

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# Spezifikation KTR-AdV

Version: 1.3.0  
Revision: 58044  
Stand: 26.10.2018  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: gemSpec\_KTR-AdV

---

## Dokumentinformationen

---

### Änderungen zur Vorversion

Die Einarbeitungen gemäß der Änderungsliste P15.10.

### Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	02.08.17		Überarbeitung Online-Produktivbetrieb (Stufe 2.1)	gematik
1.1.0	20.02.18		Einarbeitung Änderungsliste P15.1	gematik
1.2.0	14.05.18		Einarbeitung Änderungsliste P15.2	gematik
	19.09.18		Einarbeitung Änderungsliste P15.10	gematik
1.3.0	26.10.18		freigegeben	gematik

## Inhaltsverzeichnis

<b>1</b>	<b>Einordnung des Dokumentes .....</b>	<b>7</b>
1.1	Zielsetzung .....	7
1.2	Zielgruppe .....	7
1.3	Geltungsbereich .....	7
1.4	Abgrenzungen .....	7
1.5	Methodik.....	8
<b>2</b>	<b>Systemüberblick .....</b>	<b>9</b>
2.1	Einordnung des Produkttyps in die Telematikinfrastruktur .....	9
2.2	Leistungen der TI-Plattform .....	10
<b>3</b>	<b>Systemkontext .....</b>	<b>12</b>
3.1	Akteure und Rollen.....	12
3.2	Nachbarsysteme.....	14
3.3	Ablaufumgebung .....	15
<b>4</b>	<b>Zerlegung des Produkttyps .....</b>	<b>17</b>
<b>5</b>	<b>Übergreifende Festlegungen .....</b>	<b>21</b>
5.1	Datenschutz und Sicherheit.....	21
5.1.1	Verarbeitung personenbezogener Daten .....	21
5.1.2	Absicherung der AdV-Komponenten.....	22
5.1.3	Verbindungsaufbau und Freischaltung eGK .....	23
5.1.4	Filterung von Kartenkommandos an die eGK.....	25
5.2	Logging .....	25
5.3	Nicht-funktionale Anforderungen.....	28
<b>6</b>	<b>Funktionsmerkmale .....</b>	<b>29</b>
6.1	Implementation der AdV Anwendungsfälle .....	29
6.1.1	AdV-Sitzung des Versicherten .....	31
6.1.1.1	AdV-Sitzung initialisieren .....	31
6.1.1.2	AdV-Sitzung beenden.....	37
6.1.2	Übergreifende Vorbedingungen .....	38
6.1.3	Hinweistext zu Fachanwendung .....	40
6.1.4	Generische Anwendungsfälle .....	41
6.1.4.1	Anwendung auf eGK deaktivieren.....	41
6.1.4.2	Anwendung auf eGK reaktivieren .....	45
6.1.4.3	PIN-Verwaltung .....	49
6.1.4.3.1	PIN ändern .....	49
6.1.4.3.2	PIN auf eGK entsperren .....	51

6.1.4.3.3	PIN für Fachanwendung einschalten .....	53
6.1.4.3.4	PIN für Fachanwendung ausschalten .....	56
6.1.5	Verwaltung der eGK .....	59
6.1.5.1	VSD von eGK anzeigen .....	59
6.1.5.2	Zugriffsprotokoll anzeigen .....	63
6.1.5.3	Versicherten-PIN ändern .....	66
6.1.5.4	Versicherten-PIN entsperren .....	67
6.1.5.5	Datenübertragung bei Kartentausch .....	69
6.1.6	Verwaltung der NFD .....	75
6.1.6.1	NFD auf eGK verbergen .....	75
6.1.6.2	Verborgenen NFD auf eGK sichtbar machen .....	76
6.1.6.3	PIN für NFD einschalten .....	77
6.1.6.4	PIN für NFD ausschalten .....	77
6.1.7	Verwaltung des DPE .....	78
6.1.7.1	Persönliche Erklärung (DPE) von eGK anzeigen .....	78
6.1.7.2	Persönliche Erklärung (DPE) auf eGK ändern .....	80
6.1.7.3	Persönliche Erklärung (DPE) auf eGK löschen .....	84
6.1.7.4	PIN für DPE einschalten .....	86
6.1.7.5	PIN für DPE ausschalten .....	87
6.1.7.6	Persönliche Erklärung (DPE) auf eGK verbergen .....	87
6.1.7.7	Verborgene DPE auf eGK sichtbar machen .....	88
6.1.8	Verwaltung eMP/AMTS .....	89
6.1.8.1	AMTS-Vertreter-PIN ändern .....	89
6.1.8.2	AMTS-Vertreter-PIN entsperren .....	90
6.1.8.3	eMP/AMTS Datensatz verbergen .....	90
6.1.8.4	Verborgenen eMP/AMTS Datensatz sichtbar machen .....	91
6.1.8.5	PIN für AMTS einschalten .....	92
6.1.8.6	PIN für AMTS ausschalten .....	92
6.1.9	Fachanwendungsunabhängige Anwendungsfälle .....	93
6.1.9.1	Mit eGK verschlüsseln .....	93
6.1.9.2	Mit eGK entschlüsseln .....	96
6.1.9.3	Authentisierungsrequest mit eGK signieren .....	98
6.1.9.4	Zertifikat von eGK lesen .....	101
<b>6.2</b>	<b>Realisierung der Leistungen der TI-Plattform .....</b>	<b>103</b>
6.2.1	Transportschnittstelle für Kartenkommandos .....	103
6.2.1.1	Kartenterminals der Sicherheitsklasse 1 .....	104
6.2.1.2	Kartenterminals der Sicherheitsklasse 2 .....	105
6.2.1.3	Kartenterminals der Sicherheitsklasse 3 .....	105
6.2.2	Schnittstelle für PIN-Operationen und Anbindung der Karten der TI .....	106
6.2.3	Schnittstelle zur Freischaltung der eGK .....	107
6.2.4	Schnittstelle zu Diensten der zentralen TI-Plattform .....	108
<b>6.3</b>	<b>Schnittstelle zwischen AdV-App und AdV-Server .....</b>	<b>110</b>
<b>6.4</b>	<b>Identitäten der KTR-AdV .....</b>	<b>110</b>
<b>7</b>	<b>Informationsmodell .....</b>	<b>113</b>
<b>8</b>	<b>Verteilungssicht .....</b>	<b>114</b>
<b>9</b>	<b>Anhang A – Verzeichnisse .....</b>	<b>115</b>
9.1	Abkürzungen .....	115

<b>9.2</b>	<b>Glossar .....</b>	<b>117</b>
<b>9.3</b>	<b>Abbildungsverzeichnis.....</b>	<b>117</b>
<b>9.4</b>	<b>Tabellenverzeichnis.....</b>	<b>118</b>
<b>9.5</b>	<b>Referenzierte Dokumente.....</b>	<b>120</b>
9.5.1	Dokumente der gematik.....	120
9.5.2	Weitere Dokumente .....	121
<b>9.6</b>	<b>Hinweistexte der Fachanwendungen .....</b>	<b>121</b>
<b>10</b>	<b>Anhang B – Leistungen der dezentralen TI-Plattform .....</b>	<b>127</b>
<b>10.1</b>	<b>Systemprozesse für den Zugriff auf Smartcards der TI.....</b>	<b>128</b>
10.1.1	Die Realisierungsumgebung des CardProxy .....	129
10.1.1.1	ENV_TUC_CARD_SECRET_INPUT – Realisierung Eingabe PIN-Geheimnis	129
10.1.1.2	ENV_TUC_CARD_TO_CARD – Realisierung Card-2-Card.....	129
10.1.1.3	ENV_TUC_CARD_APDU_TRANSPORT – Realisierung APDU-Transport	130
10.1.2	Konfiguration und Statusinformationen .....	130
10.1.2.1	Konfiguration des CardProxy .....	130
10.1.2.2	Initialisierung CardProxy für eGK.....	131
10.1.2.3	Initialisierung CardProxy für SM-B.....	131
10.1.2.4	PL_TUC_CARD_INFORMATION – Gesammelte Statusinformationen zu einer Karte.....	132
10.1.2.5	PL_TUC_EGK_STATUS – Gültigkeit der eGK prüfen.....	135
10.1.2.6	PL_TUC_CARD_RESET – Rücksetzen einer Karte .....	137
10.1.3	Zugriff auf Smartcards der TI .....	137
10.1.3.1	PL_TUC_CARD_CHANGE_PIN – PIN Ändern.....	137
10.1.3.2	PL_TUC_CARD_ENABLE_PIN – PIN-Schutz einschalten .....	138
10.1.3.3	PL_TUC_CARD_DISABLE_PIN – PIN-Schutz abschalten .....	138
10.1.3.4	PL_TUC_CARD_UNBLOCK_PIN – PIN mit PUK entsperren .....	139
10.1.3.5	PL_TUC_CARD_VERIFY_PIN – Benutzer verifizieren .....	140
10.1.3.6	PL_TUC_CARD_ACTIVATE_APPLICATION – Anwendung aktivieren	140
10.1.3.7	PL_TUC_CARD_DEACTIVATE_APPLICATION – Anwendung deaktivieren.....	141
10.1.3.8	PL_TUC_CARD_GET_CHALLENGE – Auslesen einer Zufallszahl..	141
10.1.3.9	PL_TUC_CARD_READ_FILE – Lesen von Daten aus einer SmartCard	142
10.1.3.10	PL_TUC_CARD_WRITE_FILE – Schreiben von Daten auf eine SmartCard	143
10.1.3.11	PL_TUC_CARD_UPDATE_FILE – Aktualisieren von Daten in einer transparenten Datei einer SmartCard.....	143
10.1.3.12	PL_TUC_CARD_DELETE_FILE – Löschen von Daten auf einer SmartCard	144
10.1.3.13	PL_TUC_CARD_ERASE_FILE – Rücksetzen des Inhalts einer transparenten Datei.....	145
10.1.3.14	PL_TUC_CARD_READ_RECORD – Lesen von Daten aus einer strukturierten Datei.....	145
10.1.3.15	PL_TUC_EGK_READ_PROTOCOL – Auslesen des Zugriffprotokolls der eGK	146
10.1.3.16	PL_TUC_CARD_WRITE_RECORD – Schreiben von Daten in eine strukturierte Datei.....	147

10.1.3.17	PL_TUC_CARD_APPEND_RECORD – Anfügen von Daten an eine strukturierte Datei.....	148
10.1.3.18	PL_TUC_EGK_APPEND_PROTOCOL – Zugriff auf der eGK protokollieren.....	148
10.1.3.19	PL_TUC_CARD_DELETE_RECORD – Löschen von Daten in einer strukturierten Datei.....	150
10.1.3.20	PL_TUC_CARD_ERASE_RECORD – Rücksetzen eines Datensatzes in einer strukturierten Datei .....	151
10.1.4	Transparenter Zugriff auf eine SmartCard .....	152
10.1.4.1	PL_TUC_CARD_TC_OPEN.....	152
10.1.4.2	PL_TUC_CARD_TC_SEND .....	152
10.1.4.3	PL_TUC_CARD_TC_CLOSE.....	153
<b>10.2</b>	<b>Kommunikation und Vernetzung.....</b>	<b>153</b>
10.2.1	PL_TUC_TLS_SECURE_CHANNEL – Kartenbasierte TLS-Verbindung .....	153
10.2.2	PL_TUC_NET_NAME_RESOLUTION.....	156
10.2.3	PL_TUC_NET_SYNC_TIME .....	156
<b>10.3</b>	<b>Vertraulichkeit, Authentizität, Integrität .....</b>	<b>156</b>
10.3.1	PL_TUC_SIGN_HASH_nonQES – mit Karten-Identität signieren .....	156
10.3.2	PL_TUC_HYBRID_ENCIPHER – Hybrid verschlüsseln.....	157
10.3.3	PL_TUC_HYBRID_DECIPHER – Hybrid entschlüsseln.....	158
10.3.4	PL_TUC_SIGN_DOCUMENT_nonQES – Dokument signieren .....	160
<b>10.4</b>	<b>Leistungen der PKI.....</b>	<b>160</b>
10.4.1	PL_TUC_PKI_VERIFY_CERTIFICATE – Prüfung eines Zertifikats der TI .....	160

---

## 1 Einordnung des Dokumentes

---

### 1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps KTR-AdV.

### 1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter einer KTR-AdV sowie Hersteller und Anbieter von Produkttypen der TI, die hierzu eine Schnittstelle besitzen.

### 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 dem Produkttyp 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 9.5).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps KTR-AdV verzeichnet.

## 1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:

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

Text / Beschreibung

[<=]

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

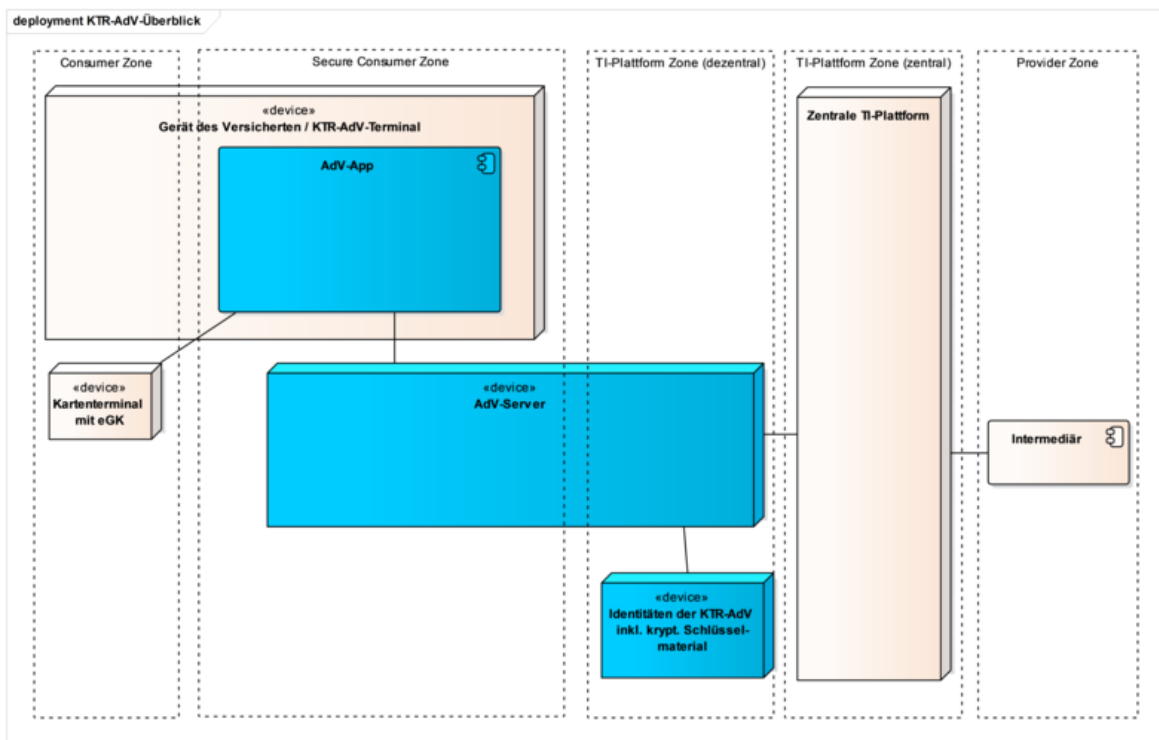


## 2 Systemüberblick

### 2.1 Einordnung des Produkttyps in die Telematikinfrastuktur

Für die eigenständige Verwaltung der Anwendungen des Versicherten auf der elektronischen Gesundheitskarte steht dem Versicherten in einer Umgebung im Auftrag der Kostenträger und @home die KTR-AdV zur Verfügung.

Mit dieser wird der Versicherte in die Lage versetzt, eigenständig seine persönlichen Daten auf der eGK einzusehen, seine freiwilligen Anwendungen zu verwalten, sowie administrative Anwendungsfälle der PIN-Verwaltung auszuführen. Die Abbildung ABB\_ADV\_300 zeigt die Einordnung des Produkttyps in die Telematikinfrastuktur.



**Abbildung 1: ABB\_ADV\_300 – Überblick AdV in einer Umgebung im Auftrag der Kostenträger**

Die KTR-AdV gliedert sich in die beiden blau dargestellten Komponenten AdV-App und AdV-Server sowie eine Komponente zur sicheren Speicherung der Kostenträgeridentitäten und des dazugehörigen kryptografischen Schlüsselmaterials (z.B. in einem HSM). Auf einem Gerät für die Benutzung durch den Versicherten wird die AdV-App zur Anbindung der eGK bereitgestellt. Diese AdV-App baut über eine produkttyp-interne Schnittstelle eine Verbindung zum zugehörigen AdV-Server auf, der im Auftrag einer Krankenkasse in einem Rechenzentrum betrieben wird.

Zur Freischaltung der eGK des Versicherten für die Umgebung der Kostenträger wird ein CV-Zertifikat des Kostenträgers mit einem Profil „KTR-AdV“ mit entsprechendem

Schlüsselmaterial verwendet, das über ein Card-to-Card-Verfahren den Zugriff für die Anwendungsfälle auf der eGK gewährt.

#### **AdV-A\_2532 - Freischaltung der eGK**

Die KTR-AdV MUSS für die Freischaltung der eGK ein CV-Zertifikat mit dem Profil „KTR-AdV“ verwenden.[<=]

Daraus folgt, dass kein anderes Zugriffsprofil für die Freischaltung der eGK verwendet werden darf .

## **2.2 Leistungen der TI-Plattform**

Dem Produkttyp KTR-AdV stehen keine dedizierten, benachbarten Produkttypen zur Realisierung der Leistung der TI-Plattform (z.B. Konnektor) zur Verfügung. Die KTR-AdV muss die Verfahren und Systemprozesse der TI-Plattform, wie den Zugriff auf Smartcards und Zugriffe auf zentrale Dienste, implementieren.

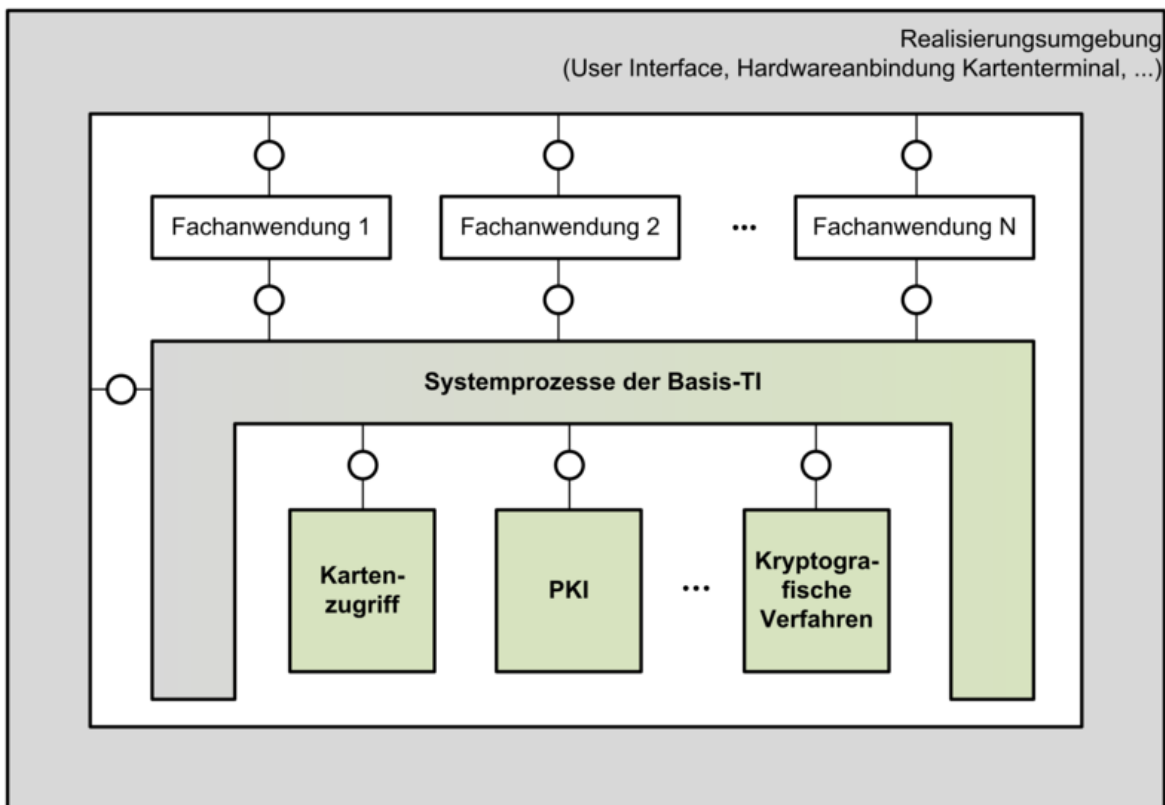
Über die logische Komponente TIP-Consumer-Adapter stehen die Schnittstellen und Dienste der zentralen TI-Plattform zur Verfügung. Die Anbindung der eGK des Versicherten an die AdV-App und die kryptografische Verwendung der Identitäten der Kostenträger im AdV-Server erfolgen über eine logische Zugriffsschicht zur Kapselung plattformspezifischer Aspekte in Systemprozessen der TI-Plattform (vgl. Abbildung ABB\_ADV\_304).

Zur Anbindung der eGK an die AdV-App soll auf Geräten des Versicherten ein einfaches kontaktbehaftetes oder kontaktloses Kartenterminal angenommen werden, das seinerseits nicht notwendigerweise über Sicherheitsmerkmale verfügt. Wird die AdV-App in einem KTR-AdV-Terminal betrieben, dann erfolgt die Anbindung der eGK über ein Kartenterminal mit Sicherheitsmerkmalen (Display und PIN-Pad).

Zur Bildung eines Vertrauensraumes steht der KTR-AdV die PKI der TI zur Verfügung. Sie setzt die Mechanismen der PKI zum Aufspannen eines Vertrauensraums um. Die zertifikatsbasierte Authentisierung in Verbindung mit den kryptografischen Verfahren der TI dient der Sicherstellung des Datenschutzes, der Integrität und der Vertraulichkeit der Daten des Versicherten.

In einer Leistungserbringerumgebung stellt der Konnektor den Fachmodulen der Fachanwendungen Schnittstellen und Dienste der TI-Plattform bereit, welche diese zur Abbildung fachlicher Anwendungsfälle nutzen. Der Konnektor kapselt zusätzlich den Zugriff auf Smartcards und steuert die Kommunikation mit den entsprechenden Kartenterminals. Im Gegensatz dazu wird die Fachlogik der Fachanwendungen in der KTR-AdV mit der für die Umsetzung notwendigen Logik der dezentralen TI-Plattform in einem einzigen Produkttyp realisiert. Die Umsetzung der Fachlogik der Fachanwendungen kann sich auf AdV-App und AdV-Server verteilen.

Die von den Fachanwendungen benötigte Logik der dezentralen TI-Plattform wird in Form von Systemprozessen beschrieben. Diese stellen eine Leistungsbeschreibung dar, ohne Vorgaben an konkrete Realisierungsdetails zu machen. Sie setzen sich aus Logik-Bausteinen der verschiedenen Domänen der TI-Plattform (Karten, PKI, Kryptografie, etc.) zusammen und beschreiben fachliche Zusammenhänge. Die Fachmodule der Fachanwendungen setzen ihre fachanwendungsspezifischen Operationen in der KTR-AdV um, in dem sie auf die entsprechenden Systemprozesse verweisen. Die folgende Abbildung ABB\_ADV\_304 zeigt diesen Zusammenhang, ohne eine Vorgabe an die Modularisierung einer KTR-AdV-Software zu machen.



