 1.4.2, 2010</del>
<del>[XMLDSig]</del>	<del>W3C Recommendation (06.2008): XML Signature Syntax and Processing <a href="http://www.w3.org/TR/2008/REC-xmlsig-core-20080610/">http://www.w3.org/TR/2008/REC-xmlsig-core-20080610/</a></del>
[XMLEnc]	XML Encryption Syntax and Processing W3C Recommendation 11 April 2013 <a href="http://www.w3.org/TR/xmlenc-core1/">http://www.w3.org/TR/xmlenc-core1/</a>
[XPath]	W3C Recommendation (14 December 2010) XML Path Language (XPath) 2.0 (Second Edition) <a href="http://www.w3.org/TR/2010/REC-xpath20-20101214/">http://www.w3.org/TR/2010/REC-xpath20-20101214/</a>

[CMS]	Cryptographic Message Syntax (CMS), September 2009 <a href="http://tools.ietf.org/html/rfc5652">http://tools.ietf.org/html/rfc5652</a>
[Canon XML1.1]	Canonical XML Version 1.1 <a href="http://www.w3.org/TR/2008/REC-xml-c14n11-20080502/">http://www.w3.org/TR/2008/REC-xml-c14n11-20080502/</a>
[CAAdES]	ETSI: Electronic Signature Formats, Electronic Signatures and Infrastructures (ESI) – Technical Specification, ETSI TS 101 733 V2.2.1, 2008-07, via <a href="http://www.etsi.org">http://www.etsi.org</a>
[CT-API]	<a href="https://www.tuvt.de/de/aktuelles/beitraege-white-paper/card-terminal-application-programing-interface-fuer-chipkartenanwendungen//">https://www.tuvt.de/de/aktuelles/beitraege-white-paper/card-terminal-application-programing-interface-fuer-chipkartenanwendungen//</a>
[CCID]	<a href="https://usb.org.10-1-108-210.causewaynow.com/sites/default/files/DWG_Smart-Card_CCID_Rev110.pdf">https://usb.org.10-1-108-210.causewaynow.com/sites/default/files/DWG_Smart-Card_CCID_Rev110.pdf</a>

## 8 Anhang B – Übersicht über die verwendeten Versionen

Für den Fall, dass Schnittstellenversionen unterstützt werden müssen, die den gleichen TargetNamespace nutzen, kann der Basis- und KTR-Consumer zu diesen Schnittstellenversionen einheitlich einen SOAP-Endpunkt anbieten, der die höchste der Schnittstellenversionen implementiert.

**Tabelle 27: Tab\_Schema\_Versionen Versionen der Schemas aus dem Namensraum des Basis- und KTR-Consumers**

Schemas aus dem Namensraum des Basis- und KTR-Consumer „http://ws.gematik.de/consumer“		
Name	Versi on	TargetNamespace
CertificateService.wsdl	2.0.0	<a href="http://ws.gematik.de/consumer/CertificateService/WSDL/v2.0">http://ws.gematik.de/consumer/CertificateService/WSDL/v2.0</a>
CertificateService.xsd	2.0.0	<a href="http://ws.gematik.de/consumer/CertificateService/v2.0">http://ws.gematik.de/consumer/CertificateService/v2.0</a>
CertificateServiceCommon.xsd	1.0.0	<a href="http://ws.gematik.de/consumer/CertificateServiceCommon/v1.0">http://ws.gematik.de/consumer/CertificateServiceCommon/v1.0</a>
ConsumerCommon.xsd	2.0.0	<a href="http://ws.gematik.de/consumer/ConsumerCommon/v2.0">http://ws.gematik.de/consumer/ConsumerCommon/v2.0</a>
EncryptionService.wsdl	2.0.0	<a href="http://ws.gematik.de/consumer/EncryptionService/WSDL/v2.0">http://ws.gematik.de/consumer/EncryptionService/WSDL/v2.0</a>
EncryptionService.xsd	2.0.0	<a href="http://ws.gematik.de/consumer/EncryptionServiceCommon/v2.0">http://ws.gematik.de/consumer/EncryptionServiceCommon/v2.0</a>
SignatureService.wsdl	2.0.0	<a href="http://ws.gematik.de/consumer/SignatureService/WSDL/v2.0">http://ws.gematik.de/consumer/SignatureService/WSDL/v2.0</a>
SignatureService.xsd	2.0.0	<a href="http://ws.gematik.de/consumer/SignatureServiceCommon/v2.0">http://ws.gematik.de/consumer/SignatureServiceCommon/v2.0</a>

## 9 Anhang C – Übersicht der genutzten Systemprozesse

Der Basis- und KTR-Consumer verwendet u.a. die in Tabelle TAB\_Systemprozesse dargestellten Plattformleistungen aus [gemSpec\_Systemprozesse\_dezTI].

**Tabelle 28: 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

1048

ENTWURF