**Abbildung 2: ABB\_ADV\_304 – Zusammenhang Systemprozesse und Fachanwendung**

In Abhängigkeit von der Ablaufumgebung, z.B. dem verwendeten Kartenterminal, sind für das Funktionieren der Systemprozesse zusätzliche Umgebungsparameter oder umgebungsspezifische Operationen erforderlich. Diese werden als Eingabe- bzw. Ausgabeschnittstellen in den Systemprozessen aufgerufen und führen zu einem Tailoring (Zuschnitt) der Leistung der TI-Plattform auf eine an die Umgebung der Kostenträger angepasste „AdV-Plattform.“ Die KTR-AdV muss diese Schnittstellen als Umgebung zur Realisierung der Leistungen der TI-Plattform implementieren (Realisierungs-umgebung).

Die Spezifikation der Systemprozesse findet sich in diesem Dokument in Anhang B. Es werden Anforderungen an die zu erbringende Leistung gestellt, ohne Vorgaben zu den zu verwendenden Technologien zu machen. Die Ausgestaltung und Modularisierung zwischen logischer Plattformebene, Kapselung von Fachlogik der weiteren Fachanwendungen sowie der gesicherten Schnittstelle zwischen AdV-App und AdV-Server obliegt dem Hersteller einer Lösung der KTR-AdV.

## 3 Systemkontext

### 3.1 Akteure und Rollen

Im Systemkontext der KTR-AdV interagieren verschiedene Akteure (aktive Komponenten) in unterschiedlichen Rollen mit der KTR-AdV. Die folgenden Akteure interagieren mit der KTR-AdV:

- **Nutzer**  
Ein Nutzer ist eine natürliche Person, die Anwendungsfälle in der KTR-AdV startet
- **Ausführungsumgebung**  
wird durch ein Gerät mit einem Betriebssystem gebildet, das die Teilkomponente AdV-App auf Seiten des Versicherten ausführt
- **Kartenterminals**  
ist eine technische Komponente zur Anbindung der eGK des Versicherten, um mit dieser die KTR-Anwendungsfälle auszuführen
- **Smartcards**  
Smartcards der TI sind Teil der dezentralen TI-Plattform und sind an die KTR-AdV zur Unterstützung der KTR-AdV-Anwendungsfälle angeschlossen
- **Zentrale TI-Plattform**  
Die Dienste der zentralen TI-Plattform unterstützen die KTR-AdV in der Ausführung der KTR-AdV-Anwendungsfälle.
- **Fachdienste**  
sind technische Komponenten, die im Rahmen fachanwendungsspezifischer Anwendungsfälle des Versicherten aufgerufen werden

Die folgende Tabelle TAB\_ADV\_300 listet diejenigen Akteure auf, die in verschiedenen Rollen mit der KTR-AdV interagieren.

**Tabelle 1: TAB\_ADV\_300 – Akteure und ihre Rollen**

Akteur	Rolle	Beschreibung
Nutzer	Versicherter	Primärer Anwender, Nutzung von fachlichen Anwendungsfällen für Zugriff auf Daten der eGK  Hinweis: Der Vertreter des Versicherten für AMTS ist kein Akteur in AdV. Ihm werden keine Anwendungsfälle bereitgestellt.

	Rollen für Administration und Betrieb	<p>Sekundärer Anwender, führt Administrations- und Betriebsaufgaben für die KTR-AdV durch, wie z. B.</p> <ul style="list-style-type: none"> <li>• Installation des Systems und von Updates,</li> <li>• Konfiguration des Systems,</li> <li>• Administration von Nutzern (jedoch nicht von Versicherten),</li> <li>• täglicher Betrieb,</li> <li>• Herstellen und Wahren der Betriebsbereitschaft (z. B. Freischaltung der SM-B(s)).</li> </ul> <p>Die Ausführung dieser Anwendungsfälle muss mit gesonderten Zugriffsrechten erfolgen.</p>
Ausführungsumgebung	KTR-AdV-Terminal	Interaktives Gerät für Zugang zu mittels eGK gespeicherten Daten des Versicherten durch den Versicherten zur Wahrnehmung der Rechte auf informationelle Selbstbestimmung
	Gerät des Versicherten	Gerät des Versicherten, dass u.a. für Zugang zu mittels der eGK gespeicherten Daten zur Wahrnehmung der Rechte auf informationelle Selbstbestimmung ermöglicht
Anbieter	Organisatorische Rolle, kein Akteur in der Ausführung von Anwendungsfällen	Hat die Betriebsverantwortung eines Produkts des Produkttyps KTR-AdV
Betreiber	Organisatorische Rolle, kein Akteur in der Ausführung von Anwendungsfällen	Der Betreiber eines konkreten Produkts, in dessen Betriebsumgebung die Teilkomponente AdV-Server (und ggfs. KTR-AdV-Terminals) betrieben werden

Der Nutzer kann in verschiedenen Rollen aktiv werden. Als Versicherter nimmt der Nutzer seine Datenschutzrechte auf informationelle Selbstbestimmung wahr, indem er fachliche Anwendungsfälle zum Anzeigen und ggfs. Bearbeiten der mittels seiner eGK gespeicherten Daten startet. Die Nutzer mit den Rollen Administration und Betrieb stellen die technische Betriebsbereitschaft der KTR-AdV her, d. h. sie konfigurieren das System für die Inbetriebnahme und stellen während des Betriebs die Betriebsbereitschaft sicher.

#### **AdV-A\_2571 - Rollen- und Berechtigungskonzept der KTR-AdV**

Der Anbieter einer KTR-AdV MUSS – als Teil des Sicherheitskonzepts – ein Rollen- und Berechtigungskonzept erstellen, welches die Administrations- und Betriebsaufgaben der KTR-AdV abdeckt. [≤]

**AdV-A\_2533 - Kartenbezogene Benutzerrollen der KTR-AdV**

Die KTR-AdV MUSS für die Benutzerverifikation für den Zugriff auf eine Karte der TI ein entsprechendes PIN-Objekt der passenden Rolle der folgenden Benutzer verwenden:

- Versicherter, für den Zugriff auf Objekte einer eGK
- Berechtigte Nutzer für Administrations- und Betriebsaufgaben, für den Zugriff auf privates Schlüsselmateriale der SM-B-Identitäten

Andere, nicht zu diesen Rollen passende PIN-Objekte, DÜRFEN NICHT verwendet werden.[<=]

Gemäß den Festlegungen in [gemSpec\_eGK\_ObjSys#5.3.10] darf die MRPIN.home nur außerhalb der TI verwendet werden. Im Produkttyp KTR-AdV als Teil der TI findet sie somit keine Verwendung.

Für die Benutzerverifikation der Rolle des Versicherten wird die PIN.CH verwendet.

Die Ausführungsumgebung kann zwei verschiedene Ausprägungen haben und bezieht sich auf die Ausführung der Teilkomponente AdV-App. Als KTR-AdV-Terminal wird sie von einem Betreiber verantwortet und muss eine bestimmte Sicherheitsleistung erbringen, um die mittels der eGK gespeicherten Daten des Versicherten zu schützen. Das KTR-AdV-Terminal wird als separater Produkttyp der TI spezifiziert. Im Gegensatz dazu ist ein *Gerät des Versicherten* ein beliebiges Gerät im Zugriff des Versicherten. Hier obliegt es dem Versicherten, die mittels seiner eGK gespeicherten Daten durch geeignete Maßnahmen zu schützen, da die hier spezifizierten Sicherheitsaspekte nur bis in die beim Versicherten ausgeführte Softwarekomponente AdV-App durchgesetzt werden können.

## 3.2 Nachbarsysteme

Die von der KTR-AdV erreichbaren Produkttypen der TI sind

- SM-B-Identitäten der KTR-AdV,
- eGK (G2 und höher),
- SZZP,
- Dienste der zentralen TI-Plattform und
- Fachdienste.

Die SM-B-Identitäten werden in der KTR-AdV benötigt, um auf der eGK des Versicherten erweiterte Zugriffsrechte freizuschalten und Verbindungen zu Fachdiensten und zu Diensten der zentralen TI-Plattform aufzubauen. Die Dienste der zentralen TI-Plattform und Fachdienste sind beispielsweise an den Anwendungsfällen zur Gültigkeitsprüfung und Aktualisierung der eGK des Versicherten beteiligt. Die Einbeziehung der SM-B-Identitäten der KTR-AdV muss unter Verwendung eines sicheren Speichers des kryptografischen Schlüsselmateriale der verwendeten Identitäten erfolgen.

Die Außenschnittstellen des Produkttyps KTR-AdV sind in der Abbildung ABB\_ADV\_301 dargestellt und im Folgenden aufgelistet:

- Die Schnittstelle zu einem Kartenterminal, wie in Abschnitt 6.2.1 beschrieben.
- Die Schnittstellen des Consumer Adapters zu den zentralen Diensten der TI, wie in Abschnitt 6.2.4 beschrieben.
- Eine grafische Benutzeroberfläche, deren Aspekte in den jeweiligen Anwendungsfällen in Abschnitt 6.1 beschrieben sind.

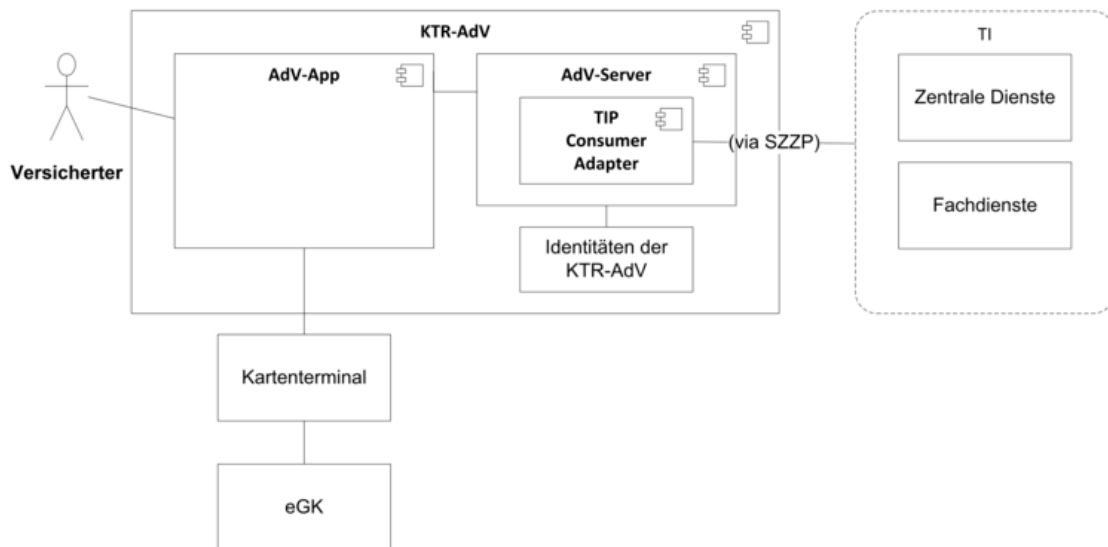


Abbildung 3: ABB\_ADV\_301 – Kontextdiagramm

### 3.3 Ablaufumgebung

Die Komponenten der KTR-AdV werden in verschiedenen Umgebungen betrieben, die in ABB\_ADV\_303 dargestellt sind.

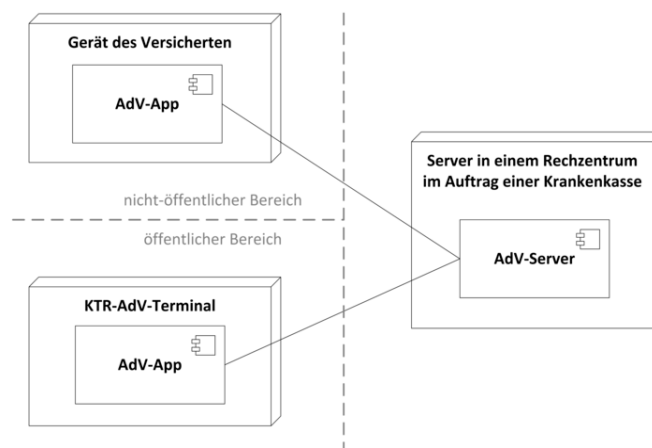


Abbildung 4: ABB\_ADV\_303 – Verteilungsdiagramm

Die Komponente „AdV-Server“ wird in einem Rechenzentrum betrieben:

**AdV-A\_2403 - AdV-Server: Betrieb in Rechenzentrum im Auftrag der Krankenkassen**

Der Anbieter einer AdV in einer Umgebung im Auftrag der Kostenträger MUSS den AdV-Server in einem Rechenzentrum im Auftrag der Krankenkassen betreiben.[<=]

Der Komponente „AdV-App“ stehen zwei verschiedene Ablaufumgebungen zur Verfügung.

Im nicht-öffentlichen zugänglichen Bereich (@home) wird die AdV-App auf einem Gerät des Versicherten betrieben. An diese Umgebung können keine Sicherheitsanforderungen gestellt werden. Der Schutz des eingesetzten Gerätes liegt in der Verantwortung des Versicherten. Durch geeignete Hinweise und Empfehlungen soll der Versicherte aufgeklärt werden, wie die AdV-App sicher genutzt werden kann und dass auch der Versicherte selbst hierzu beitragen kann. Im Rahmen dieser Informationen sollen insbesondere die Vorteile eines Kartenterminals mit Sicherheitsmerkmalen (bspw. Display, PIN-Pad) beschrieben und entsprechende Empfehlungen ausgesprochen werden.

#### **AdV-A\_2404 - AdV-App: Information zum sicheren Betrieb**

Der Anbieter einer KTR-AdV MUSS den Versicherten informieren, welche Maßnahmen zum sicheren Betrieb der AdV-App auf dem Gerät eines Versicherten beitragen.[<=]

Im öffentlichen zugänglichen Bereich wird die AdV-App in einem KTR-AdV-Terminal betrieben.

#### **AdV-A\_2405 - AdV-App: Betrieb in KTR-AdV-Terminal**

Der Betreiber einer KTR-AdV MUSS die AdV-App, falls sie innerhalb eines öffentlich zugänglichen Bereichs zur Verfügung gestellt wird, in einem KTR-AdV-Terminal betreiben.[<=]

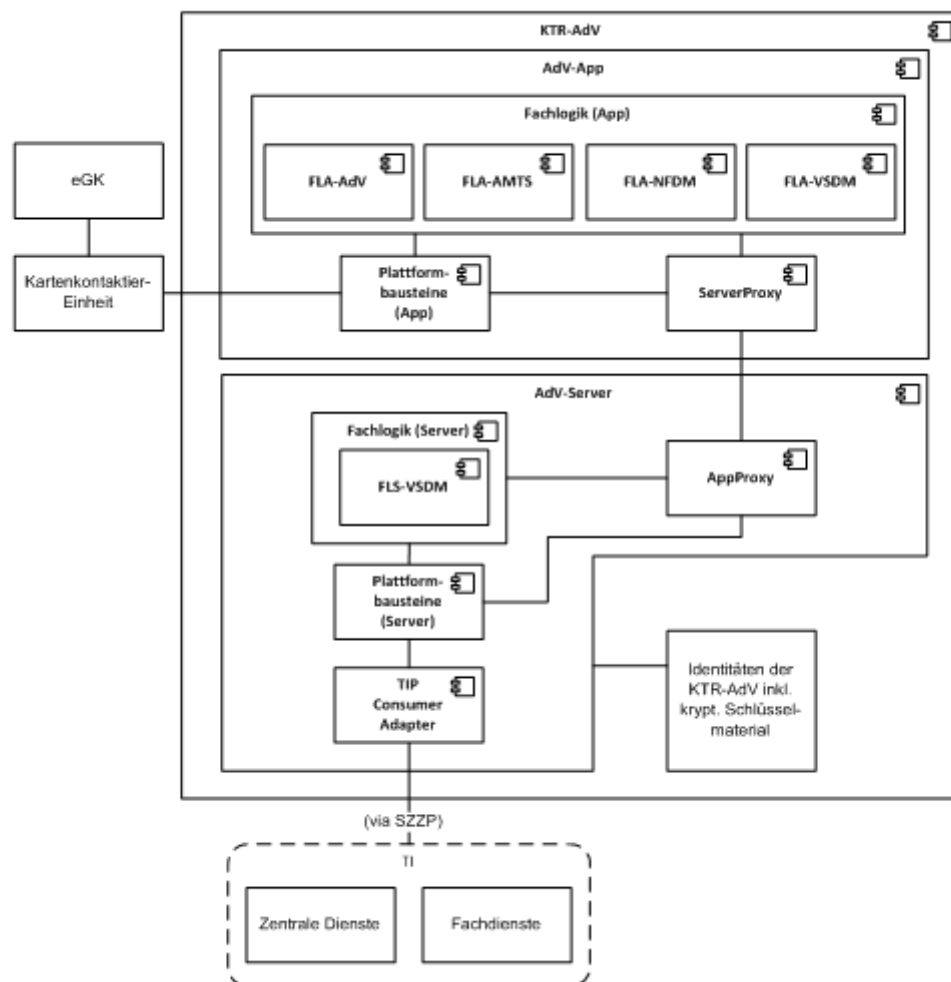
Das KTR-AdV-Terminal ist ein Produkttyp der TI. Anforderungen an den Produkttyp sind in [gemSpec\_KTR-AdV-Terminal] spezifiziert.



## 4 Zerlegung des Produkttyps

Der Produkttyp KTR-AdV besteht aus den Teilsystemen AdV-Server und AdV-App.

Im Folgenden wird die Zerlegung des Produkttyps KTR-AdV dargestellt, welche für die Übersicht der funktionalen Leistungsmerkmale in vorliegender Spezifikation nötig ist.



**Abbildung 5: ABB\_ADV\_329 – Komponentendiagramm der KTR-AdV**

In Tabelle TAB\_ADV\_329 werden die Komponenten, ihre Verantwortlichkeit und spezifische Funktionalitäten dargestellt.

**Tabelle 2: TAB ADV 329 – Komponenten, Verantwortung und Funktionalitäten**

Komponente	Verantwortung und Funktionalität	Spezifiziert in
------------	----------------------------------	-----------------

AdV-App	<p>Diese Komponente stellt die clientseitige Funktionalität zur Verfügung.</p> <ul style="list-style-type: none"> <li>Darstellung der Benutzeroberfläche für den Versicherten</li> </ul>	Kap. 6
Fachlogik (App)	<p>In dieser Komponente wird die gesamte Fachlogik in Form von fachanwendungsspezifischen Modulen gebündelt. Daten werden - soweit möglich - ausschließlich lokal verarbeitet.</p>	Kap. 6.1
FLA-AdV	<p>Dieses Modul setzt die Anwendungsfälle der Fachanwendung AdV um. Das Modul stellt generische Funktionalitäten bereit, welche durch die Fachanwendungen für ihre Anwendungsfälle genutzt werden können.</p>	Kap. 6.1.4
FLA-AMTS	<p>Dieses Modul setzt die Anwendungsfälle der Fachanwendung eMP/AMTS um. Aktuell können alle AMTS-Anwendungsfälle durch generische AdV-Operationen umgesetzt werden. Deshalb enthält dieser Modul derzeit keine fachanwendungsspezifischen Abläufe.</p>	Kap. 6.1.8
FLA-NFDM	<p>Dieses Modul setzt die Anwendungsfälle der Fachanwendungen NFDM um. Wenn sich die Anwendungsfälle aufgrund fachanwendungsspezifischer Abläufe nicht durch generische AdV-Operationen umsetzen lassen, dann werden Leistungen von fachanwendungsspezifischen Operationen genutzt. Diese sind in [gemSpec_FLA_NFDM] spezifiziert.</p>	Kap. 6.1.6 Kap. 6.1.7 [gemSpec_FLA_NFDM]
FLA-VSDM	<p>Dieses Modul setzt den Anwendungsfall der Fachanwendung VSDM um. Für den Ablauf wird eine fachanwendungsspezifische Operation genutzt, welche in [gemSpec_FM_VSDM] spezifiziert ist.</p>	6.1.5 [gemSpec_FM_VSDM]
Plattformbausteine (App)	<p>In dieser Komponente sind sämtliche Plattformbausteine, die in der App benötigt werden, enthalten. Diese Komponente wird von der Fachlogik angesteuert und stellt Funktionalitäten der TI-Plattform zur Verfügung:</p> <ul style="list-style-type: none"> <li>Zugriff auf die eGK</li> </ul>	Kap. 6.1.10
ServerProxy	<p>Diese Komponente stellt die Verbindung zum AdV-Server her.</p> <ul style="list-style-type: none"> <li>Sichere Verbindung mit dem AdV-Server</li> </ul> <p>Diese Verbindung ist eine Innenschnittstelle</p>	Kap. 5.1.2

	an die nur Sicherheitsanforderungen im Abschnitt 5.1.2 gestellt werden.	
AdV-Server	Diese Komponente stellt die Funktionalitäten zur Verfügung, die eine AdV-App benötigt, um mit den Diensten der zentralen TI und Fachdiensten in der TI zu kommunizieren.	Kap. 6
Fachlogik (Server)	In dieser Komponente wird die gesamte Fachlogik in Form von fachanwendungsspezifischen Modulen gebündelt, die im AdV-Server benötigt wird.	Kap. 6.1
FLS-VSDM	<p>Dieses Modul setzt die Fachlogik um, die zwischen dem Modul FLA-VSDM in der AdV-App und den Fachdiensten VSDM in der TI benötigt wird:</p> <ul style="list-style-type: none"> <li>Aufbau der Verbindung zum Intermediär VSDM</li> </ul> <p>Festlegungen zum Verbindungsaufbau und die entsprechenden Schnittstelle der Fachdienste sind in [gemSpec_SST_VSDM] und [gemSpec_SST_FD_VSDM] spezifiziert.</p>	Kap. 6.1.5 [gemSpec_SST_VSDM] [gemSpec_SST_FD_VSDM]
Plattformbausteine (Server)	<p>In dieser Komponente sind sämtliche Plattformbausteine, die der AdV-Server benötigt, enthalten. Diese Komponente wird von der Fachlogik angesteuert und stellt Funktionalitäten der TI-Plattform zur Verfügung:</p> <ul style="list-style-type: none"> <li>Einbeziehung der Identitäten der Kostenträger mit kryptografischen Operation auf deren geheimen Schlüsselmaterial in die AdV-Anwendungsfälle</li> <li>Prüfung von Zertifikaten</li> <li>Zugriff auf zentrale Dienste / Fachdienste über den Consumer Adapter</li> </ul>	Kap. 6.1.10
Consumer Adapter	<p>Diese Komponente wird durch die TI-Plattform spezifiziert. Der Consumer Adapter stellt Leistung der TI-Plattform innerhalb des Produkttyps KTR-AdV bereit. Die Anforderungen an diese Komponente finden sich in übergreifenden Spezifikationen und sind im Produkttypsteckbrief zur KTR-AdV aufgeführt. Folgende Funktionalitäten erfüllt diese Komponente:</p> <ul style="list-style-type: none"> <li>Anbindung zu den relevanten</li> </ul>	Kap. 6.2.4

	<p>zentralen Diensten der TI</p> <ul style="list-style-type: none"> <li>• Anbindung zu den relevanten Fachdiensten der TI</li> <li>• Prüfung von Zertifikaten der TI</li> <li>• Verwaltung des lokalen Truststores</li> </ul> <p>Diese Leistungen können durch Plattformbausteine oder Module mit Fachlogik genutzt werden.</p>	
AppProxy	<p>Diese Komponente stellt die Verbindung zur AdV-App her.</p> <ul style="list-style-type: none"> <li>• Sichere Verbindung mit der AdV-App</li> </ul> <p>Diese Verbindung ist eine Innenschnittstelle an die nur Sicherheitsanforderungen im Abschnitt 5.1.2 gestellt werden.</p>	Kap. 5.1.2

---

## 5 Übergreifende Festlegungen

---

### 5.1 Datenschutz und Sicherheit

In diesem Kapitel werden übergreifende Anforderungen beschrieben, die sich aus den Themenfeldern Datenschutz und Sicherheit ergeben.

#### 5.1.1 Verarbeitung personenbezogener Daten

Um den Datenschutz des Versicherten zu gewährleisten, werden folgende Anforderungen gestellt:

**AdV-A\_2407 - Keine persistente Speicherung von Daten des Versicherten**

Die KTR-AdV DARF personenbezogene Daten von Versicherten, mit Ausnahme der ICCSN der betroffenen eGK bei eGK-bezogenen Fehlern, NICHT persistent speichern.[<=]

**AdV-A\_2409 - Löschen der Daten nach Abmeldung**

Die KTR-AdV MUSS alle Daten des Versicherten, mit Ausnahme der ICCSN der betroffenen eGK bei eGK-bezogenen Fehlern, aus seinem Speicher löschen, sobald die AdV-Sitzung des Versicherten beendet wird.[<=]

**AdV-A\_2410 - Abmeldung des Nutzers nach 5 Minuten Inaktivität**

Die AdV-App MUSS den Versicherten nach spätestens fünf Minuten Inaktivität von der AdV-App automatisch abmelden und die Sitzung beenden. Eine Aktivität binnen der maximalen Inaktivitätsdauer MUSS die Ablaufzeit für die Inaktivitätsdauer erneut starten.[<=]

**AdV-A\_2568 - Warnung des Nutzers vor Abmeldung nach Inaktivität**

Die AdV-App KANN dem Versicherten vor der Abmeldung wegen Inaktivität einen Hinweis einblenden, der es dem Nutzer ermöglicht die Sitzung fortzuführen.[<=]

Es kann vor der Abmeldung des Versicherten ein Hinweis eingeblendet werden, der es dem Nutzer ermöglicht die Session fortzuführen.

**AdV-A\_2534 - Ausführung von Anwendungsfällen mit lokalen Mitteln**

Die AdV-App DARF NICHT Daten des Versicherten an den AdV-Server übertragen, wenn sich der Anwendungsfall auch mit lokalen Mitteln ausführen lässt. Dies betrifft alle medizinischen Daten nach § 291a Abs.2 und Abs.3 SGB V, eGK-Protokolldaten, die Information über genutzte Fachanwendungen, den DPE, die VSD (ausgenommen die KVNR), die PIN und Zertifikate der eGK außer C.CH.AUTN und C.eGK.AUT\_CVC. [<=]

Hiermit soll erreicht werden, dass die AdV-App nur dann mit dem AdV-Server kommuniziert, wenn dies für den Anwendungsfall unbedingt notwendig ist. Beispiele hierfür sind die Gültigkeitsprüfung beim Sitzungsstart oder die Kommunikation zu den Fachdiensten VSDM für die Onlineprüfung und -aktualisierung der Versichertenstammdaten. Die Änderung einer PIN oder das Anzeigen von Protokolldaten der eGK hingegen lässt sich mit lokalen Mitteln durchführen und darf nicht über den AdV-Server umgesetzt werden.

Die AdV-App kann unter Wahrung der gesetzlichen Rahmenbedingungen die KVNR an den AdV-Server übertragen.

### **AdV-A\_2411 - Keine Protokollierung medizinischer Daten**

Die KTR-AdV DARF NICHT medizinische Daten protokollieren.[<=]

### **AdV-A\_2412 - Keine Protokollierung personenbezogener Daten**

Die KTR-AdV DARF NICHT personenbezogene Daten von Versicherten, mit Ausnahme der ICCSN der betroffenen eGK bei kartenbezogenen Fehlern, protokollieren.[<=]

## **5.1.2 Absicherung der AdV-Komponenten**

Um die verarbeiteten Daten zu schützen, werden folgende Anforderungen zur Absicherung der AdV-Komponenten erhoben:

### **AdV-A\_2413 - AdV-Server: Keine unberechtigten Zugriffe**

Der AdV-Server MUSS unberechtigte Zugriffe auf die dort gespeicherten und verarbeiteten Daten und das zentrale Netz der TI verhindern.[<=]

Hierzu zählen bspw. der Zugriff über externe Schnittstellen zum Internet oder der TI, das Ausnutzen von Schwachstellen der installierten Software bzw. des Betriebssystems / der Firmware oder das Einbringen von Schadsoftware. Je nach Ausgestaltung und Funktionsumfang können geeignete Maßnahmen bspw. sein:

- Härtung des Betriebssystems (nur notwendige Software / Dienste)
- Schließen nicht verwendeter Ports
- Einsatz einer Statefull Packetinspection / Firewall
- Einsatz von Intrusion Detection/Prevention Systemen
- Validierung von eingehenden Anfragen
- Einsatz einer Antiviren-Software inklusive regelmäßiger Aktualisierung dieser Software
- ggf. logische Trennung von anderen Anwendungen (Virtualisierung).

### **AdV-A\_2546 - AdV-App: Sichere Verteilung**

Der Anbieter der KTR-AdV MUSS die AdV-App so an die Nutzer verteilen und diese darüber informieren, dass sie in der Lage sind, die Quelle und damit auch die Integrität und Authentizität der AdV-App zu prüfen.[<=]

Mit dieser Anforderung soll erreicht werden, dass die AdV-App über den offiziellen Weg des Herstellers bzw. die technologischen Standardmechanismen einer Plattform verteilt wird. Bspw. sollte der Play-Store für die Verteilung einer Android-Variante der AdV-App verwendet werden und für PC-Installationen sollte die Anwendung von der offiziellen Website des Anbieters herunterladbar sein. Nutzer müssen ausreichend informiert werden. Zum Beispiel könnte auf der Website des Anbieters der Name und der Hersteller der AdV-App genannt werden, damit diese im jeweiligen App-Store leicht zu identifizieren ist. Ziel ist es, dem Nutzer der AdV-App Sicherheit zu geben, dass er die richtige AdV-App nutzt.

### **AdV-A\_2414 - AdV-App: Bereitstellen von Softwareaktualisierungen**

Der Anbieter der AdV-App MUSS zeitnah Softwareaktualisierungen zur Beseitigung von Schwachstellen der AdV-App bereitstellen.

[<=]

Die Reaktionszeiten auf Schwachstellen sind vom Hersteller für die einzelnen Softwarekomponenten anzugeben und werden im Rahmen der Sicherheitsprüfung bewertet.

### **AdV-A\_2415 - AdV-App: Vertrauliche PIN-Eingabe erlauben**

Die AdV-App MUSS die vertrauliche PIN-Eingabe des Versicherten erlauben.[<=]

Für die Umsetzung sind bspw. folgende Maßnahmen sinnvoll:

- Die AdV-App implementiert ein virtuelles PIN-Pad um eine externe Softwaretastatur zu umgehen, falls das Kartenterminal kein PIN-Pad besitzt.
- Die PIN wird nicht im Klartext angezeigt.

Die Verbindung zwischen AdV-Server und AdV-App wird mittels TLS gemäß den Vorgaben aus [gemSpec\_Krypt] abgesichert.

#### **AdV-A\_2416 - TLS-Verbindung zwischen AdV-Server und AdV-App**

Die AdV-App MUSS mit dem AdV-Server ausschliesslich über TLS kommunizieren. [≤]

Die AdV-App muss dabei in der Lage sein, auch ohne Verwaltung einer aktuellen TSL einen AdV-Server zu authentisieren. Daher benötigt sie einen Truststore, in dem sich bereits vor dem Verbindungsaufbau die TLS-Zertifikate der AdV-Server befinden, mit denen sie sich verbinden kann. Die TLS-Zertifikate müssen den Vorgaben von [gemSpec\_Krypt] entsprechen.

#### **AdV-A\_2417 - AdV-App: lokaler Truststore**

Die AdV-App MUSS Zugriff auf einen lokalen integer geschützten Truststore besitzen, der die TLS-Zertifikate der AdV-Server enthält, mit denen die AdV-App sich verbinden kann. [≤]

#### **AdV-A\_2572 - AdV-App: interner Truststore**

Die AdV-App SOLL den lokalen Truststore enthalten. [≤]

Ein möglicher Grund, die Anforderung AdV-A\_2572 nicht umzusetzen, ist die Verwendung einer Plattform für die Ausführung der AdV-App, die einen eigenen Truststore anbietet und dessen Verwendung verlangt.

#### **AdV-A\_2573 - AdV-App: Initialisierung und Aktualisierung des TLS-Vertrauensankers**

Der Anbieter der KTR-AdV MUSS für die AdV-App ein Verfahren zur initialen Auslieferung sowie Aktualisierung des Vertrauensankers für die AdV-Server-TLS-Zertifikate implementieren, das die Integrität und Authentizität des Vertrauensankers wahrt. [≤]

Damit die AdV-App stets aktuelle Zertifikate der AdV-Server erhält, ist ein Verfahren notwendig, den lokalen Truststore der AdV-App initial zu befüllen und zu aktualisieren. Dies kann zum Beispiel durch neue Versionen der AdV-App – welche einen aktualisierten Truststore enthalten – realisiert werden. Es sind aber auch andere Verfahren denkbar.

#### **AdV-A\_2421 - AdV-Server: Schnittstelle Internet - Ablehnung unzulässiger Verbindungen**

Der AdV-Server MUSS Verbindungen an der Schnittstelle zum Internet ablehnen, wenn keine TLS-Verbindung aufgebaut werden kann oder die nachgelagerte Authentifizierung gemäß ABB\_ADV\_333 fehlschlägt. [≤]

### **5.1.3 Verbindungsaufbau und Freischaltung eGK**

In diesem Kapitel ist der Verbindungsaufbau von der AdV-App zum AdV-Server und die anschließende Freischaltung der eGK durch ein Card-to-Card (C2C) beschrieben, welche im Rahmen des Anwendungsfalls „Starten einer Sitzung“ durchgeführt werden.



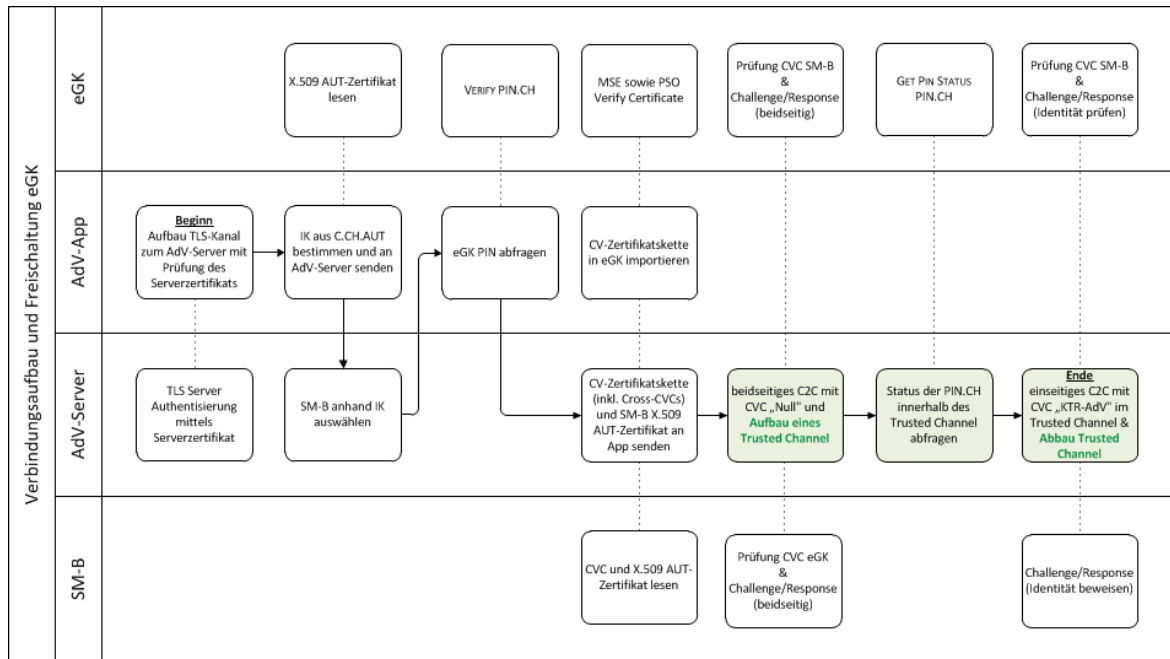


Abbildung 6 : ABB\_ADV\_333 Verbindungsaufbau und Freischaltung eGK

**A\_15110 - Adv-App: TLS-Verbindung zum Adv-Server initiieren**

Die Adv-App MUSS während des Sitzungsstarts eine TLS-Verbindung zum Adv-Server aufbauen.[<=]

**Adv-A\_2418 - Adv-App: unzulässige TLS-Verbindungen ablehnen**

Die Adv-App MUSS bei jedem Verbindungsaufbau den Adv-Server anhand seines TLS-Zertifikats mittels des lokalen Truststores authentifizieren und MUSS die Verbindungen ablehnen, falls die Authentifizierung fehlschlägt.[<=]

**A\_15111 - Adv-App: Institutskennzeichen an Adv-Server senden**

Die Adv-App MUSS für die Freischaltung der eGK die IK-Nummer aus dem C.CH.AUT Zertifikat der eGK an den Adv-Server senden.[<=]

Das Institutskennzeichen entspricht der 9-stelligen Nummer aus dem Organizational Unit Name im Subject Distinguished Name des C.CH.AUT-Zertifikates des Versicherten.

**A\_15112 - Adv-Server, Adv-App: Beidseitiges Card-to-Card mit Flagliste Null**

Der Adv-Server und Adv-App MÜSSEN ein beidseitiges Card-to-Card durchführen, wobei der Adv-Server ein CV Zertifikat mit Zugriffsprofil CHA.0 verwendet, und einen Trusted Channel etablieren.[<=]

Ein CVC Zertifikat mit dem Zugriffsprofil CHA.0 besitzt keine Rechte zum Freischalten der eGK.

**Adv-A\_2570 - SM-B des Herausgebers der eGK verwenden**

Der Adv-Server MUSS für das Card-to-Card eine SM-B des Herausgebers der eGK verwenden und die Verbindung abbrechen, wenn diese SM-B nicht verfügbar ist.[<=]

Die Zuordnung zwischen der eGK und der SM-B des Herausgebers kann anhand der von der Adv-App übermittelten IK-Nummer erfolgen.

**A\_15113 - Adv-App: Flaglist prüfen**

Die Adv-App MUSS während des beidseitigen Card-to-Card prüfen, dass das zu importierende CV-EE-Zertifikat das Zugriffsprofil CHA.0 besitzt.[<=]



**A\_15114 - AdV-Server: Prüfung Status PIN.CH der eGK**

Der AdV-Server MUSS in dem Trusted Channel den Status der PIN.CH der eGK abfragen und die Verbindung abbrechen, wenn der Sicherheitszustand des Passwortobjektes nicht gesetzt ist.[<=]

Die erwartete Antwort der eGK auf das Kartenkommando Get PIN Status ist NoError (,90 00').

**A\_15115 - AdV-Server, AdV-App: Einseitiges Card-to-Card mit CVC „KTR-AdV“**

Der AdV-Server und die AdV-App MÜSSEN nach erfolgreicher Prüfung des Status der PIN.CH der eGK ein einseitiges Card-to-Card durchführen, wobei der AdV-Server ein CV Zertifikat mit Zugriffsprofil CHA.1 verwendet.[<=]

Dieses einseitige Card-to-Card schaltet die eGK frei. Der für die Statusabfrage aufgebaute Trusted Channel kann abgebaut werden.

**A\_15116 - AdV-App: Abbruch bei Fehler im Verbindungsaufbau und Freischaltung eGK**

Die AdV-App MUSS bei Fehlern in den Operationen zum Verbindungsaufbau und der Freischaltung der eGK während des Sitzungsstarts die Sitzung beenden.[<=]

Für Erläuterungen zum Card-2-Card und der Prüfung des Status einer PIN siehe auch [gemSpec\_CardProxy].

**5.1.4 Filterung von Kartenkommandos an die eGK**

Während der Freischaltung der eGK durch ein Card-to-Card und der Onlineaktualisierung der VSD findet eine direkte Kommunikation zwischen der eGK und dem AdV-Server bzw. den Fachdiensten VSDM über den AdV-Server statt. Damit eine freigeschaltete eGK nicht durch einen manipulierten AdV-Server ausgelesen werden kann, muss die AdV-App alle Kartenkommandos, welche über den AdV-Server an die eGK gesendet werden, prüfen.

**A\_15117 - AdV-App: Ablehnen von Kartenkommandos**

Die AdV-App MUSS alle vom AdV-Server gesendeten Kartenkommandos ablehnen, welche nicht gemäß [TR AdV-App#Anhang C] zulässig sind, und die AdV-Sitzung beenden.[<=]

**5.2 Logging**

Der AdV-Server und die AdV-App auf dem KTR-AdV-Terminal sollen Protokolldateien schreiben, die eine Analyse technischer Vorgänge erlauben. Diese Protokolldateien sind dafür vorgesehen, aufgetretene Fehler zu identifizieren, die Performance zu analysieren und interne Abläufe zu beobachten. Bei der Erstellung von Einträgen in ein Protokoll bzw. Log sind die Anforderungen aus Kapitel 5.1.1 Verarbeitung personenbezogener Daten umzusetzen.

Ein Logging der AdV-App auf Geräten des Versicherten ist nicht vorgesehen.

**AdV-A\_2437 - AdV-App: Kein Logging auf Geräten des Versicherten**

Die AdV-App MUSS als Standardkonfiguration das Logging deaktiviert haben und auf dem KTR-AdV-Terminal die Aktivierung dieser Option durch einen berechtigten Nutzer ermöglichen.[<=]

Es gelten die übergreifenden Anforderungen zum Logging aus [gemSpec\_OM].

**AdV-A\_2422 - AdV-Server: Erzeugung von FehlerLog-Einträgen**

Der AdV-Server MUSS bei lokal erkannten Fehlern und Remote-Fehlern ein Fehlerprotokoll schreiben, welches dem berechtigten Nutzer für Administrations- und Betriebsaufgaben Rückschlüsse auf die aufgetretenen Fehler ermöglicht.[<=]

**AdV-A\_2423 - AdV-App: Erzeugen von FehlerLog-Einträgen**

Die AdV-App MUSS, wenn sie auf einem KTR-AdV-Terminal betrieben wird, bei lokal erkannten Fehlern und Remote-Fehlern ein Fehlerprotokoll schreiben, welches dem berechtigten Nutzer für Administrations- und Betriebsaufgaben Rückschlüsse auf die aufgetretenen Fehler ermöglicht.[<=]

**AdV-A\_2424 - Speichern der ICCSN zur Fehleranalyse**

Die KTR-AdV MUSS die ICCSN der eGK im Protokoll speichern, wenn ein eGK-bezogener Fehler aufgetreten ist.[<=]

**AdV-A\_2426 - Löschen der ICCSN aus Fehlerprotokoll**

Die KTR-AdV MUSS jede ICCSN nach maximal 180 Tagen aus dem Fehlerprotokoll löschen.[<=]

**AdV-A\_2428 - AdV-Server: Ablaufprotokoll**

Der AdV-Server MUSS ein Ablaufprotokoll schreiben, das geeignet ist, die ausgeführten Abläufe nachzuvollziehen. Das Ablaufprotokoll erfasst für jeden ausgeführten Vorgang: Vorgangsbezeichner, Datum mit Uhrzeit von Beginn und Ende, vollständiger Name des Vorgangs, Beschreibung des Vorgangs inkl. des Ergebnisses: Erfolg oder Fehlermeldung (Returnwert/Fehlercode).[<=]

**AdV-A\_2429 - AdV-App: Ablaufprotokoll**

Die AdV-App MUSS, wenn sie auf einem KTR-AdV-Terminal betrieben wird, ein Ablaufprotokoll schreiben, das geeignet ist, die ausgeführten Abläufe nachzuvollziehen. Das Ablaufprotokoll erfasst für jeden ausgeführten Vorgang: Vorgangsbezeichner, Datum mit Uhrzeit von Beginn und Ende, vollständiger Name des Vorgangs, Beschreibung des Vorgangs inkl. des Ergebnisses: Erfolg oder Fehlermeldung (Returnwert/Fehlercode).[<=]

**AdV-A\_2430 - AdV-Server: PerformanceLog**

Der AdV-Server SOLL ein Performanceprotokoll schreiben, welches geeignet ist, die Ausführungszeit von Operationen auf dem AdV-Server zu überprüfen.[<=]

**AdV-A\_2431 - AdV-App: PerformanceLog**

Die AdV-App SOLL, wenn sie auf einem KTR-AdV-Terminal betrieben wird, ein Performanceprotokoll schreiben, welches geeignet ist, die Ausführungszeit der Operationen der AdV-App zu überprüfen.[<=]

**AdV-A\_2432 - AdV-Server: DebugLog**

Der AdV-Server KANN im Testbetrieb unter Verwendung des Severity Codes "Debug" ein DebugLog schreiben, welches eine erweiterte Protokollierung für Testzwecke ermöglicht.[<=]

**AdV-A\_2433 - AdV-App: DebugLog**

Die AdV-App KANN, wenn sie auf einem KTR-AdV-Terminal betrieben wird, im Testbetrieb unter Verwendung des Severity Codes "Debug" ein DebugLog schreiben, welches eine erweiterte Protokollierung für Testzwecke ermöglicht.[<=]

**AdV-A\_2434 - AdV-Server: SecurityLog**

Der AdV-Server KANN ein SecurityLog zur Protokollierung sicherheitsrelevanter Ereignisse implementieren.[<=]

**AdV-A\_2435 - AdV-App: SecurityLog**

Die AdV-App KANN, wenn sie auf einem KTR-AdV-Terminal betrieben wird, ein SecurityLog zur Protokollierung sicherheitsrelevanter Ereignisse implementieren.[<=]

#### **AdV-A\_2436 - Verfügbarkeit interner Logdaten**

Der Betreiber der KTR-AdV MUSS im Rahmen von Testmaßnahmen dem Testbetriebsverantwortlichen auf Anforderung die Log-Dateien übermitteln.[<=]

Die Rolle des Testbetriebsverantwortlichen ist im Testkonzept [gemKPT\_Test] beschrieben.

#### **AdV-A\_2438 - AdV-Server: Erweiterte Loglevel zur Bezeichnung der Granularität des FehlerLog**

Der AdV-Server SOLL die Fehleranalyse durch eine mit Logleveln konfigurierbare Speicherung der aufgetretenen Fehlerfälle unterstützen.[<=]

#### **AdV-A\_2439 - AdV-App: Erweiterte Loglevel zur Bezeichnung der Granularität des FehlerLog**

Die AdV-App SOLL, wenn sie auf einem KTR-AdV-Terminal betrieben wird, die Fehleranalyse durch eine mit Logleveln konfigurierbare Speicherung der aufgetretenen Fehlerfälle unterstützen.[<=]

#### **AdV-A\_2440 - AdV-Server: Art der Protokollierung**

Der AdV-Server MUSS Protokolleinträge so anlegen, dass eine Analyse der Einträge unterstützt wird:

- Protokolleinträge zum selben Vorgang (der ausgelöst werden kann z.B. durch eine Außenoperation, eine Administrations- oder Betriebsinteraktion, ein Ereignis, ...) MÜSSEN entlang der Aufrufkette über Protokollgrenzen hinweg dem Vorgang zugeordnet werden können (gleiche Vorgangsbezeichner).
- Die Protokolleinträge MÜSSEN eine patternbasierte Filterung unterstützen. Protokollwert/-texte sowie Attribute MÜSSEN in ihren Namensstrukturen hierauf abgestimmt sein.

[<=]

#### **AdV-A\_2441 - AdV-App: Art der Protokollierung**

Die AdV-App MUSS, wenn sie auf einem KTR-AdV-Terminal betrieben wird, Protokolleinträge so anlegen, dass eine Analyse der Einträge unterstützt wird:

- Protokolleinträge zum selben Vorgang (der ausgelöst werden kann z.B. durch eine Außenoperation, eine Administrations- oder Betriebsinteraktion, ein Ereignis, ...) MÜSSEN entlang der Aufrufkette über Protokollgrenzen hinweg dem Vorgang zugeordnet werden können (gleiche Vorgangsbezeichner).
- Die Protokolleinträge MÜSSEN eine patternbasierte Filterung unterstützen. Protokollwert/-texte sowie Attribute MÜSSEN in ihren Namensstrukturen hierauf abgestimmt sein.

[<=]

#### **AdV-A\_2442 - AdV-Server: Zugriff auf Protokolldateien**

Der AdV-Server MUSS den Zugriff auf Protokolldateien auf berechtigte Nutzer für Administrations- und Betriebsaufgaben beschränken.[<=]

#### **AdV-A\_2443 - AdV-App: Zugriff auf Protokolldateien**

Die AdV-App MUSS, wenn sie auf einem KTR-AdV-Terminal betrieben wird, den Zugriff auf Protokolldateien auf berechtigte Nutzer für Administrations- und Betriebsaufgaben beschränken.[<=]

### 5.3 Nicht-funktionale Anforderungen

Die KTR-AdV ist ein dezentraler Produkttyp der TI, welcher nicht direkt in den Versorgungsprozess beim Leistungserbringer eingebunden ist. Die Beauftragung zur Umsetzung erfolgt durch die Kostenträger. Diese haben durch eine Integration der AdV-Lösung in ihre Onlinestrategie eine Möglichkeit, Mehrwert für ihre Versicherten zu schaffen. Aus diesem Grund werden Anforderungen zur Verfügbarkeit und Performance der KTR-AdV nicht durch die gematik, sondern durch den beauftragenden Kostenträger gestellt.

## 6 Funktionsmerkmale

### 6.1 Implementation der AdV Anwendungsfälle

Die folgenden Anwendungsfälle beschreiben das Außenverhalten des Systems anhand der Implementierung von AdV-Anwendungsfällen. Diese sind für den Versicherten zur Verwaltung seiner elektronischen Gesundheitskarte ausgelegt. Jeder Anwendungsfall wird durch den Versicherten eigenständig initiiert.

Dieses Kapitel beschreibt die übergreifenden Funktionalitäten der AdV Anwendungsfälle. Zur Realisierung dieser Funktionalitäten werden

- Leistungen der TI-Plattform (Plattformleistungen „PL\_TUC\_“\*) aus Anhang B und
- spezifische Fachlogik aus den entsprechenden (Fach-)Modulen NFDM [gemSpec\_FLA\_NFDM] und VSDM [gemSpec\_FM\_VSDM]

eingesetzt.

Falls während der Ausführung eines Plattformbausteins ein Fehler auftritt, liefert dieser einen Fehlercode zurück. Falls diese Fehler im lokalen Kontext des Anwendungsfalls lösbar sind, wird diese Behandlung des Fehlers dort beschrieben. Alle weiteren Fehler werden wie folgt behandelt:

#### **AdV-A\_2444 - AdV-App Fehlerverarbeitung**

Die AdV-App MUSS

- In allen Fehlerfällen dem Versicherten eine Fehlermeldung anzeigen und verständliche Hinweise zur Lösung des Problems geben.
- Die in TAB\_ADV\_318 aufgeführten Fehlercodes der Plattformbausteine gemäß dieser Tabelle verarbeiten, falls im Anwendungsfall keine abweichende Behandlung definiert ist.

**Tabelle 3: TAB\_ADV\_318 – Behandlung von Fehlercodes der Plattformbausteine**

Fehlercode	Fehlertext	Spezifische Aktionen durch AdV-App
CardTerminated	Ihre Gesundheitskarte ist gesperrt, bitte wenden Sie sich an Ihre Krankenkasse.	
CorruptDataWarning	Fehler beim Lesen von der eGK. Daten möglicherweise verfälscht.	
DataTooBig	Technischer Fehler. Fehler beim Schreiben auf die eGK. Die Daten sind zu groß.	

ErrorAuthentication	Technischer Fehler. Kartenfreischaltung fehlgeschlagen.	
ErrorImportCVC	Technischer Fehler. Kartenfreischaltung fehlgeschlagen.	
ErrorUserVerification	Technischer Fehler. Kartenfreischaltung fehlgeschlagen.	
FileNotFound	Technischer Fehler. Die Daten wurden auf der eGK nicht gefunden.	
MemoryFailure	Ihre Gesundheitskarte ist beschädigt, bitte wenden Sie sich an Ihre Krankenkasse.	
NotEnoughMemorySpace	Technischer Fehler. Fehler beim Schreiben auf die eGK. Die Daten sind zu groß.	
ObjectNotFound	Technischer Fehler. Die Daten wurden auf der eGK nicht gefunden.	
ObjectTerminated	Technischer Fehler. Das Objekt auf der eGK ist nicht mehr verwendbar.	
OffsetTooBig	Technischer Fehler. Die Daten auf der eGK werden nicht korrekt adressiert.	
PasswordBlocked	Das Passwort wurde – nach zu häufiger falscher PIN/PUK Eingabe – blockiert.	Eine Fehlermeldung anzeigen und dem Versicherten empfehlen, entweder die PIN mit Hilfe der PUK zu entsperren bzw. bei einer gesperrten PUK sich an seine Krankenkasse zu wenden.
PasswordDisabled	Das Passwort ist abgeschaltet.	

SecurityStatusNotSatisfied	Technischer Fehler. Es fehlen Zugriffsrechte für die Ausführung des Anwendungsfalls.	
UpdateRetryWarning	Die Operation war erfolgreich, musste jedoch mehrmals für die eGK wiederholt werden. Wegen dieses Speicherfehlers ist es angebracht, die Smart Card baldmöglichst zu ersetzen.	Eine Warnung anzeigen.
WrongSecretWarning	Falsche PIN, verbleibende Eingabeversuche <x>	Eine Fehlermeldung mit der verbleibenden Anzahl der Eingabeversuche bis zur Sperrung der PIN anzeigen.
WrongEndEntityCVC	Technischer Fehler. Kartenfreischaltung fehlgeschlagen.	

[&lt;=]

### 6.1.1 AdV-Sitzung des Versicherten

Nach der erfolgreichen Initialisierung der AdV-Sitzung kann der Versicherte Anwendungsfälle zur Verwaltung seiner Gesundheitskarte ausführen, bspw. PINs auf seiner Karte verwalten und Anwendungsfälle weiterer Fachanwendungen ausführen.

#### 6.1.1.1 AdV-Sitzung initialisieren

Mit diesem Anwendungsfall wird die AdV-Sitzung des Versicherten gestartet, der Start des Anwendungsfalls erfolgt implizit durch Stecken der eGK und Starten der AdV-App durch den Versicherten.

Hinweis: Unter "Stecken der eGK" kann auch der Aufbau einer Verbindung zur eGK über die kontaktlose Schnittstelle der eGK verstanden werden.

#### AdV-A\_2445 - AdV-App: Starten einer Sitzung

Die AdV-App MUSS den Anwendungsfall „Starten einer Sitzung“ gemäß TAB\_ADV\_303 umsetzen.

**Tabelle 4: TAB\_ADV\_303 – Starten einer AdV-Sitzung**

Name	Starten einer AdV-Sitzung
------	---------------------------

Auslöser	Der Versicherte startet die AdV-App und steckt seine eGK in ein Kartenterminal.
Akteure	Versicherter
Vorbedingung	Die AdV-App kann auf die eGK des Versicherten zugreifen und den AdV-Server erreichen. Eine SM-B des Herausgebers der eGK ist vorhanden.
Nachbedingung	<ul style="list-style-type: none"> <li>Die AdV-App hat für die AdV-Sitzung eine TLS-Verbindung zum AdV-Server aufgebaut.</li> <li>Die Benutzerverifikation mit der PIN.CH wurde erfolgreich durchgeführt.</li> <li>Die eGK wurde durch ein Card-2-Card mit einer korrespondierenden SM-B freigeschaltet und auf Gültigkeit geprüft.</li> <li>Die eGK wurde auf Gültigkeit geprüft.</li> <li>Für die eGK werden durch Plattformbaustein PL_TUC_CARD_INFORMATION die dort spezifizierten Informationen bereitgestellt.</li> <li>Die Sitzung des Versicherten wurde gestartet.</li> <li>Der Gültigkeitsstatus der eGK wird angezeigt.</li> <li>Es werden die mit der eGK des Versicherten verfügbaren Fachanwendungen aufgelistet.</li> </ul> <p>In allen - nicht behebbaren – Fehlerfällen wird die AdV-Sitzung beendet (Kap. 6.1.1.2 AdV-Sitzung beenden).</p>
Aktivitäten	<p>Die Umsetzung ist in Tabelle TAB_ADV_304 beschrieben. Falls eine Aktivität für die eGK bereits durchgeführt wurde (z.B. eine PIN-Prüfung), muss sie nicht wiederholt werden.</p> <ul style="list-style-type: none"> <li>Einlesen der Karte</li> <li>Einverständnis des Versicherten einholen (Benutzerverifikation)</li> <li>Versicherten-PIN entsperren (optional)</li> <li>Verbindungsaufbau zum AdV-Server und Freischaltung eGK</li> <li>Protokollieren des eGK-Zugriffs (für eGK G2)</li> <li>Online-Gültigkeitsprüfung der eGK</li> <li>Verfügbare Anwendungen anzeigen</li> </ul>

Tabelle 5: TAB\_ADV\_304 – Ablaufaktivitäten - Starten einer AdV-Sitzung

<b>Einlesen der Karte</b>	
Plattformbaustein	PL_TUC_CARD_INFORMATION
Eingangsdaten	



eGK	Nach Stecken der eGK werden durch den Plattformbaustein PL_TUC_CARD_INFORMATION Statusinformationen bereitgestellt.
Beschreibung	<p>Die AdV-App MUSS nach Stecken der eGK und vor dem Ausführen eines anderen Anwendungsfalls die Karteninformationen in PL_TUC_CARD_INFORMATION auswerten hinsichtlich</p> <ul style="list-style-type: none"> <li>• Kartentyp, MUSS vom Typ eGK sein</li> <li>• Produkttypversion des Objektsystems, MUSS G2 oder höher sein</li> <li>• Echtheit der Karte, die Karte MUSS für echt befunden sein</li> </ul> <p>und bei unpassenden Kartendaten die Sitzung beenden.</p> <p>Falls entsprechend PL_TUC_CARD_INFORMATION der Status der PIN.CH "PIN gesperrt" ist, wird mit Aktivität "Versicherten-PIN entsperren" fortgefahren.</p>
<b>Einverständnis des Versicherten einholen (Benutzerverifikation)</b>	
Plattformbaustein	PL_TUC_CARD_VERIFY_PIN
<i>Eingangsdaten</i>	
Identifikator	PIN.CH
Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im AdV-App-Benutzerinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT	„Eingabe Versicherten-PIN: “
<i>Rückgabedaten</i>	
<i>Rückgabe - Beschreibung</i>	<i>Aktion durch AdV-App</i>
OK - PIN erfolgreich verifiziert	Verarbeitung mit Aktivität "Verbindungsaufbau zum AdV-Server und Freischaltung eGK" fortsetzen.
WrongSecretWarning.X - PIN falsch, noch X Versuche	Wird durch den Versicherten ein falsches PIN-Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung des PINs zurückgemeldet. Der Versicherte hat die Wahl die PIN erneut einzugeben oder die Sitzung zu beenden.

PasswordBlocked - PIN ist durch Fehleingaben blockiert	Verarbeitung mit Aktivität "Versicherten-PIN entsperren" fortsetzen.
Weitere Fehlerfälle	Siehe Beschreibung PL_TUC_CARD_VERIFY_PIN und "TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine" für die Behandlung in der AdV-App. In all diesen Fehlerfällen muss nach Information des Versicherten die Sitzung beendet werden.
<i>Beschreibung</i>	Der Versicherte muss den Zugriff auf seine eGK mittels PIN-Verifikation autorisieren. Falls der Versicherte die PIN.CH der eGK bereits eingegeben hat, kann diese Aktivität entfallen.  Es ist möglich, dass die PIN blockiert ist, der Versicherte seine Versicherten-PIN falsch eingibt oder ein technischer Fehler auftritt. Der Start der AdV-Sitzung ist in diesen Fällen nicht erfolgreich. Im Folgenden sind keine weiteren Anwendungsfälle außer dem Beenden der Sitzung (6.1.1.2 AdV-Sitzung beenden) bzw. dem Entsperren der Versicherten-PIN zulässig.
<b>Versicherten-PIN entsperren (optional)</b>	
Anwendungsfall	Versicherten-PIN entsperren (Kap 6.1.5.4)
<i>Beschreibung</i>	Der Versicherte kann seine Versicherten-PIN (PIN.CH) in diesem Anwendungsfall entsperren. Nach erfolgreichem Entsperren der Versicherten-PIN ist die Aktivität "Einverständnis des Versicherten einholen" zu wiederholen.  Es ist möglich, dass die PIN nicht entsperret wurde oder ein technischer Fehler auftritt. Der Start der AdV-Sitzung ist in diesen Fällen nicht erfolgreich. Die Sitzung wird beendet (6.1.1.2 AdV-Sitzung beenden).
<b>Verbindungsaufbau zum AdV-Server und Freischaltung eGK</b>	
<i>Beschreibung</i>	Siehe Kap. 5.1.3 Verarbeitung mit Aktivität "Protokollieren des eGK-Zugriffs" fortsetzen.
<b>Protokollieren des eGK-Zugriffs (für eGK G2)</b>	
Plattformbaustein	PL_TUC_EGK_APPEND_PROTOCOL
<i>Eingangsdaten</i>	

DATATYPE	„V“ (Anwendungen des <b>V</b> ersicherten in der KTR-AdV Umgebung)
ACCESSTYPE	„Z“ (allgemeiner <b>Z</b> ugriff; Lesen und bearbeiten).
<i>Rückgabedaten</i>	
<i>Rückgabe - Beschreibung</i>	<i>Aktion durch AdV-App</i>
OK - Protokolleintrag erfolgreich hinzugefügt	Verarbeitung mit Aktivität "Online-Gültigkeitsprüfung der eGK" fortsetzen.
Fehlerfälle	Siehe Beschreibung PL_TUC_EGK_APPEND_PROTOCOL und "TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine" für die Behandlung in der AdV-App. In all diesen Fehlerfällen muss nach Information des Versicherten die Sitzung beendet werden (Kap. 6.1.1.2 AdV-Sitzung beenden).
<i>Beschreibung</i>	Nach erfolgreicher Freischaltung der eGK erfolgt die Protokollierung des Datenzugriffs für eine eGK der Version G2. Für eine eGK G2 wird genau ein Eintrag am Beginn einer AdV-Sitzung in das Zugriffsprotokoll EF.Logging der Karte geschrieben. Für alle höheren Versionen der eGK wird dieser Logeintrag nicht benötigt, da das Logging innerhalb der ausgeführten Anwendungsfälle erfolgt.  Der Aufbau der Eingangsdaten wird in PL_TUC_EGK_APPEND_PROTOCOL beschrieben.
<b>Online-Gültigkeitsprüfung der eGK</b>	
Plattformbaustein	PL_TUC_EGK_STATUS
<i>Rückgabedaten</i>	
<i>Rückgabe</i>	<i>Aktion durch AdV-App</i>
Status der Gesundheitsanwendung auf der eGK: Gesundheitsanwendung aktiv	Fortfahren und Aufbereitung der Menüstruktur
Status der Gesundheitsanwendung auf der eGK: Gesundheitsanwendung nicht-aktiv	Beschränkung der Anwendungsfälle entsprechend Tabelle TAB_ADV_384. Hinweis: In dem Fall wird der Anwendungsfall dem Versicherten mit der Bezeichnung „Entsperren der Gesundheitsanwendung prüfen“

	angezeigt.
Status der Gesundheitsanwendung auf der eGK: Gesundheitsanwendung Prüffehler	Eine verständliche Fehlermeldung anzeigen und die eGK Sitzung beenden (Kap. 6.1.1.2 AdV-Sitzung beenden).
Mathematische Prüfung des Karteninhabertzertifikats: Zertifikat mathematisch gültig	Fortfahren und Aufbereitung der Menüstruktur
Mathematische Prüfung des Karteninhabertzertifikats: Zertifikat mathematisch ungültig oder Prüffehler	Fortfahren und Aufbereitung der Menüstruktur und den Versicherten informieren.
Prüfung auf zeitliche Gültigkeit des Karteninhabertzertifikats: Zertifikat zeitlich gültig	Fortfahren und Aufbereitung der Menüstruktur
Prüfung auf zeitliche Gültigkeit des Karteninhabertzertifikats: Zertifikat zeitlich ungültig oder Prüffehler	Fortfahren und Aufbereitung der Menüstruktur und den Versicherten informieren.
<i>Beschreibung</i>	Plattformbaustein PL_TUC_EGK_STATUS führt die Gültigkeitsprüfung der eGK durch. Zum einen werden Prüfschritte direkt auf der Karte durchgeführt und andererseits die Legitimität der Karte mittels Onlineabfrage beim Trust Service Provider geprüft.
<b>Verfügbare Anwendungen anzeigen</b>	
<i>Beschreibung</i>	<p>Die AdV-App MUSS am Ende des Anwendungsfalls die Menüstruktur der verfügbaren Anwendungsfälle entsprechend dem Status der Fachanwendung und PIN ergänzen.</p> <ul style="list-style-type: none"> <li>Ist der Ordner DF.HCA gesperrt, sind nur Anwendungsfälle der PIN-Verwaltung für die PIN.CH (Kap. 6.1.5.3, 6.1.5.4) und das Lesen und Aktualisieren der VSD (Kap.6.1.5.1) möglich.</li> <li>Fachanwendungen im Status ABSENT bzw. TERMINATED sind auf der eGK nicht vorhanden bzw. nicht mehr zu verwenden, deren fachspezifische Anwendungsfälle sollten in der AdV-App nicht auswählbar sein.</li> <li>Fachanwendungen im Status AVAILABLE oder HIDDEN sind auf der eGK verfügbar, deren fachspezifische</li> </ul>

	<p>Anwendungsfälle sind je nach vorangegangener Operation logisch sinnvoll (Daten lesen, Anwendung verbergen nur im Zustand AVAILABLE, Anwendung sichtbar machen nur im Zustand HIDDEN) und sollten entsprechend angeboten bzw. temporär nicht auswählbar sein.</p> <ul style="list-style-type: none"> <li>• Wenn die Fachanwendung über eine PIN verfügt: PINs im Zustand DISABLED können über einen Anwendungsfall eingeschaltet werden, PINs im Zustand OK und VERIFIABLE können abhängig von den Zugriffsrechten im Objektsystem der eGK ausgeschaltet werden, PINs im Zustand BLOCKED müssen vor der Verwendung und den Zugriff auf die Fachanwendung entsperrt werden.</li> </ul> <p>Fachanwendungsunabhängige Anwendungsfälle dürfen durch den Status der Fachanwendungen nicht eingeschränkt werden und müssen immer verfügbar sein.</p>
<i>Hinweis zur Umsetzung</i>	<p>Je nach Generation der vom Versicherten gesteckten eGK sind verschiedene Fachanwendungscontainer auf der eGK vorhanden. Zusätzlich kann sich der Status der Fachanwendungscontainer vom Zustand „aktiv“ unterscheiden, wodurch die im Folgenden beschriebenen Anwendungsfälle erst zulässig werden oder nicht mehr zulässig sind.</p>

[&lt;=]

**AdV-A\_2446 - AdV-App: Warnung eGK nicht ziehen**

Die AdV-App MUSS den Nutzer warnen, wenn er seine eGK nicht aus dem Kartenterminal entfernen darf (z.B. während Schreibzugriffen/VSD Update) zur Vermeidung von inkonsistenten Zuständen auf der eGK.[<=]

**6.1.1.2 AdV-Sitzung beenden**

Mit der Umsetzung dieses Anwendungsfalls wird die Sitzung des Versicherten beendet. Der Versicherte kann keine fachlichen Anwendungsfälle bis zum Start einer neuen Sitzung aufrufen. In der AdV-App und dem AdV-Server liegen keine persistent oder temporär gespeicherten, personenbezogenen oder medizinischen Daten des Versicherten vor. Auf dem Display wird eine neutrale Anzeige dargestellt.

**AdV-A\_2447 - AdV-App: Menüpunkt zum Beenden einer Sitzung**

Die AdV-App MUSS dem Nutzer eine Menüoption anbieten, mit der er seine aktuelle Sitzung beenden kann.[<=]

**AdV-A\_2448 - AdV-App: Ziehen der eGK des Versicherten**

Die AdV-App MUSS bei dem Ziehen der eGK des Versicherten die Sitzung des Versicherten sofort beenden.[<=]

**AdV-A\_2449 - AdV-App: Beenden einer Sitzung in AdV-App**

Die AdV-App MUSS das Beenden der Sitzung des angemeldeten Versicherten derart umsetzen, dass ein ggfs. in der Ausführung befindlicher Anwendungsfall – welcher

inkonsistente Daten auf der eGK hinterlassen könnte – vor dem Ende der Sitzung abgeschlossen wird. Die AdV-App MUSS zum Beenden der Sitzung

- mit PL\_TUC\_CARD\_RESET ein Reset der gesteckten Karte anfordern,
- die TLS Verbindung zum AdV-Server beenden
- und den Versicherten zum Ziehen der eGK auffordern.

[<=]

#### **AdV-A\_2450 - AdV-App: Darstellung einer neutralen Anzeige**

Die AdV-App MUSS nach dem Beenden einer Sitzung auf dem Bildschirm eine neutrale Anzeige, insbesondere ohne Daten des Versicherten, darstellen.[<=]

### **6.1.2 Übergreifende Vorbedingungen**

Die ab Kapitel 6.1.5 beschriebenen fachlichen Anwendungsfälle werden durch den Versicherten eigenständig ausgeführt, die AdV-App ruft die dort benannten Operationen nur bei explizitem Wunsch des Versicherten auf. Folgende Vorbedingungen müssen beim Start jedes Anwendungsfalles erfüllt sein.

#### **AdV-A\_2451 - AdV-App: Übergreifende Vorbedingung**

Die AdV-App MUSS die Zulässigkeit aller Anwendungsfälle in Abhängigkeit von folgenden Kriterien sicherstellen:

**Tabelle 6: TAB\_ADV\_320 – Übergreifende Vorbedingungen**

Erfolgsbedingung
<ul style="list-style-type: none"> <li>• Der Anwendungsfall „Starten einer Sitzung“ wurde erfolgreich ausgeführt.</li> <li>• Die eGK des Versicherten wird für die Nutzung in den Anwendungsfällen für den Zeitraum der Sitzung eindeutig identifiziert.</li> </ul>

[<=]

#### **AdV-A\_2452 - AdV-App: Zulässigkeit der Anwendungsfälle**

Die AdV-App MUSS die Zulässigkeit des Anwendungsfalles in Abhängigkeit von folgenden Kriterien sicherstellen:

VerificationResult

- K1: Echtheit eGK: Authentic und X.509  
(Karteninhaberzertifikat) mathematisch gültig [ja / nein / Prüffehler]
- K2: Status des DF.HCA (Gesundheitsanwendung): [aktiv / nicht aktiv / Prüffehler]
- K3: X.509 (Karteninhaberzertifikat) Gültigkeit: Valid  
[TRUE (zeitlich gültig),  
FALSE (zeitlich ungültig bzw. Prüffehler)]
- K4: X.509 (Karteninhaberzertifikat) Status: CertificateResult  
[OK (Online gültig),  
REVOKED (Online gesperrt),

UNKOWN(Onlinestatus unbekannt|Prüffehler)]

#### Application

- K5: Status der Anwendungen auf der eGK je Anwendung [AVAILABLE, HIDDEN, ABSENT, TERMINATED]
- K6: Status der PINs der eGK je Anwendung  
 [OK (PasswordEnabledVerified),  
 BLOCKED (PasswordBlocked),  
 DISABLED (PasswordDisabled),  
 VERIFYABLE (PasswordEnabledNotVerified.X)]

**Tabelle 7: TAB\_ADV\_384 – Zulässige Anwendungsfälle nach Status von Karte, Anwendung und PIN**

	K1	K2	K3	K4	K5	K6
Beenden einer eGK Sitzung	immer	immer	immer	immer	immer	immer
VSD von eGK anzeigen	ja	aktiv nicht aktiv	TRUE	OK REVOKED UNKOWN	n/a	OK VERIFYABLE
Zugriffsprotokoll von eGK lesen	ja	aktiv	TRUE FALSE	OK REVOKED UNKOWN	n/a	OK VERIFYABLE
PIN ändern	ja	aktiv (für PIN.CH immer)	TRUE	OK UNKOWN	AVAILABLE HIDDEN	OK DISABLED VERIFYABLE
PIN auf eGK entsperren	ja	aktiv (für PIN.CH immer)	TRUE FALSE	OK REVOKED UNKOWN	AVAILABLE HIDDEN	BLOCKED
Datenübertragung bei Kartentausch	ja	aktiv	TRUE FALSE	OK REVOKED UNKOWN	AVAILABLE HIDDEN	OK DISABLED VERIFYABLE
PIN für Fachanwendung einschalten	ja	aktiv	TRUE	OK UNKOWN	AVAILABLE HIDDEN	DISABLED
PIN für Fachanwendung ausschalten	ja	aktiv	TRUE	OK UNKOWN	AVAILABE HIDDEN	OK VERIFYABLE

Daten von Fachanwendung anzeigen	ja	aktiv	TRUE FALSE	OK REVOKED UNKOWN	AVAILABLE	OK DISABLED VERIFYABLE
Daten von Fachanwendung ändern	ja	aktiv	TRUE	OK UNKOWN	AVAILABLE	OK DISABLED VERIFYABLE
Daten von Fachanwendung löschen	ja	aktiv	TRUE	OK UNKOWN	AVAILABLE	OK DISABLED VERIFYABLE
Fachanwendung verbergen	ja	aktiv	TRUE	OK UNKOWN	AVAILABLE	OK DISABLED VERIFYABLE
Fachanwendung sichtbar machen	ja	aktiv	TRUE FALSE	OK REVOKED UNKOWN	HIDDEN	OK DISABLED VERIFYABLE
Zertifikat von eGK lesen	ja	aktiv	TRUE FALSE	OK REVOKED UNKOWN	n/a	OK VERIFYABLE
Authentisierungsrequest mit eGK signieren	ja	aktiv	TRUE	OK UNKOWN	n/a	OK VERIFYABLE
Mit eGK verschlüsseln	ja	aktiv	TRUE	OK UNKOWN	n/a	OK VERIFYABLE
Mit eGK entschlüsseln	ja	aktiv	TRUE FALSE	OK REVOKED UNKOWN	n/a	OK VERIFYABLE

[<=]

Definiert eine Fachanwendung in ihrer Fachmodulspezifikation abweichende Kriterien oder von den in TAB\_ADV\_384 definierten Bedingungen abweichende Vorbedingung zur Zulässigkeit ihrer Anwendungsfälle, so sind jene der Fachanwendung bindend.

### 6.1.3 Hinweistext zu Fachanwendung

Nach dem Start der AdV-App und Stecken der eGK wird dem Versicherten eine Startoberfläche angezeigt, auf der klar erkennbar ist, welche Art von Daten verwaltet werden können. Hier sollen alle Anwendungen, die aktuell bereitstehen, in übersichtlicher Form angezeigt werden, auch wenn der Versicherte nicht alle Anwendungen nutzt bzw. in bestimmte Anwendungen nicht oder noch nicht eingewilligt hat.

#### AdV-A\_2547 - Empfehlung: Hinweistext zu Fachanwendung



Die AdV-App SOLL im Kontext jeder Fachanwendung einen Hinweistext gemäß TAB\_ADV\_461 anzeigen, der den Zweck der Fachanwendung beschreibt.

**Tabelle 8: TAB\_ADV\_461 – Benennung der Anwendungen und Hinweise am Terminal**

Anwendung	Anzeigetext	Hinweistext
Allgemein: Verwaltung der eGK durch den Versicherten	Ihre Gesundheitskarte	Sie können das Zugriffsprotokoll auf Ihrer Gesundheitskarte einsehen, Ihre PIN verwalten und Ihre Versichertendaten einsehen und online aktualisieren lassen.
AMTS	Medikationsplan	Sie können die auf Ihrer Gesundheitskarte gespeicherten Daten des Medikationsplans und arzneimitteltherapiesicherheitsrelevante Daten samt Einwilligung auf der Gesundheitskarte verbergen und Ihre verborgenen Daten wieder sichtbar machen.
DPE	Hinweise auf Persönliche Erklärungen	Hinweise auf persönliche Erklärungen sind Angaben zu den Aufbewahrungsorten von Patientenverfügung, Vorsorgevollmacht, Erklärung zur Organ- und Gewebespender (Organspendeausweis) und weiteren persönlichen Dokumenten. Sie können die auf Ihrer Gesundheitskarte gespeicherten Hinweise auf persönliche Erklärungen einsehen, bearbeiten und wenn gewünscht löschen. Zusätzlich können Sie Ihre Hinweise auf der Gesundheitskarte verbergen und die verborgenen Hinweise wieder sichtbar machen.
NFD	Notfalldaten	Sie können Ihre Notfalldaten auf der Gesundheitskarte verbergen und einen verborgenen Datensatz wieder sichtbar machen.

[<=]

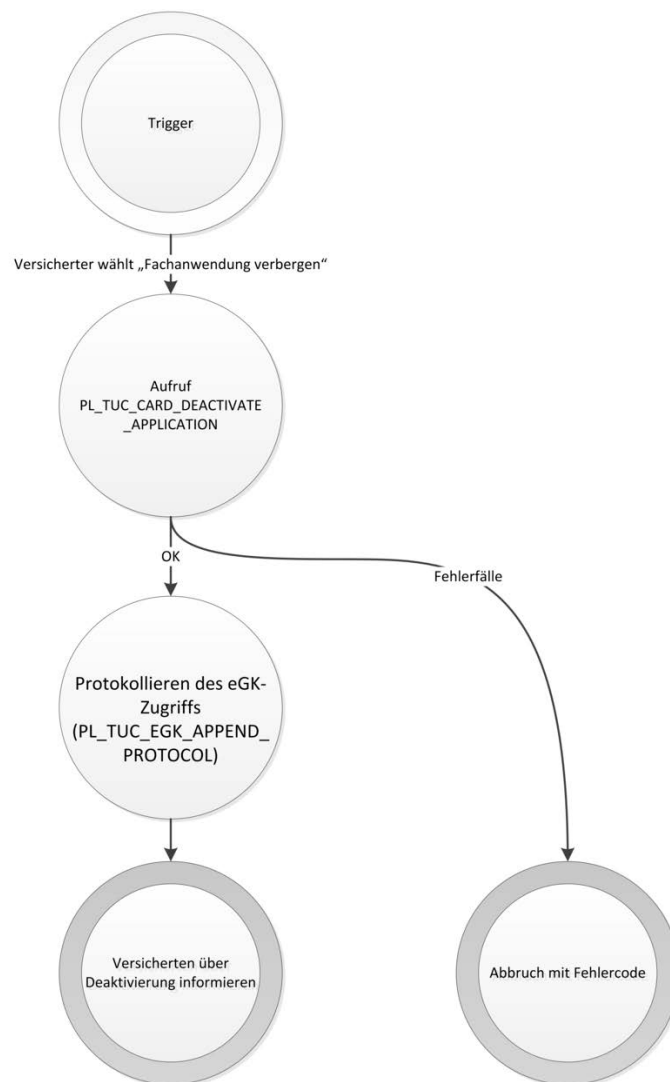
#### 6.1.4 Generische Anwendungsfälle

Dieses Kapitel beschreibt die generischen Anwendungsfälle, welche durch Anwendungsfälle verschiedener Fachanwendungen genutzt werden. Unter anderem wird die Möglichkeit geboten PIN-Objekte, die im Kontext einer Fachanwendung stehen, ein- oder auszuschalten.

##### 6.1.4.1 Anwendung auf eGK deaktivieren

Der Versicherte kann die Daten einer freiwilligen Anwendung verbergen. Durch das Verbergen ist nur noch für den Versicherten selbst erkennbar, dass die freiwillige Anwendung eingerichtet ist. Die Daten der Fachanwendung sind weiterhin auf der eGK vorhanden, können aber weder angezeigt noch verändert werden.

Die folgende Abbildung ABB\_ADV\_305 zeigt informativ, welche Schritte für Anwendungsfall AdV-UC\_14 „Anwendung auf eGK deaktivieren“ ausgeführt werden müssen.



**Abbildung 7: ABB\_ADV\_305 – Ablauf „Anwendung auf eGK deaktivieren“**

#### **AdV-A\_2453 - AdV-UC\_14: Anwendung auf eGK deaktivieren**

Die AdV-App MUSS den Anwendungsfall AdV-UC\_14 „Anwendung auf eGK deaktivieren“ gemäß TAB\_ADV\_305 umsetzen.

**Tabelle 9: TAB\_ADV\_305 – AdV-UC\_14 „Anwendung auf eGK deaktivieren“**

Name des Anwendungsfalls	„Anwendung auf eGK deaktivieren“
Hinweistext für den Versicherten	Siehe aufrufenden Anwendungsfall der Fachanwendung.

Auslöser	Der Versicherte möchte in einer Fachanwendung eine Anwendung auf seiner eGK verbergen. Dazu nutzt die Fachanwendung vorliegenden generischen Anwendungsfall.
Akteure	Dieser Anwendungsfall wird nicht direkt vom Versicherten aufgerufen sondern in Rahmen eines übergeordneten Anwendungsfalls einer Fachanwendung, welche die benötigten Eingangsdaten bereitstellt.
Vorbedingung	Die Fachanwendung übergibt den Identifikator der zu deaktivierenden Applikation. Siehe auch übergreifende Vorbedingungen.
Nachbedingung	Anwendung ist auf der eGK verborgen. Für eGK >= G2.1 wurde das Verbergen auf der eGK protokolliert.
Standardablauf	Die Umsetzung ist in „TAB_ADV_306 – Ablaufaktivitäten – AdV-UC_14“ beschrieben. <ol style="list-style-type: none"> <li>1. PL_TUC_CARD_DEACTIVATE_APPLICATION aufrufen</li> <li>2. PL_TUC_CARD_DEACTIVATE_APPLICATION Ergebnis verarbeiten</li> <li>3. Protokollieren des eGK-Zugriffs (für eGK &gt;=G2.1)</li> <li>4. Ergebnis anzeigen</li> </ol>
Diagramm	Abbildung ABB_ADV_305 – Ablauf „Anwendung auf eGK deaktivieren“

Tabelle 10: TAB\_ADV\_306 – Ablaufaktivitäten – AdV-UC\_14

<b>1. PL_TUC_CARD_DEACTIVATE_APPLICATION aufrufen</b>	
Plattformbaustein	PL_TUC_CARD_DEACTIVATE_APPLICATION
<i>Eingangsdaten</i>	
Identifikator	Der Identifikator der zu deaktivierenden Applikation gemäß PL_TUC_CARD_INFORMATION.<Anwendung> (z.B. DF.NFD, DF.DPE, DF.AMTS).
<i>Beschreibung</i>	

Für die Deaktivierung der Applikation wird der Plattformbaustein genutzt.	
<b>2. PL_TUC_CARD_DEACTIVATE_APPLICATION Ergebnis verarbeiten</b>	
<i>Rückgabedaten</i>	
OK	Anwendung erfolgreich deaktiviert
Fehlerfälle	Siehe Beschreibung PL_TUC_CARD_DEACTIVATE_APPLICATION und „TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine“ für die Behandlung in der AdV-App.
<i>Beschreibung</i>	
Das Deaktivieren der Anwendung basiert auf dem parametrisierten Plattformbaustein PL_TUC_CARD_DEACTIVATE_APPLICATION. Dieser liefert eine Statusmeldung zurück. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben.	
<b>3. Protokollieren des eGK-Zugriffs</b>	
Plattformbaustein	PL_TUC_EGK_APPEND_PROTOCOL
<i>Eingangsdaten</i>	
DATATYPE	Wenn der Identifikator der zu deaktivierenden Applikation <ul style="list-style-type: none"> <li>• „DF.NFD“ ist, dann „b“</li> <li>• „DF.DPE“ ist, dann „c“</li> <li>• „DF.AMTS“ ist, dann „e“</li> </ul>
ACCESSTYPE	„V“ (Verbergen der Anwendung).
<i>Rückgabedaten</i>	
OK	Protokolleintrag erfolgreich hinzugefügt
Fehlerfälle	Siehe Beschreibung PL_TUC_EGK_APPEND_PROTOCOL und Tabelle „TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine“ für die Behandlung in der AdV-App. Im Fehlerfall wird der Versicherte in „4. Ergebnis anzeigen“ über das Ergebnis der Deaktivierung und den aufgetretenen Fehler bei der

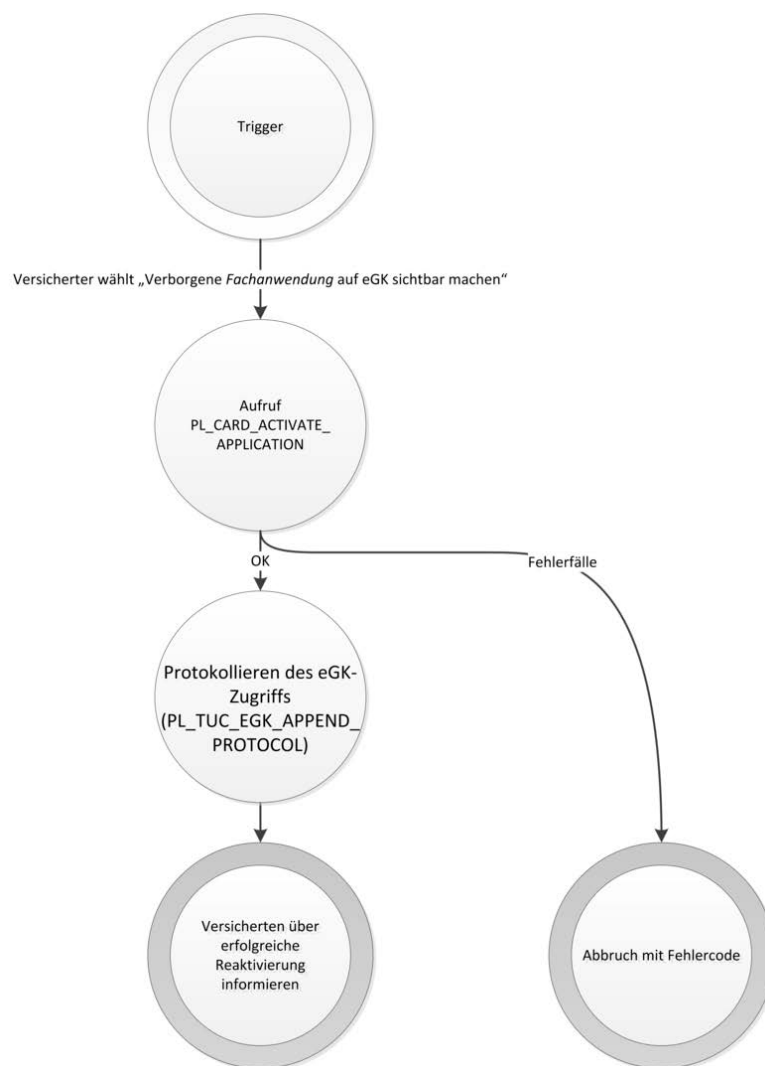
	Protokollierung informiert.
<i>Beschreibung</i>	
Die Protokollierung des Datenzugriffs erfolgt für eine eGK der Version größer oder gleich G2.1.  Der Aufbau der Eingangsdaten wird in PL_TUC_EGK_APPEND_PROTOCOL beschrieben.	
<b>4. Ergebnis anzeigen</b>	
Hinweis an den Versicherten	Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen.

[&lt;=]

#### 6.1.4.2 Anwendung auf eGK reaktivieren

Der Versicherte kann nach vorherigem Verbergen die Daten einer freiwilligen Anwendung wieder sichtbar machen.

Die folgende Abbildung ABB\_ADV\_383 zeigt informativ, welche Schritte für Anwendungsfall Adv-UC\_15 „Anwendung auf eGK reaktivieren“ ausgeführt werden müssen.



**Abbildung 8: ABB\_ADV\_383 – Ablauf „Anwendung auf eGK reaktivieren“**

**AdV-A\_2454 - AdV-UC\_15: Anwendung auf eGK reaktivieren**

Die AdV-App MUSS den Anwendungsfall AdV-UC\_15 „Anwendung auf eGK reaktivieren“ gemäß TAB\_ADV\_383 umsetzen.

**Tabelle 11: TAB\_ADV\_383 – AdV-UC\_15 „Anwendung auf eGK reaktivieren“**

Name des Anwendungsfalls	„Anwendung auf eGK reaktivieren“
Hinweistext für den Versicherten	Siehe aufrufenden Anwendungsfall der Fachanwendung.
Auslöser	Der Versicherte möchte in einer Fachanwendung eine verborgene Anwendung auf seiner eGK wieder sichtbar machen. Dazu nutzt die Fachanwendung vorliegenden generischen Anwendungsfall.

Akteure	Dieser Anwendungsfall wird nicht direkt vom Versicherten aufgerufen sondern in Rahmen eines übergeordneten Anwendungsfalls einer Fachanwendung, welche die benötigten Eingangsdaten bereitstellt.
Vorbedingung	Die Fachanwendung übergibt den Identifikator der wieder sichtbar zu machenden Applikation. Siehe auch übergreifende Vorbedingungen.
Nachbedingung	Anwendung ist auf der eGK wieder sichtbar. Für eGK >= G2.1 wurde das Reaktivieren auf der eGK protokolliert.
Standardablauf	Die Umsetzung ist in „TAB_ADV_307 – Ablaufaktivitäten – AdV-UC_15“ beschrieben. <ol style="list-style-type: none"> <li>1. PL_TUC_CARD_ACTIVATE_APPLICATION aufrufen</li> <li>2. PL_TUC_CARD_ACTIVATE_APPLICATION Ergebnis verarbeiten</li> <li>3. Protokollieren des eGK-Zugriffs (für eGK &gt;=G2.1)</li> <li>4. Ergebnis anzeigen</li> </ol>
Diagramm	Abbildung ABB_ADV_383 – Ablauf „Anwendung auf eGK reaktivieren“

Tabelle 12: TAB\_ADV\_307 – Ablaufaktivitäten – AdV-UC\_15

<b>1. PL_TUC_CARD_ACTIVATE_APPLICATION aufrufen</b>	
Plattformbaustein	PL_TUC_CARD_ACTIVATE_APPLICATION
<i>Eingangsdaten</i>	
Identifikator	Der Identifikator der wieder sichtbar zu machenden Applikation gemäß PL_TUC_CARD_INFORMATION.<Anwendung> (z.B. DF.NFD, DF.DPE, DF.AMTS).
<i>Beschreibung</i>	Für die Aktivierung der Applikation wird der Plattformbaustein genutzt.
<b>2. PL_TUC_CARD_ACTIVATE_APPLICATION Ergebnis verarbeiten</b>	
<i>Rückgabedaten</i>	
OK	Anwendung erfolgreich aktiviert

Fehlerfälle	Siehe Beschreibung PL_TUC_CARD_ACTIVATE_APPLICATION und „TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine“ für die Behandlung in der AdV-App.
<i>Beschreibung</i>	Das Aktivieren der Anwendung basiert auf dem parametrisierten Plattformbaustein PL_TUC_CARD_ACTIVATE_APPLICATION. Dieser liefert eine Statusmeldung zurück. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben.
<b>3. Protokollieren des eGK-Zugriffs</b>	
Plattformbaustein	PL_TUC_EGK_APPEND_PROTOCOL
<i>Eingangsdaten</i>	
DATATYPE	Wenn der Identifikator der zu deaktivierenden Applikation <ul style="list-style-type: none"> <li>• „DF.NFD“ ist, dann „b“</li> <li>• „DF.DPE“ ist, dann „c“</li> <li>• „DF.AMTS“ ist, dann „e“</li> </ul>
ACCESSTYPE	„S“ (Sichtbar machen der verborgenen Anwendung).
<i>Rückgabedaten</i>	
OK	Protokolleintrag erfolgreich hinzugefügt
Fehlerfälle	Siehe Beschreibung PL_TUC_EGK_APPEND_PROTOCOL und „TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine“ für die Behandlung in der AdV-App. Im Fehlerfall wird der Versicherte in „4. Ergebnis anzeigen“ über das Ergebnis der Aktivierung und den aufgetretenen Fehler bei der Protokollierung informiert.
<i>Beschreibung</i>	Die Protokollierung des Datenzugriffs erfolgt für eine eGK der Version größer oder gleich G2.1.  Der Aufbau der Eingangsdaten wird in PL_TUC_EGK_APPEND_PROTOCOL beschrieben.
<b>4. Ergebnis anzeigen</b>	
Hinweis an den Versicherten	Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der



	Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen.
--	--

[&lt;=]

#### 6.1.4.3 PIN-Verwaltung

Auf der eGK des Versicherten sind mehrere PIN-Objekte gespeichert. Wird im Aufruf der PIN-Operationen Ändern und Entsperren der Identifier einer Multireferenz-PIN (MRPIN) übergeben, so wirkt diese Operation auf die referenzierte PIN und betrifft auch alle übrigen Multireferenz-PINs, die auf diese PIN verweisen. Aktuell sind folgende PIN-Referenzen vorgesehen:

- Versicherten-PIN (PIN.CH)  
(auch verwendet als MRPIN.NFD, MRPIN.NFD\_READ, MRPIN.DPE, MRPIN.DPE\_READ, MRPIN.GDD, MRPIN.OSE, MRPIN.AMTS)
- Vertreter-PIN für eMP/AMTS (PIN.AMTS\_REP)

Die oben genannten Multireferenz-PINs können genutzt werden, um die Versicherten-PIN PIN.CH im Kontext der aktuellen Anwendung zu ändern, ohne auf der eGK zunächst in ein anderes Verzeichnis zu navigieren. Das heißt der Anwendungsfall zum Ändern oder Entsperren der Versicherten-PIN darf vom Versicherten im Kontext der jeweils aktiven Fachanwendung erfolgen, wenn der MRPIN der Fachanwendung als PIN-Referenz angegeben wird. Das Einschalten/Ausschalten einer MRPIN wirkt sich jeweils nur auf den MRPIN der referenzierten Fachanwendung aus. Die Benutzeroberfläche muss es dem Versicherten ermöglichen, den Status eines PIN-Objektes zu erfahren. Dies kann über eine Übersicht über alle PIN-Objekte oder in den Anwendungen erfolgen.

#### AdV-A\_2535 - Anzeige des Status eines PIN-Objekts

Die AdV-App MUSS dem Versicherten über die Benutzeroberfläche den aktuellen Status eines ausschaltbaren PIN-Objekts darstellen.[<=]

Die AMTS-Vertreter-PIN darf in den PIN-Operationen nur im Kontext der Fachanwendung AMTS referenziert werden.

##### 6.1.4.3.1 PIN ändern

Mit der Umsetzung dieses Anwendungsfalls ändert der Versicherte eine im Parameter der Operation benannte PIN auf der eGK.

Die folgende Abbildung ABB\_ADV\_312 zeigt informativ, welche Schritte für Anwendungsfall AdV-UC\_01: „PIN ändern“ ausgeführt werden müssen.

#### AdV-A\_2458 - AdV-UC\_01: PIN ändern

Die AdV-App MUSS den Anwendungsfall AdV-UC\_01: „PIN ändern“ gemäß TAB\_ADV\_312 umsetzen.

**Tabelle 13: TAB\_ADV\_312 – PIN der eGK ändern**

Name des Anwendungsfalls	„PIN ändern“
--------------------------	--------------

Hinweistext für den Versicherten	Siehe aufrufenden Anwendungsfall der Fachanwendung.
Auslöser	Dieser Anwendungsfall wird nicht direkt vom Versicherten aufgerufen, sondern im Rahmen eines übergeordneten Anwendungsfalls, welche die benötigten Eingangsdaten (den Identifikator des Passwortobjektes) bereitstellt.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	PIN wurde geändert.
Standardablauf	<p>Die Umsetzung ist in „TAB_ADV_313 – Ablaufaktivitäten – PIN ändern“ beschrieben.</p> <ol style="list-style-type: none"> <li>1. PL_TUC_CARD_CHANGE_PIN nutzen</li> <li>2. PL_TUC_CARD_CHANGE_PIN Ergebnis verarbeiten</li> <li>3. Ergebnis anzeigen</li> </ol>
Diagramm	Abbildung ABB_ADV_312 – Ablauf des AdV-UC_01: „PIN ändern“

Tabelle 14: TAB\_ADV\_313 – Ablaufaktivitäten – PIN der eGK ändern

<b>1. PL_TUC_CARD_CHANGE_PIN nutzen</b>	
Plattformoperation	PL_TUC_CARD_CHANGE_PIN
<i>Eingangsdaten</i>	
Identifikator	Zulässige PIN-Referenzen gemäß PL_TUC_CARD_INFORMATION.<Pin_der_eGK> (z.B. PIN.CH, PIN. AMTS_REP und ggf. weitere, je nach Release der eGK)
Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im AdV-App-Benutzerinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT	<p>Für Identifikator in (PIN.CH, MRPIN.NFD, MRPIN.DPE, MRPIN.AMTS)</p> <p>Alte PIN: „Eingabe alte Versicherten-PIN: “ bzw. Neue PIN: „Eingabe neue Versicherten-PIN: “</p> <p>Für Identifikator = PIN.AMTS_REP</p> <p>Alte PIN: „Eingabe Versicherten-PIN: “ bzw. Neue PIN: „Eingabe neue Vertreter-PIN: “</p>
<i>Beschreibung</i>	Der Plattformbaustein wird zur Änderung den PIN genutzt.
<b>2. Rückgabewert von PL_TUC_CARD_CHANGE_PIN</b>	

<b>verarbeiten</b>	
<i>Rückgabedaten</i>	
OK	PIN erfolgreich geändert
Fehlerfälle	Siehe Beschreibung PL_TUC_CARD_CHANGE_PIN und „TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine“ für die Behandlung in der AdV- App.
<i>Beschreibung</i>	<p>Das Ändern einer PIN auf der eGK basiert auf der parametrisierten Plattformbaustein PL_TUC_CARD_CHANGE_PIN. Diese liefert ein Ergebnis zurück. Zur Änderung muss zwingend die Eingabe der alten PIN (bzw. bei Änderung der PIN.AMTS_REP Eingabe der Versicherten-PIN) erfolgen.</p> <p>Wird durch den Versicherten ein falsches altes PIN-Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung des PINs zurückgemeldet. Im Fehlerfall wird eine Fehlermeldung entsprechenden Details zurückgegeben.</p>
<b>3. Ergebnis anzeigen</b>	
<i>Hinweis an den Versicherten</i>	<p>Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen.</p> <p>Falls eine Warnung aufgetreten ist, wird diese dem Versicherten in verständlicher Form angezeigt. Bei einer Fehleingabe der Pin des Versicherten wird dem Versicherten die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PIN zurückgemeldet.</p>

[&lt;=]

#### 6.1.4.3.2 PIN auf eGK entsperren

Mit der Umsetzung dieses Anwendungsfalls entsperrt der Versicherte eine im Parameter der Operation benannte PIN auf der eGK.

Die folgende Abbildung ABB\_ADV\_316 zeigt informativ, welche Schritte für Anwendungsfall AdV-UC\_02: „PIN auf eGK entsperren“ ausgeführt werden müssen.

#### AdV-A\_2459 - AdV-UC\_02: PIN der eGK entsperren

Die AdV-App MUSS den Anwendungsfall AdV-UC\_02: „PIN der eGK entsperren“ gemäß TAB\_ADV\_316 umsetzen.

**Tabelle 15: TAB\_ADV\_316 – PIN der eGK entsperren**

Benennung des Anwendungsfalls	„PIN der eGK entsperren“
Hinweistext für den Versicherten	Siehe aufrufenden Anwendungsfall der Fachanwendung.
Auslöser	Der Versicherte möchte eine PIN auf seiner eGK entsperren. Dazu wählt er eine Aktion in der AdV-App aus, die das Entsperren startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nach-bedingung	PIN des Versicherten wurde entsperrt.
Standardablauf	<p>Die Umsetzung ist in „TAB_ADV_317 – Ablaufaktivitäten – PIN der eGK entsperren“ beschrieben.</p> <ol style="list-style-type: none"> <li>1. PL_TUC_CARD_UNBLOCK_PIN aufrufen</li> <li>2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten</li> <li>3. Ergebnis anzeigen</li> </ol>
Diagramm	Abbildung ABB_ADV_316 – Ablauf des AdV-UC_02: „PIN auf eGK entsperren“

**Tabelle 16: TAB\_ADV\_317 – Ablaufaktivitäten – PIN der eGK entsperren**

<b>1. PL_TUC_CARD_UNBLOCK_PIN aufrufen</b>	
Plattformbaustein	PL_TUC_CARD_UNBLOCK_PIN
Eingangsdaten	
Identifikator	Zulässige PIN-Referenzen gemäß PL_TUC_CARD_INFORMATION.<Pin_der_eGK> (z.B. PIN.CH, PIN.AMTS_REP und ggf. weitere, je nach Release der eGK)
Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im AdV-App-Benutzerinterface bei Aufruf der Umgebungsoperation	<p>Für Identifikator in (PIN.CH, MRPIN.NFD, MRPIN.DPE, MRPIN.AMTS)            PUK: „Eingabe PUK: “ bzw. Neue PIN: „Eingabe neue Versicherten-PIN: “            Für Identifikator = PIN.AMTS_REP            PIN.CH: „Eingabe Versicherten-PIN: “ bzw.</p>

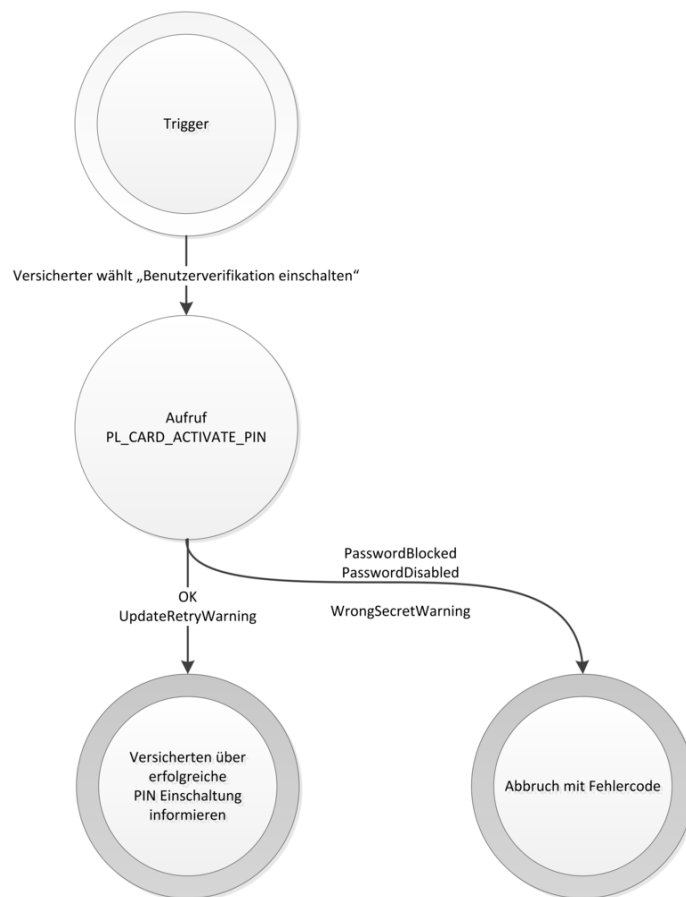
ENV_TUC_SECRET_INPUT	Neue PIN: „Eingabe neue Vertreter-PIN: “
Beschreibung	Für das Entsperren der PIN wird ein Plattformbaustein genutzt.
<b>2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten</b>	
<i>Rückgabedaten</i>	
OK	PIN wurde entsperrt.
PasswordBlocked	Die PUK wurde wegen zu häufiger Nutzung gesperrt. Der Versicherte muss darüber in verständlicher Form informiert und auf die Notwendigkeit einer neuen eGK hingewiesen werden.
Weitere Fehlerfälle	Siehe Beschreibung PL_TUC_CARD_UNBLOCK_PIN und „TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine“ für die Behandlung in der AdV-App.
<i>Beschreibung</i>	Das Entsperren einer PIN auf der eGK basiert auf dem parametrisierten Plattformbaustein PL_TUC_CARD_UNBLOCK_PIN. Zum Entsperren muss zwingend die Eingabe einer PUK bzw. im Fall des Entsperren der PIN.AMTS_REP die Eingabe der Versicherten-PIN erfolgen.  Wird durch den Versicherten ein falsches PIN- bzw. PUK-Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung des PUKs bzw. PINs zurückgemeldet. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben.
<b>3. Ergebnis anzeigen</b>	
<i>Hinweis an den Versicherten</i>	Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen. Falls eine Warnung aufgetreten ist, wird diese dem Versicherten in verständlicher Form angezeigt.

[&lt;=]

#### 6.1.4.3.3 PIN für Fachanwendung einschalten

Wenn die Multireferenz-PIN einer Fachanwendung deaktiviert ist, dann kann der Versicherte diese PIN mit diesem Anwendungsfall aktivieren.

Die folgende Abbildung ABB\_ADV\_308 zeigt informativ, welche Schritte für Anwendungsfall AdV-UC\_03 „PIN für Fachanwendung einschalten“ ausgeführt werden müssen.



**Abbildung 9: ABB\_ADV\_308 – Ablauf AdV-UC\_03 „PIN für Fachanwendung einschalten“**

#### **AdV-A\_2455 - AdV-UC\_03 „PIN für Fachanwendung einschalten“**

Die AdV-App MUSS den Anwendungsfall AdV-UC\_03 „PIN für Fachanwendung einschalten“ gemäß TAB\_ADV\_308 umsetzen.

**Tabelle 17: TAB\_ADV\_308 – AdV-UC\_03 „PIN für Fachanwendung einschalten“**

Benennung des Anwendungsfalls	„PIN für Fachanwendung einschalten“
Hinweistext für den Versicherten	Ein konkreter Hinweistext für den Versicherten wird für jede Fachanwendung im aufrufenden Anwendungsfall festgelegt.
Auslöser	Der Anwendungsfall wird ausgelöst, wenn der Versicherte auf seiner eGK die Benutzerverifikation einer Fachanwendung einschalten will. Dazu nutzt die Fachanwendung vorliegenden generischen Anwendungsfall.

Akteure	Dieser Anwendungsfall wird nicht direkt vom Versicherten aufgerufen sondern im Rahmen eines übergeordneten Anwendungsfalls einer Fachanwendung, welche die benötigten Eingangsdaten (bspw. den Identifikator des PIN-Objektes) bereitstellt.
Vorbedingung	Die Fachanwendung übergibt den <i>Identifikator</i> des Passwortobjektes. Siehe auch übergreifende Vorbedingungen.
Nachbedingung	Benutzerverifikation ist aktiviert.
Standardablauf	Die Umsetzung ist in „TAB_ADV_309 – Ablaufaktivitäten – AdV-UC_03“ beschrieben.  <ol style="list-style-type: none"> <li>1. PL_TUC_CARD_ENABLE_PIN aufrufen</li> <li>2. PL_TUC_CARD_ENABLE_PIN Ergebnis verarbeiten</li> <li>3. Ergebnis anzeigen</li> </ol>
Diagramm	Abbildung ABB_ADV_308 – Ablauf AdV-UC_03 „PIN für Fachanwendung einschalten“

Tabelle 18: TAB\_ADV\_309 – Ablaufaktivitäten – AdV-UC\_03

<b>1. PL_TUC_CARD_ENABLE_PIN aufrufen</b>	
Plattformbaustein	PL_TUC_CARD_ENABLE_PIN
Eingangsdaten	
Identifikator	Zulässige PIN-Referenzen gemäß PL_TUC_CARD_INFORMATION.<Pin_der_eGK> (z.B. MRPIN.NFD, MRPIN.DPE, MRPIN.GDD, MRPIN.AMTS und ggf. weitere, je nach Release der eGK)
Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im AdV-App-Benutzerinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT	Für Identifikator in (MRPIN.NFD, MRPIN.DPE, MRPIN.AMTS) MRPIN.NFD: „PIN-Schutz für Notfalldaten einschalten - Versicherten-PIN: “ MRPIN.DPE: „PIN-Schutz für Pers. Erklärungen einschalten - Versicherten-PIN: “ MRPIN.AMTS: „PIN-Schutz für Medikationsplan einschalten - Versicherten-PIN: “
Beschreibung	Für die Aktivierung der Benutzerverifikation wird der Plattformbaustein genutzt.
<b>2. PL_TUC_CARD_ENABLE_PIN Ergebnis verarbeiten</b>	

<i>Rückgabedaten</i>	
OK	PIN erfolgreich eingeschaltet
Fehlerfälle	Siehe Beschreibung PL_TUC_CARD_ENABLE_PIN und „TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine“ für die Behandlung in der AdV-App.
<i>Beschreibung</i>	Das Aktivieren der Benutzerverifikation basiert auf dem parametrisierten Plattformbaustein PL_TUC_CARD_ENABLE_PIN. Dieser liefert eine Statusmeldung zurück. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben. Wird durch den Versicherten ein falsches PIN- Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung des PINs zurückgemeldet. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben.
<b>3. Ergebnis anzeigen</b>	
<i>Hinweis an den Versicherten</i>	Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen. Falls eine Warnung aufgetreten ist, wird diese dem Versicherten in verständlicher Form angezeigt. Bei einer Fehleingabe der Pin des Versicherten wird dem Versicherten die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PIN zurückgemeldet.

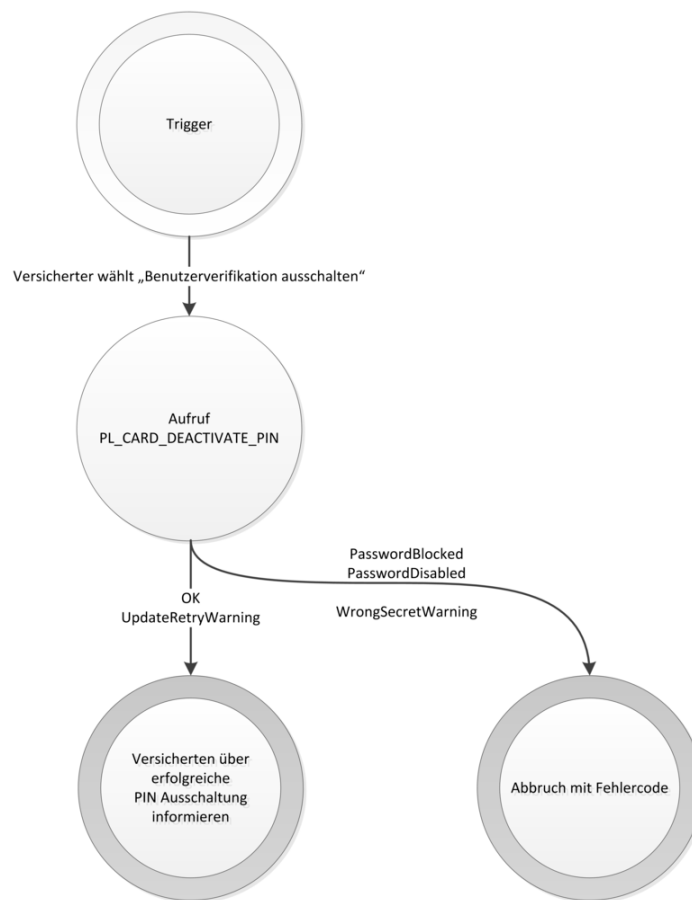
[&lt;=]

#### 6.1.4.3.4 PIN für Fachanwendung ausschalten

Um die Anzahl der beim Leistungserbringer notwendigen PIN-Eingaben pro Kartensteckzyklus zu minimieren, kann der Versicherte für bestimmte Fachanwendungen die Multireferenz-PIN für diese Fachanwendung deaktivieren.

Die folgende Abbildung ABB\_ADV\_310 zeigt informativ, welche Schritte für Anwendungsfall AdV-UC\_04 „PIN für Fachanwendung ausschalten“ ausgeführt werden müssen.





**Abbildung 10: ABB\_ADV\_310 – Ablauf AdV-UC\_04 „PIN für Fachanwendung ausschalten“**

#### **AdV-A\_2456 - AdV-UC\_04 Hinweis bei ausgeschaltetem PIN**

Die AdV-App MUSS, wenn der Versicherte den PIN einer Anwendung ausschalten möchte, dem Versicherten einen Hinweis anzeigen, dass bei ausgeschalteter PIN ein Arzt oder Apotheker auf die Daten dieser Anwendung ohne die Eingabe einer PIN zugreifen kann.[<=]

#### **AdV-A\_2457 - AdV-UC\_04 „PIN für Fachanwendung ausschalten“**

Die AdV-App MUSS den Anwendungsfall AdV-UC\_04 „PIN für Fachanwendung ausschalten“ gemäß TAB\_ADV\_310 umsetzen.

**Tabelle 19: TAB\_ADV\_310 – AdV-UC\_04 „PIN für Fachanwendung ausschalten“**

Name des Anwendungsfalls	„PIN für Fachanwendung ausschalten“
Hinweistext für den Versicherten	Ein konkreter Hinweistext für den Versicherten wird für jede Fachanwendung im aufrufenden Anwendungsfall festgelegt.

Auslöser	Der Anwendungsfall wird ausgelöst, wenn der Versicherte auf seiner eGK die Benutzerverifikation einer Fachanwendung ausschalten will. Dazu nutzt die Fachanwendung vorliegenden generischen Anwendungsfall.
Akteure	Dieser Anwendungsfall wird nicht direkt vom Versicherten aufgerufen sondern im Rahmen eines übergeordneten Anwendungsfalls einer Fachanwendung, welche die benötigten Eingangsdaten (den Identifikator des PIN-Objektes) bereitstellt.
Vorbedingung	MRPIN der Fachanwendung auf der eGK ist ausschaltbar. Die Fachanwendung übergibt den <i>Identifikator</i> des Passwortobjektes. Siehe auch übergreifende Vorbedingungen.
Nachbedingung	Benutzerverifikation ist deaktiviert.
Standardablauf	Die Umsetzung ist in „TAB_ADV_311 – Ablaufaktivitäten – AdV-UC_04“ beschrieben.  <ol style="list-style-type: none"> <li>1. PL_TUC_CARD_DISABLE_PIN aufrufen</li> <li>2. PL_TUC_CARD_DISABLE_PIN Ergebnis verarbeiten</li> <li>3. Ergebnis anzeigen</li> </ol>
Diagramm	Abbildung ABB_ADV_310 – Ablauf AdV-UC_04 „PIN für Fachanwendung ausschalten“

Tabelle 20: TAB\_ADV\_311 – Ablaufaktivitäten – AdV-UC\_04

<b>1. PL_TUC_CARD_DISABLE_PIN aufrufen</b>	
Plattformbaustein	PL_TUC_CARD_DISABLE_PIN
<i>Eingangsdaten</i>	
Identifikator	Zulässige PIN-Referenzen sind <i>MRPIN.NFD</i> , <i>MRPIN.DPE</i> , <i>MRPIN.GDD</i> , <i>MRPIN.AMTS</i> und ggf. weitere, je nach Ausprägung der eGK.
Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im AdV-App-Benutzerinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT	Für Identifikator in (MRPIN.NFD, MRPIN.DPE, MRPIN.AMTS) MRPIN.NFD: „PIN-Schutz für Notfalldaten ausschalten - Versicherten-PIN: “ MRPIN.DPE: „PIN-Schutz für Pers. Erklärungen ausschalten - Versicherten-PIN: “ MRPIN.AMTS: „PIN-Schutz für Medikationsplan ausschalten - Versicherten-PIN: “

<i>Beschreibung</i>	Für die Deaktivierung der Benutzerverifikation wird der Plattformbaustein genutzt.
<b>2. PL_TUC_CARD_DISABLE_PIN Ergebnis verarbeiten</b>	
<i>Rückgabedaten</i>	
OK	PIN erfolgreich abgeschaltet
Fehlerfälle	Siehe Beschreibung PL_TUC_CARD_DISABLE_PIN und „TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine“ für die Behandlung in der AdV-App.
<i>Beschreibung</i>	Das Deaktivieren der Benutzerverifikation basiert auf dem parametrisierten Plattformbaustein PL_TUC_CARD_DISABLE_PIN. Dieser liefert eine Statusmeldung zurück. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben. Wird durch den Versicherten ein falsches PIN-Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung des PINs zurückgemeldet. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben.
<b>3. Ergebnis anzeigen</b>	
<i>Hinweis an den Versicherten</i>	Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen. Falls eine Warnung aufgetreten ist, wird diese dem Versicherten in verständlicher Form angezeigt. Bei einer Fehleingabe der Pin des Versicherten wird dem Versicherten die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PIN zurückgemeldet.

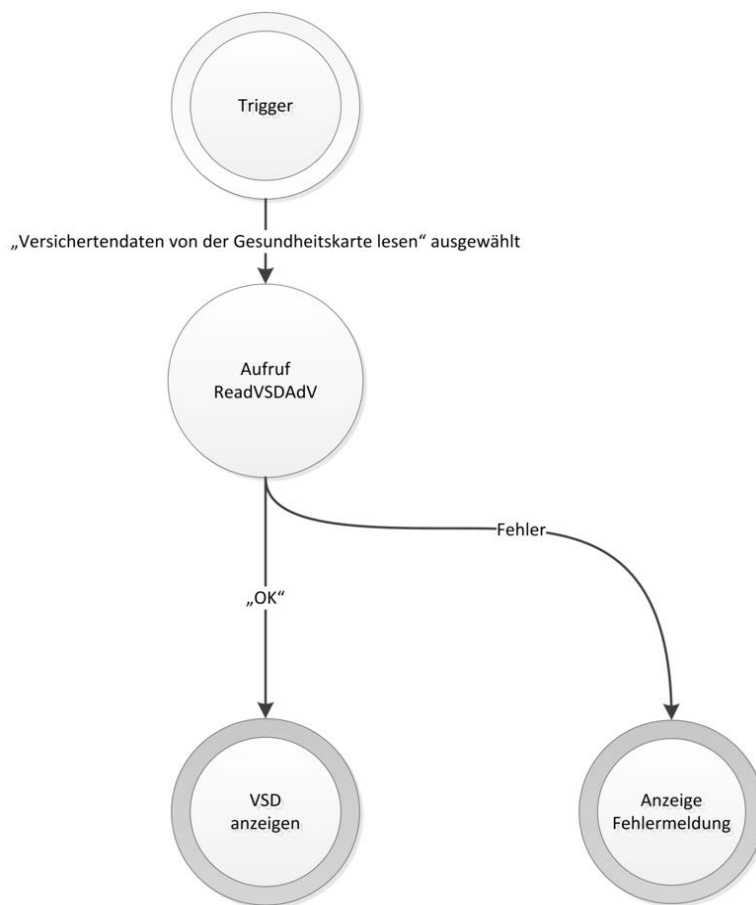
[&lt;=]

## 6.1.5 Verwaltung der eGK

### 6.1.5.1 VSD von eGK anzeigen

Mit der Umsetzung dieses Anwendungsfalls werden dem Versicherten die auf seiner eGK gespeicherten Versichertenstammdaten zur Anzeige gebracht.

Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall AdV-UC\_101: „VSD von eGK lesen“ ausgeführt werden müssen.



**Abbildung 11: ABB\_ADV\_317 - Ablauf des „VSD von eGK lesen“**

#### **AdV-A\_2460 - AdV-App: VSD von eGK anzeigen**

Die AdV-App MUSS den Anwendungsfall „VSD von eGK anzeigen“ gemäß TAB\_ADV\_314 umsetzen.

**Tabelle 21: TAB\_ADV\_314 – VSD von eGK anzeigen**

Benennung des Anwendungsfalls	„Versichertendaten anzeigen“
	Alternative Benennung, wenn PL_TUC_CARD_INFORMATION für DF.HCA den Status HIDDEN liefert: „Entsperren der Gesundheitsanwendung prüfen“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV001

Auslöser	Der Versicherte möchte die VSD von seiner eGK anzeigen lassen oder eine Onlineprüfung und -aktualisierung der VSD durchführen. Dazu wählt er eine Aktion in der AdV-App aus, die das Auslesen startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	Die Versichertenstammdaten werden in der AdV-App angezeigt.
Standardablauf	<p>Die Umsetzung ist in „TAB_ADV_315 – Ablaufaktivitäten – VSD von eGK anzeigen“ beschrieben.</p> <ol style="list-style-type: none"> <li>1. Aufruf Operation ReadVSDAdV</li> <li>2. Response von Operation ReadVSDAdV verarbeiten</li> <li>3. VSD anzeigen</li> </ol>
Diagramm	Abbildung ABB_ADV_317 - Ablauf des „VSD von eGK lesen“

Tabelle 22: TAB\_ADV\_315 – Ablaufaktivitäten – VSD von eGK anzeigen

<b>1. AdV-LeseRequest erzeugen</b>	
Operation	ReadVSDAdV
<i>Eingangsdaten</i>	
getGVD	True (GVD sollen gelesen werden)
<b>2. VSD-LeseResponse verarbeiten</b>	
<i>Rückgabedaten</i>	
StatusOperation	Status über die erfolgreiche Ausführung der Operation
StatusOnlineaktualisierung	Status über die erfolgreiche Ausführung einer Onlineaktualisierung
StatusVSD	Status der VSD auf der eGK

Versichertenstammdaten	Persönliche Versichertendaten (PD), Allgemeine Versicherungsdaten (VD), Geschützte Versichertendaten (GVD)
Beschreibung	<p>Das Lesen der Versichertenstammdaten basiert auf der Operation ReadVSDAdV. Im Ergebnis stehen die Elemente <code>PersoenlicheVersichertendaten</code>, <code>AllgemeineVersicherungsdaten</code> und <code>GeschuetzteVersichertendaten</code> zur Verfügung, die gemäß <code>Schema_VSD.xsd</code> strukturiert sind. Das Element <code>VSD_Status</code> ist gemäß <code>VSDService.xsd</code> strukturiert. Für weitere Informationen siehe auch <code>[gemSysL_VSDM#Anhang C]</code>.</p> <p>Im Erfolgsfall werden die angefragten Daten zurückgeliefert. Tritt während der Verarbeitung ein Fehler auf, wird eine entsprechende Fehlermeldung zurückgegeben. Die Fehlercodes 106, 107 und 114 weisen auf einen technischen Fehler hin. Sie sind jedoch keine fachlichen Fehler, d.h. der Anwendungsfall wurde trotz Fehlermeldung erfolgreich abgearbeitet. Dem Versicherten sind die folgenden Hinweise anzuzeigen :</p> <ul style="list-style-type: none"> <li>• Fehlercode 114: „Ihre Gesundheitskarte ist gesperrt. Bitte wenden Sie sich an Ihre Krankenkasse“</li> <li>• Fehlercode 106: „Ihre Gesundheitskarte ist ungültig. Bitte prüfen Sie, ob diese Gesundheitskarte Ihre aktuellste ist. Falls ja, wenden Sie sich bitte an Ihre Krankenkasse.“</li> <li>• Fehlercode 107: „Ihre Gesundheitskarte ist zeitlich abgelaufen. Bitte prüfen Sie, ob diese Gesundheitskarte Ihre aktuellste ist. Falls ja, wenden Sie sich bitte an Ihre Krankenkasse.“</li> </ul> <p>Für alle anderen Fehlercodes siehe Beschreibung ReadVSDAdV und „TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine“ für die Behandlung in der AdV-App.</p>
3. VSD anzeigen	
VSD aufbereiten	<p><code>PersoenlicheVersichertendaten</code> - XML-Element  <code>UC_PersoenlicheVersichertendatenXML</code></p> <p><code>AllgemeineVersicherungsdaten</code> - XML-Element  <code>UC_AllgemeineVersicherungsdatenXML</code></p> <p><code>GeschuetzteVersichertendaten</code> - XML-Element  <code>UC_GeschuetzteVersichertendatenXML</code>)</p> <p>Die Inhalte der oben angegebenen Elemente für PD, VD und GVD enthalten die Versichertenstammdaten. Die AdV-App muss die Inhalte der ReadVSDAdV Rückgabewerte aufbereiten (siehe Beschreibung der Rückgabewerte im Fachmodul VSDM)</p>

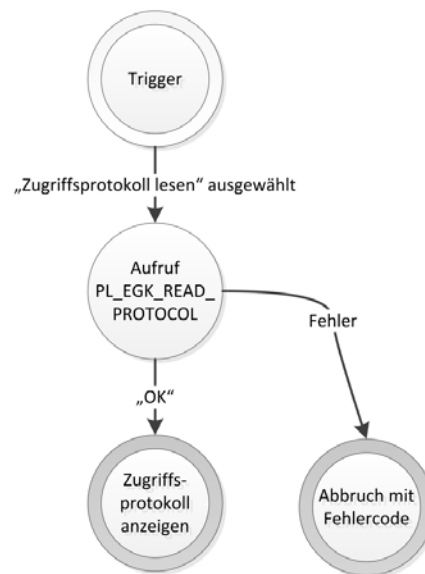
	[gemSpec_FM_VSDM] in der KTR Umgebung). Im Ergebnis stehen drei XML-Fragmente zur Verfügung, die gemäß Schema_VSD.xsd strukturiert sind. Für weitere Informationen siehe auch gemSysL_VSDM#Anhang C.
Aufbereitete VSD zur Anzeige bringen	<p>Die aus der Dekodierung ermittelten Versichertenstammdaten der eGK des Versicherten müssen dem Versicherten in verständlicher Form zur Anzeige gebracht werden. Dazu sind sämtliche Inhalte der XML-Strukturen aus UC_PersoенlicheVersichertendatenXML, UC_AllgemeineVersicherungsdatenXML und UC_GeschuetzteVersichertendatenXML anzuzeigen. Aus VSD_Status ist der Zeitpunkt der letzten Aktualisierung der VSD anzuzeigen.</p> <p>Der Inhalt von StatusOnlineaktualisierung ist wie folgt zu behandeln:          Die AdV-App MUSS dem Versicherten, falls eine Onlineaktualisierung durchgeführt wurde, den Hinweis „Die Versichertendaten auf Ihrer Gesundheitskarte wurden aktualisiert.“ anderenfalls „Die Versichertendaten auf Ihrer Gesundheitskarte sind aktuell.“ anzeigen.</p>

[&lt;=]

#### 6.1.5.2 Zugriffsprotokoll anzeigen

Mit der Umsetzung dieses Anwendungsfalls sollen dem Versicherten das auf seiner eGK gespeicherte Zugriffsprotokoll zur Anzeige gebracht werden.

Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall AdV-UC\_21: „Zugriffprotokoll von eGK lesen“ ausgeführt werden müssen.



**Abbildung 12: ABB\_ADV\_314 – Ablauf des AdV-UC\_21: „Zugriffsprotokoll anzeigen“**

#### **AdV-A\_2461 - AdV-App: Decodierung von Schlüsselwerten im Zugriffsprotokoll**

Die AdV-App MUSS zur besseren Lesbarkeit die Schlüsselwerte in den Zugriffsprotokolleinträgen gemäß [gemSpec\_Karten\_Fach\_TIP#Tab\_Karten\_Fach\_TIP\_010\_StrukturEF.Logging] decodieren und in für den Versicherten verständlichen Text übersetzen.[<=]

#### **AdV-A\_2462 - AdV-App: Decodierung von Schlüsselwerten im Zugriffsprotokoll – Fachmodul**

Die AdV-App MUSS zur besseren Lesbarkeit die Schlüsselwerte in den Zugriffsprotokolleinträgen gemäß der jeweiligen Festlegung der Fachmodule der Fachanwendungen (Fachmodulspezifikation) decodieren und in einen für den Versicherten verständlichen Text übersetzen.[<=]

#### **AdV-A\_2463 - AdV-App: Zugriffsprotokoll anzeigen**

Die AdV-App MUSS den Anwendungsfall „Zugriffsprotokoll anzeigen“ gemäß TAB\_ADV\_350 umsetzen.

**Tabelle 23: TAB\_ADV\_350 – Zugriffsprotokoll anzeigen**

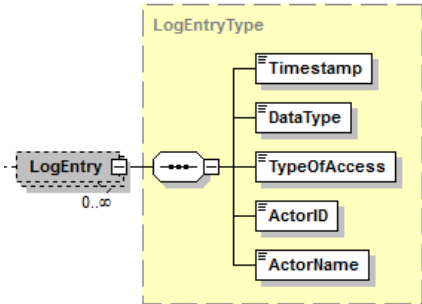
Benennung des Anwendungsfalls	„Zugriffsprotokoll anzeigen“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV002
Auslöser	Der Versicherte möchte das Zugriffsprotokoll seiner eGK anzeigen lassen. Dazu wählt er eine Aktion in der AdV-App aus, die das Auslesen des



	Protokolls startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	Das Zugriffsprotokoll wird dem Versicherten angezeigt.
Standardablauf	<p>Die Umsetzung ist in „TAB_ADV_351 – Ablaufaktivitäten – Zugriffsprotokoll anzeigen“ beschrieben.</p> <ol style="list-style-type: none"> <li>1. LeseRequest erzeugen</li> <li>2. LeseResponse verarbeiten</li> <li>3. Protokoll anzeigen</li> </ol>
Diagramm	Abbildung ABB_ADV_314 – Ablauf des AdV-UC_21: „Zugriffsprotokoll anzeigen“

Tabelle 24: TAB\_ADV\_351 – Ablaufaktivitäten – Zugriffsprotokoll anzeigen

<b>1. LeseRequest erzeugen</b>	
Plattformbaustein	PL_TUC_EGK_READ_PROTOCOL
<i>Eingangsdaten</i>	
-	-
<i>Beschreibung</i>	Es wird das gesamte Zugriffsprotokoll auf der elektronischen Gesundheitskarte ausgelesen.
<b>2. LeseResponse verarbeiten</b>	
<i>Rückgabedaten</i>	
OK + Liste	„Daten wurden erfolgreich gelesen“ Beinhaltet das Zugriffsprotokoll. Den Aufbau zeigt die folgende Abbildung und wird in [gemSpec_Karten_Fach_TIP] definiert.

	
CorruptDataWarning +Liste	„Daten gelesen, Speicher möglicherweise defekt “ Beinhaltet das Zugriffsprotokoll. Den Aufbau zeigt die Abbildung oben.
Beschreibung	Das Auslesen des Zugriffsprotokolls auf der eGK basiert auf dem Plattformbaustein PL_TUC_EGK_READ_PROTOCOL. Dieser liefert den Status der Leseoperation und im Erfolgsfall die Recordliste zurück. Im Fehlerfall wird eine Fehlermeldung mit einem Fehlercode zurückgegeben.
<b>3. Protokoll anzeigen</b>	
Zugriffsprotokoll zur Anzeige bringen	Die aus der eGK des Versicherten gelesenen Protokolleinträge sollen dem Versicherten vollständig zur Anzeige gebracht werden. Dazu sind sämtliche Elemente vom Typ LogEntry in einer geeigneten Form anzuzeigen. Das Protokoll umfasst bis zu 50 Einträge. Die im Protokoll enthaltenen Felder haben dabei die folgende Bedeutung: Timestamp: Zeitpunkt, zu dem der Protokolleintrag erzeugt wurde Data Type: Identifikator der Anwendung auf der eGK, auf die zugegriffen wurde Type of Access: Art des Zugriffs auf die Anwendung auf der eGK Actor-ID: Identifikator des Akteurs, des Zugriffs auf die Anwendung auf der eGK Actor Name: Klarname des Akteurs, des Zugriffs auf die Anwendung auf der eGK

[&lt;=]

**AdV-A\_2464 - AdV-App: Filtern von Protokolleinträgen**

Die AdV-App MUSS es dem Versicherten ermöglichen, die angezeigten Einträge des Zugriffsprotokolls nach Anwendung, Art des Zugriffs, Zeitraum und zugreifendem Akteur zu filtern.[<=]

**6.1.5.3 Versicherten-PIN ändern**

Mit diesem Anwendungsfall kann der Versicherte das Geheimnis der Versicherten-PIN ändern.

Für die Umsetzung wird der in Kap. 6.1.4.3.1 PIN ändern beschriebene generische Anwendungsfall genutzt.

**AdV-A\_2465 - AdV-App: Versicherten-PIN ändern**

Die AdV-App MUSS den Anwendungsfall „Versicherten-PIN ändern“ gemäß TAB\_ADV\_352 umsetzen.

**Tabelle 25: TAB\_ADV\_352 – Versicherten-PIN der eGK ändern**

Benennung des Anwendungsfalls	„Versicherten-PIN ändern“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV003
Auslöser	Der Versicherte möchte die Versicherten-PIN auf seiner eGK ändern. Dazu wählt er eine Aktion in der AdV-App aus, die das Ändern startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	PIN wurde geändert.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls AdV-UC_01: „PIN ändern“ mit dem Parameter Identifikator = PIN.CH

[&lt;=]

**6.1.5.4 Versicherten-PIN entsperren**

Mit der Umsetzung dieses Anwendungsfalls kann die gesperrte Versicherten-PIN entsperrt werden.

Für die Umsetzung wird der in Kap. 6.1.4.3.2 PIN auf eGK entsperren beschriebene generische Anwendungsfall genutzt.

**AdV-A\_2466 - AdV-App: Versicherten-PIN entsperren**

Die AdV-App MUSS den Anwendungsfall „Versicherten-PIN entsperren“ gemäß TAB\_ADV\_353 umsetzen.

**Tabelle 26 TAB\_ADV\_353 – Versicherten-PIN entsperren**

Benennung des Anwendungsfalls	„Versicherten-PIN entsperren“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV004
Auslöser	Der Versicherte möchte seine gesperrte Versicherten-PIN entsperren. Dazu wählt er eine Aktion in der AdV-App aus, die das Entsperren startet.

Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nach-bedingung	Die Versicherten-PIN auf der eGK ist entsperrt.
Standardablauf	<p>Die Umsetzung ist in der Tabelle TAB_ADV_354 – Ablaufaktivitäten – Versicherten-PIN entsperren beschrieben.</p> <ol style="list-style-type: none"> <li>1. Abfrage Kenntnis PUK</li> <li>2. Ergebnis Abfrage Kenntnis PUK verarbeiten</li> <li>3. Gemäß Beschreibung AdV-UC_02: „PIN auf eGK entsperren“</li> </ol>

Tabelle 27: TAB\_ADV\_354 – Ablaufaktivitäten – Versicherten-PIN entsperren

<b>1. Abfrage Kenntnis PUK</b>	
<i>Beschreibung</i>	Die AdV-App MUSS den Versicherten vor einem Versuch der Entsperrung fragen, ob der PUK bekannt ist
<b>2. Ergebnis Abfrage Kenntnis PUK verarbeiten</b>	
Rückgabedaten	
JA (Dem Versicherten ist der PUK bekannt.)	Aufruf des folgenden Schritts im Standardablauf.
NEIN (Dem Versicherten ist der PUK nicht bekannt.)	Den Versicherten darüber informieren, dass die eGK nur mit dem PUK entsperrt werden kann. Zusätzlich soll ein Hinweis gegeben werden, wie der Versicherte den PUK erhalten hat und wie er ihn ggf. erneut erhalten kann. Falls eine AdV-Sitzung aktiv ist, muss anschließend der Anwendungsfall "AdV-Sitzung beenden" aufgerufen werden.
<b>3. Umsetzung entsprechend AdV-UC_02: „PIN der eGK entsperren“</b>	
<i>Beschreibung</i>	Die weitere Umsetzung erfolgt gemäß der Beschreibung des Anwendungsfalls AdV-UC_02: „PIN der eGK entsperren“ mit dem Parameter <code>Identifikator = PIN.CH</code>

[&lt;=]

**AdV-A\_2467 - AdV-App: AdV-UC\_02: Abbruch der AdV-Sitzung**

Die AdV-App MUSS, falls die PIN.CH nicht erfolgreich entsperrt wurde und eine AdV-Sitzung aktiv ist, den Anwendungsfall "AdV-Sitzung beenden" aufrufen.[<=]

#### **6.1.5.5 Datenübertragung bei Kartentausch**

Dieser Anwendungsfall erlaubt dem Versicherten, Daten von seiner eGK auf eine weitere, d.h. ihm neu ausgestellte eGK zu kopieren. Mit der Umsetzung dieses Anwendungsfalls kann der Versicherte seine Daten – welche in der KTR Umgebung zugreifbar sind – auf eine neue eGK übertragen, wenn der Versicherte von seiner Krankenversicherung eine neue Karte ausgestellt bekommt.

Der Versicherte kann die Datenbereiche auswählen, deren Daten er auf die Zielkarte übertragen will. Dafür muss der Datenbereich dieser Anwendung(en) auf der Zielkarte leer sein. In einer Datenübertragung können ein oder mehrere Datenbereiche übertragen werden. Der Versicherte kann die Datenübertragung erneut durchführen, solange noch nicht alle Datenbereiche übertragen wurden.

Zum Zeitpunkt der Erstellung dieser Spezifikation kann in der KTR-AdV nur der Datenbereich DPE ausgewählt werden.

Die unten beschriebene Lösung sieht vor, dass am KTR-AdV-Terminal für die eGK nur ein Slot zur Verfügung steht, so dass die beiden eGKs nacheinander gesteckt werden müssen. In diesem Ausnahmefall dürfen die medizinischen Daten des Versicherten über den Steckzyklus der Quellkarte hinaus in der AdV-App gespeichert werden. Nach dem Ende des Vorgangs müssen die Daten gelöscht werden.

Die AdV-App steuert den Ablauf der Datenübertragung vom Lesen der Daten von der Quellkarte über den Wechsel der Karten bis zum Schreiben auf die neue Karte und Löschen der zwischengespeicherten Daten. Für die anwendungsspezifischen Lese- und Schreiboperationen ruft es interne Methoden der entsprechenden Fachmodule auf.

Die Datenübertragung soll auch dann möglich sein, wenn das AUT-Zertifikat der Quellkarte zeitlich abgelaufen oder online ungültig ist. Daher muss die AdV-App eine eGK auch in diesem Fall akzeptieren.

Bei den folgenden Beschreibungen wird angenommen, dass zu Beginn die Quellkarte steckt. Dies kann die AdV-App jedoch erst prüfen, wenn die Zielkarte gesteckt wurde und ihr AUT-Zertifikat ein neueres Gültigkeitsbeginn-Datum aufweist als das der anderen eGK.

Falls das Gültigkeitsbeginn-Datum der Zielkarte kleiner als das Gültigkeitsbeginn-Datum der Quellkarte ist, wird die Kopieroperation abgebrochen. Weiterhin führt zum Abbruch, wenn die Zielkarte mathematisch oder zeitlich ungültig ist oder gesperrt wurde.

#### **AdV-A\_2548 - Auswahl der zu kopierenden Daten durch den Versicherten**

Die AdV-App MUSS beim Start des Anwendungsfalls Datenübertragung bei Kartentausch und vor den Kopier-Operationen die Liste der zu kopierenden Anwendungen beim Versicherten abfragen. Dem Versicherten ist dafür die Liste der in der KTR Umgebung zugreifbaren und kopierbaren Anwendungen zur Auswahl anzubieten.[<=]

#### **AdV-A\_2549 - Reaktion auf Kartenevents während Anwendungsfall Datenübertragung bei Kartentausch**

Die AdV-App MUSS, falls der Anwendungsfall "Datenübertragung bei Kartentausch durchführen" umgesetzt wird, während der gesamten Datenübertragung sicherstellen, dass die KVNR (Unveränderbarer Teil) der Quell- und Ziel-Karte mit der zum Beginn der Sitzung temporär gespeicherten KVNR (Unveränderbarer Teil) der Quell-Karte übereinstimmt und bei Ungleichheit die Sitzung nach Hinweis abbrechen.[<=]

### AdV-A\_2550 - Aufrechterhaltung der Sitzung des Versicherten bei gezogener Karte während Anwendungsfall Datenübertragung bei Kartentausch

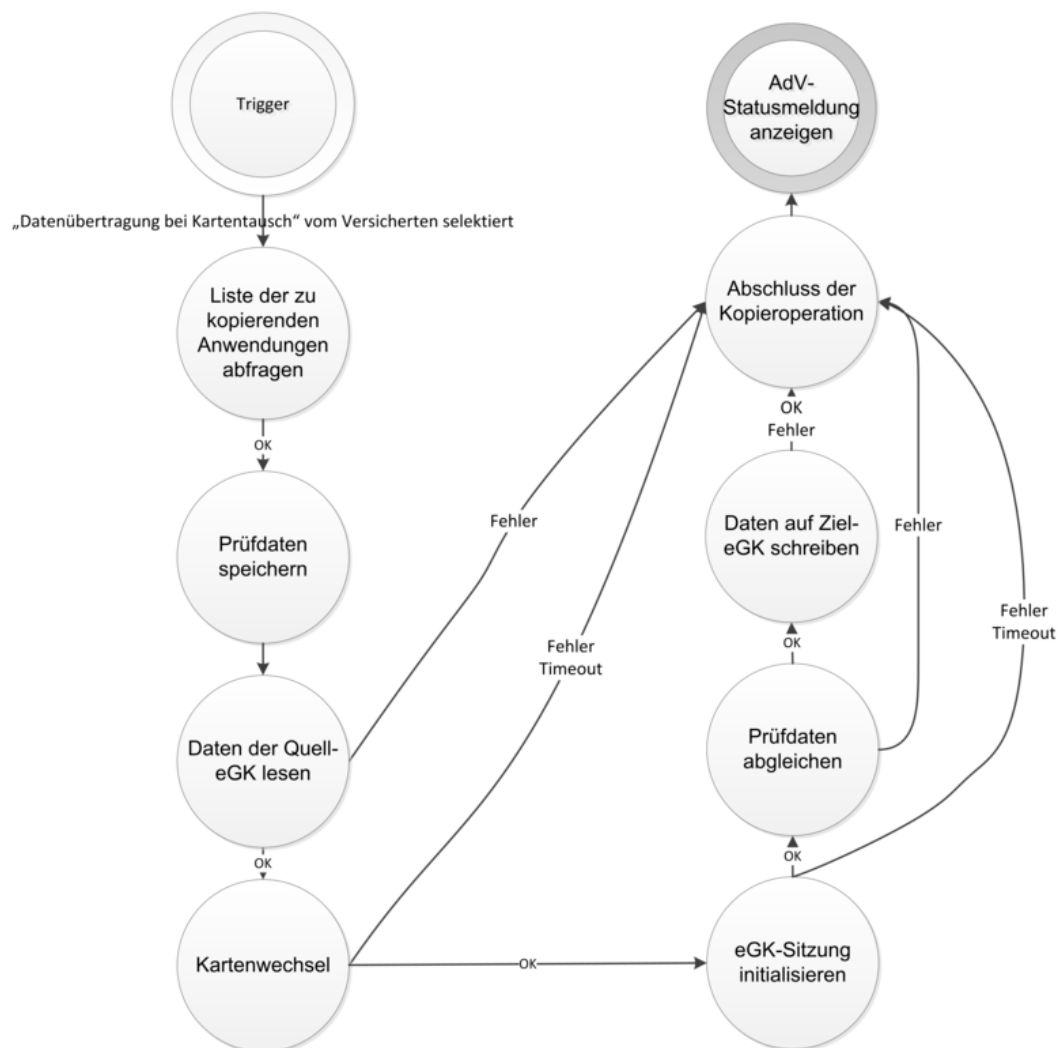
Die AdV-App MUSS, falls der Anwendungsfall "Datenübertragung bei Kartentausch durchführen" umgesetzt wird und während des Anwendungsfalls die eGK des Versicherten aus dem Kartenterminal gezogen wird ohne dass der Versicherte die Operation explizit abbricht, die Sitzung des Versicherten für zwei Minuten aufrecht erhalten.[<=]

### AdV-A\_2551 - Keine Neuanmeldung des Versicherten bei Stecken der eGK während Anwendungsfall Datenübertragung bei Kartentausch

Die AdV-App MUSS, falls der Anwendungsfall "Datenübertragung bei Kartentausch durchführen" umgesetzt wird und während des Anwendungsfalls eine neue eGK mit derselben KVNR (Unveränderbarer Teil) des angemeldeten Versicherten in das Kartenterminal gesteckt wird, die aktuelle Sitzung des Versicherten für diese Karte übernehmen.[<=]

### AdV-A\_2552 - Anzeige einer Aufforderung zum Kartenwechsel

Die AdV-App MUSS, falls der Anwendungsfall "Datenübertragung bei Kartentausch durchführen" umgesetzt wird, dem Versicherten eine Aufforderung zum Kartenwechsel anzeigen, wenn während der Ausführung des Anwendungsfalls Datenübertragung ein Kartentausch von der Quell- zur Ziel-Karte nötig ist.[<=]



**Abbildung 13: ABB\_ADV\_315 Standardablauf – Datenübertragung bei Kartentausch durchführen**

**AdV-A\_2553 - AdV-App: Datenübertragung bei Kartentausch durchführen**

Die AdV-App KANN den Anwendungsfall "Datenübertragung bei Kartentausch durchführen" gemäß TAB\_ADV\_324 umsetzen.

**Tabelle 28: TAB\_ADV\_324 – Datenübertragung bei Kartentausch durchführen**

Benennung des Anwendungsfalls	„Datenübertragung bei Kartentausch“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV005
Auslöser	Der Versicherte möchte Daten von seiner alten eGK auf seine neue eGK übertragen. Dazu wählt er eine Aktion in der AdV-App aus, die das Kopieren startet.
Akteure	Versicherter
Vorbedingung	<p>Siehe übergreifende Vorbedingungen und</p> <ul style="list-style-type: none"> <li>• Quell- und Zielkarte (eGK) sind für den selben Versicherten personalisiert</li> <li>• Die Zielkarte ist neuer als die Quellkarte.</li> <li>• eGK Zielkarte: X.509 (Karteninhaberzertifikat) ist mathematisch und zeitlich gültig</li> <li>• eGK Zielkarte: X.509 (Karteninhaberzertifikat) ist Online gültig oder Onlinestatus unbekannt</li> <li>• Auf der Zielkarte sind die ausgewählten Datenbereiche leer (falls ein Datenbereich gefüllt ist, liefert putData einen Fehler).</li> </ul>
Nachbedingung	<ul style="list-style-type: none"> <li>• Anwendungsdaten auf neue eGK übertragen.</li> <li>• In EF.Logging der Zielkarte befindet sich je bearbeiteter Anwendung ein neuer Eintrag, der dokumentiert, dass die Daten dieser Anwendung aus der Übernahme von einer anderen eGK des Versicherten stammen.</li> <li>• Auf der Quellkarte sind die bearbeiteten Anwendungen verborgen</li> <li>• Auf der Zielkarte haben die erfolgreich bearbeiteten Anwendungen den Status (verborgen/sichtbar) der Quellkarte. Tritt ein Fehler beim Schreiben auf die Zielkarte auf, wird der Ausgangsstatus der betroffenen Anwendung auf der Zielkarte wiederhergestellt.</li> </ul>

Standardablauf	<p>Die Umsetzung ist in der Tabelle TAB_ADV_325 – Ablaufaktivitäten – Datenübertragung bei Kartentausch durchführen beschrieben.</p> <ol style="list-style-type: none"> <li>1. Liste der zu kopierenden Anwendungen abfragen</li> <li>2. Prüfdaten speichern</li> <li>3. Daten der Quell-eGK lesen</li> <li>4. Kartenwechsel</li> <li>5. AdV-Sitzung initialisieren</li> <li>6. Prüfdaten abgleichen</li> <li>7. Daten auf Ziel-eGK schreiben</li> <li>8. Abschluss der Kopieroperation</li> <li>9. AdV-Statusmeldung anzeigen</li> </ol>
Diagramm	ABB_ADV_315 Standardablauf – Datenübertragung bei Kartentausch durchführen

**Tabelle 29: TAB\_ADV\_325 – Ablaufaktivitäten – Datenübertragung bei Kartentausch durchführen**

<b>1. Liste der zu kopierenden Anwendungen abfragen</b>	
Anzeige einer Auswahlliste	Dem Versicherten ist eine Liste der auf der eGK vorhandenen und in der KTR-AdV zugreifbaren - medizinischen Anwendungen anzuzeigen. Durch Markieren der zu kopierenden Anwendungen wählt der Versicherte diejenigen aus, deren Daten von einer alten auf eine neue eGK kopiert werden sollen.
<b>2. Prüfdaten speichern</b>	
Daten der Quell-eGK in der AdV-App speichern	<ul style="list-style-type: none"> <li>• ICCSN der Karte</li> <li>• KVNR (Unveränderbarer Teil) des Versicherten</li> <li>• Gültigkeitsdatum des AUT-Zertifikats</li> <li>• Version des Objektsystems der eGK</li> </ul>
<i>Beschreibung</i>	Die Daten der Quell-eGK werden für die spätere Prüfung der Ziel-eGK zwischengespeichert.
<b>3. Daten der Quell-eGK lesen</b>	
<i>Eingangsdaten</i>	



n*[Application]	Liste der Bezeichner der zu kopierenden Fachanwendungen Zulässige Bezeichner sind: DF . DPE
Beschreibung	<p>Schleife über alle in den Eingangsparametern angegebenen Anwendungen:</p> <pre>{   1. Anwendungsstatus speichern und danach ggf. die   Anwendung sichtbar machen durch Aufruf von   Anwendungsfall „Anwendung auf eGK reaktivieren“ mit   dem <i>Identifikator</i> = Bezeichner der Anwendung   2. getData(     objsysVersion,     application   );   3. Daten der Anwendung im Arbeitsspeicher der AdV-App   ablegen   4. Falls die Anwendungsdaten fehlerfrei gelesen und   abgelegt wurden: Anwendung deaktivieren   Aufruf von Plattformbaustein   PL_TUC_CARD_DEACTIVATE_APPLICATION mit dem   Parameter <i>Identifikator</i> = Bezeichner der Anwendung   5. Falls ein Aufruf mit einem Fehler beendet wird (z.B. weil   keine Daten auf der Quell-eGK vorhanden sind), so wird der   Fehler, den AdV vom aufgerufenen Fachmodul erhalten hat,   in verständlicher Form in die im letzten Schritt anzuzeigende   AdV-Statusmeldung eingefügt.   Für dieses Element wird putData zum Schreiben der   Daten auf die Ziel-eGK nicht aufgerufen. Wenn für alle zu   kopierenden Elemente ein Fehler vom Fachmodul gemeldet   wurde, wird der Anwendungsfall mit Punkt 9 Abschluss der   Kopieroperation fortgesetzt. }</pre>
<b>4. Kartenwechsel</b>	
Beschreibung	<ul style="list-style-type: none"> <li>• Quellkarte auswerfen: Der Versicherte wird zum Ziehen der Quellkarte aufgefordert.</li> <li>• Wenn nach einem Timeout von 2 Minuten die Quellkarte nicht gezogen wurde, dann wird mit Punkt 9 Abschluss der Kopieroperation fortgesetzt.</li> <li>• Neue eGK anfordern: Der Versicherte wird zum Stecken seiner neuen eGK aufgefordert.</li> </ul>
<b>5. AdV-Sitzung initialisieren</b>	
Beschreibung	<p>Wenn neue Karte gesteckt wurde, dann werden alle Schritte zum Initialisieren der neuen Kartensitzung gemäß AdV-A_2445 – ohne Verlassen des aktuellen Anwendungsfalls - durchgeführt.</p> <p>Wenn nach einem Timeout von 2 Minuten keine neue Karte gesteckt wurde, dann wird die Operation mit Punkt 9 Abschluss der Kopieroperation fortgesetzt.</p>
<b>6. Prüfdaten abgleichen</b>	

<b>Beschreibung</b>	<p>Prüfdaten der neuen eGK mit denen der alten eGK vergleichen:</p> <ul style="list-style-type: none"> <li>• Wenn <math>ICCSN_{alt} = ICCSN_{neu}</math>, dann Abbruch der Operation mit der Fehlermeldung "Sie haben zweimal die selbe Karte verwendet, bitte wiederholen Sie den Vorgang mit der alten und der neuen Gesundheitskarte."</li> <li>• Wenn <math>KVNR_{alt} \neq KVNR_{neu}</math> (Karteninhaber nicht identisch), dann Abbruch mit der Fehlermeldung "Die neue Gesundheitskarte ist für einen anderen Versicherten ausgestellt. Bitte wiederholen Sie den Vorgang mit Ihrer neuen Gesundheitskarte." Hinweis: Der unveränderbare Teil der KVNR wird verglichen.</li> <li>• Sei <i>validfrom</i> das Gültigkeitsbeginn-Datum des X.509-AUT-Zertifikats. Wenn <math>validfrom_{neu} &lt; validfrom_{alt}</math>, dann Abbruch mit der Fehlermeldung "Falsche Reihenfolge. Bitte wiederholen Sie den Vorgang mit Ihrer alten Gesundheitskarte und stecken Sie dann erst Ihre neue Gesundheitskarte."</li> </ul> <p>Prüfung der Gültigkeit des Karteninhaberzertifikat der eGK Zielkarte (Falls die eGK nicht den Gültigkeitskriterien entspricht wird mit der Fehlermeldung "Die Zielkarte ist nicht gültig, bitte wenden Sie sich an Ihre Krankenkasse." abgebrochen):</p> <ul style="list-style-type: none"> <li>• eGK Zielkarte: X.509 (Karteninhaberzertifikat) ist mathematisch und zeitlich gültig (PL_TUC_EGK_STATUS # Mathematische Gültigkeit &amp; Gültigkeit zu Referenzzeitpunkt)</li> <li>• eGK Zielkarte: X.509 (Karteninhaberzertifikat) ist Online gültig oder Onlinestatus unbekannt (PL_TUC_EGK_STATUS # OCSP-Prüfung)</li> </ul> <p>Bei Abbruch: gespeicherte Daten der Quellkarte verwerfen und eGK Sitzung beenden, falls der Karteninhaber nicht identisch ist.</p>
<b>7. Daten auf Ziel-eGK schreiben</b>	
<b>Beschreibung</b>	<p>Schleife über alle Anwendungen, für die getData() Anwendungsdaten geliefert hat:</p> <pre> {   1. Anwendungstatus der Ziel-eGK speichern und danach ggf. die Anwendung sichtbar machen     durch Aufruf von Anwendungsfall „6.1.4.2 Anwendung auf eGK reaktivieren“ mit dem       <i>Identifikator</i> = Bezeichner der Anwendung   2. putData(     objsysVersionSrc,     objsysVersionDest,     application,     applicationData   );   3. Falls ein Aufruf mit einem Fehler beendet wird (z.B. weil auf der Ziel-eGK schon Daten vorhanden waren), so wird der Fehler, den AdV vom aufgerufenen Fachmodul erhalten hat, in verständlicher Form in die im letzten Schritt </pre>

	anzuzeigende AdV-Statusmeldung eingefügt. Im Fehlerfall wird der Anwendungstatus der Ziel-eGK wieder hergestellt: Falls auf der Ziel-eGK die Anwendung verborgen war, wird sie wieder verborgen durch Aufruf von Plattformbaustein PL_TUC_CARD_DEACTIVATE_APPLICATION mit dem Parameter <i>Identifikator</i> = Bezeichner der Anwendung 4. Wenn die Anwendung auf der Quellkarte verborgen gewesen war und erfolgreich kopiert wurde, diese gemäß appStatus durch Aufruf des Anwendungsfalls in „Anwendung auf eGK deaktivieren“ mit dem Parameter <i>Identifikator</i> = Bezeichner der Anwendung wieder verbergen. }
<b>8. Abschluss der Kopieroperation</b>	
	<ul style="list-style-type: none"> <li>• Alle zwischengespeicherten Anwendungsdaten aus dem Arbeitsspeicher entfernen</li> </ul>
<b>9. AdV-Statusmeldung anzeigen</b>	
<i>Hinweis an den Versicherten</i>	Die AppResult-Elemente enthalten Informationen über das erfolgreiche Kopieren der Datensätze von einer eGK auf eine andere eGK des Versicherten. Im Fehlerfall werden entsprechende Fehlerinformationen ausgegeben. Dem Versicherten ist das Ergebnis des Kopiervorgangs für jede ausgewählte Fachanwendung - in einer für ihn verständlichen Form - anzuzeigen.

[&lt;=]

### 6.1.6 Verwaltung der NFD

In diesem Abschnitt sind die Anwendungsfälle für die Verwaltung des Notfalldatensatzes (NFD) beschrieben. Ein Zugriff auf medizinische Daten ist nicht möglich.

#### AdV-A\_2468 - AdV-App: Hinweis bei verborgenem Notfalldatensatz

Die AdV-App MUSS, wenn die Anwendung NFD auf der eGK des Versicherten verborgen ist, einen Hinweis an den Versicherten ausgeben, dass der Notfalldatensatz verborgen ist und im Notfall nicht gelesen werden kann.[<=]

#### 6.1.6.1 NFD auf eGK verbergen

Mit der Umsetzung dieses Anwendungsfalls soll der Notfalldatensatz des Versicherten auf seiner eGK verborgen werden.

#### AdV-A\_2469 - AdV-App: NFD auf eGK verbergen

Die AdV-App MUSS den Anwendungsfall „NFD auf eGK verbergen“ gemäß TAB\_ADV\_355 umsetzen.

**Tabelle 30: TAB\_ADV\_355 – NFD auf eGK verbergen**

Benennung des Anwendungsfalls	„Notfalldaten verbergen“
-------------------------------	--------------------------

Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV008
Auslöser	Der Versicherte möchte den auf seiner eGK gespeicherten Notfalldatensatz verbergen. Dazu wählt er eine Aktion in der AdV-App aus, die das Verbergen des Notfalldatensatzes auf der eGK startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen. Notfalldatensatz ist auf der eGK sichtbar.
Nachbedingung	Notfalldatensatz ist auf der eGK verborgen.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls AdV-UC_14 „Anwendung auf eGK deaktivieren“ mit dem Parameter <code>Identifikator = DF.NFD</code>

[&lt;=]

#### 6.1.6.2 Verborgenen NFD auf eGK sichtbar machen

Mit der Umsetzung dieses Anwendungsfalls soll der verborgene Notfalldatensatz des Versicherten auf seiner eGK sichtbar gemacht werden.

##### AdV-A\_2470 - AdV-App: Verborgene NFD auf eGK sichtbar machen

Die AdV-App MUSS den Anwendungsfall „Verborgene NFD auf eGK sichtbar machen“ gemäß TAB\_ADV\_356 umsetzen.

**Tabelle 31 TAB\_ADV\_356 – Verborgene NFD auf eGK sichtbar machen**

Benennung des Anwendungsfalls	„Verborgene Notfalldaten wieder anzeigen“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV009
Auslöser	Der Versicherte möchte den auf seiner eGK gespeicherten, verborgenen Notfalldatensatz sichtbar machen. Dazu wählt er eine Aktion in der AdV-App aus, die die Sichtbarkeit des Notfalldatensatzes auf der eGK aktiviert.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen. Notfalldatensatz ist auf der eGK verborgen.
Nachbedingung	Notfalldatensatz ist auf der eGK sichtbar.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls AdV-UC_15 „Anwendung auf eGK reaktivieren“ mit dem Parameter <code>Identifikator = DF.NFD</code>

[&lt;=]

### 6.1.6.3 PIN für NFD einschalten

Mit diesem Anwendungsfall soll die technische Notwendigkeit der Verifikation der MRPIN.NFD eingeschaltet werden.

#### AdV-A\_2471 - AdV-App: PIN für NFD einschalten

Die AdV-App MUSS den Anwendungsfall „PIN für NFD einschalten“ gemäß TAB\_ADV\_357 umsetzen.

**Tabelle 32: TAB\_ADV\_357 – PIN für NFD einschalten**

Benennung des Anwendungsfalls	„PIN-Schutz für Notfalldaten einschalten“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV010
Auslöser	Der Versicherte möchte MRPIN.NFD einschalten. Dazu wählt er eine Aktion in der AdV-App aus, die das Einschalten startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen. Die MRPIN.NFD auf der eGK ist ausgeschaltet.
Nachbedingung	Die MRPIN.NFD auf der eGK ist eingeschaltet.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls AdV-UC_03 „PIN für Fachanwendung einschalten“ mit dem Parameter Identifikator = MRPIN.NFD

[&lt;=]

### 6.1.6.4 PIN für NFD ausschalten

Mit diesem Anwendungsfall soll die technische Notwendigkeit der Verifikation der MRPIN.NFD ausgeschaltet werden.

#### AdV-A\_2472 - AdV-App: PIN für NFD ausschalten

Die AdV-App MUSS den Anwendungsfall „PIN für NFD ausschalten“ gemäß TAB\_ADV\_358 umsetzen.

**Tabelle 33: TAB\_ADV\_358 – PIN für NFD ausschalten**

Benennung des Anwendungsfalls	„PIN-Schutz für Notfalldaten ausschalten“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV011
Auslöser	Der Versicherte möchte MRPIN.NFD ausschalten. Dazu wählt er eine Aktion in der AdV-App aus, die das

	Ausschalten startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen. Die MRPIN.NFD auf der eGK ist eingeschaltet.
Nachbedingung	Die MRPIN.NFD auf der eGK ist ausgeschaltet.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls AdV-UC_04 „PIN für Fachanwendung ausschalten“ mit dem Parameter Identifikator = MRPIN.NFD

[&lt;=]

### 6.1.7 Verwaltung des DPE

In diesem Abschnitt sind die Anwendungsfälle für die Verwaltung der Anwendung Datensatz ‚Persönliche Erklärungen‘ (DPE) beschrieben.

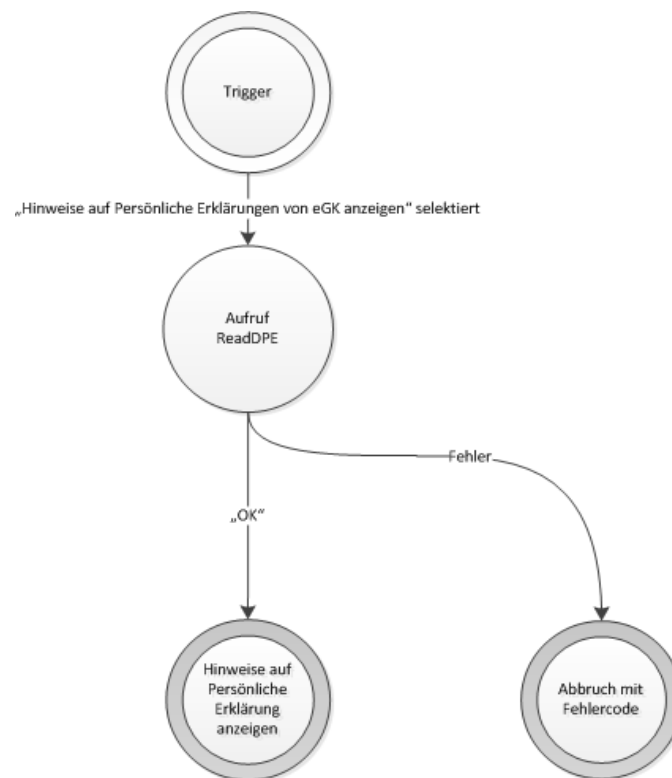
#### AdV-A\_2473 - AdV-App: Hinweis bei verborgenem DPE

Die AdV-App MUSS beim Aufruf des Bereiches mit den Anwendungsfälle zur Anwendung DPE, wenn der DPE auf der eGK des Versicherten verborgen ist, einen Hinweis an den Versicherten ausgeben, dass die Anwendung verborgen ist und die Daten im Notfall nicht gelesen werden können.[<=]

#### 6.1.7.1 Persönliche Erklärung (DPE) von eGK anzeigen

Mit der Umsetzung dieses Anwendungsfalls soll dem Versicherten der auf seiner eGK gespeicherte Datensatz Persönliche Erklärungen (DPE) zur Anzeige gebracht werden.

Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall AdV-UC\_121: „DPE von eGK anzeigen“ ausgeführt werden müssen.



**Abbildung 14: ABB\_ADV\_359 – Ablauf des AdV-UC\_121: „DPE von eGK anzeigen“**

#### **AdV-A\_2474 - AdV-App: DPE von eGK anzeigen**

Die AdV-App MUSS den Anwendungsfall „DPE von eGK anzeigen“ gemäß TAB\_ADV\_359 umsetzen.

**Tabelle 34: TAB\_ADV\_359 – DPE von eGK anzeigen**

Benennung des Anwendungsfalls	„Hinweise auf Persönliche Erklärungen von eGK anzeigen“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV012
Auslöser	Der Versicherte möchte die auf seiner eGK gespeicherten Hinweise auf Persönliche Erklärungen (DPE) einsehen. Dazu wählt er eine Aktion in der AdV-App aus, die das Auslesen startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	Datensatz Persönliche Erklärungen (DPE) wird in der AdV-App angezeigt.

Standardablauf	Die Umsetzung ist in der Tabelle 35: TAB_ADV_360 – Ablaufaktivitäten – DPE von eGK anzeigen beschrieben. <ol style="list-style-type: none"> <li>1. DPE-LeseRequest erzeugen</li> <li>2. DPE-LeseResponse verarbeiten</li> <li>3. DPE anzeigen</li> </ol>
Diagramm	Abbildung ABB_ADV_359 – Ablauf des Adv-UC_121: „DPE von eGK anzeigen“

Tabelle 35: TAB\_ADV\_360 – Ablaufaktivitäten – DPE von eGK anzeigen

<b>1. DPE-LeseRequest erzeugen</b>	
Operation	ReadDPE
Eingangsdaten	
(keine)	
<b>2. DPE-LeseResponse verarbeiten</b>	
Rückgabedaten	
ReadDPEResponse	Beinhaltet den Datensatz Persönliche Erklärungen (DPE).
Beschreibung	Das Lesen des DPE basiert auf der Operation ReadDPE. Diese liefert ein <code>DPEDocument</code> zurück. Das <code>DPEDocument</code> entspricht dem von der eGK des Versicherten gelesenen, dekomprimierten und validierten DPE. Die Operation ReadDPE liefert im Erfolgsfall die angefragten Daten zurück. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben.
<b>3. DPE anzeigen</b>	
	Der von der eGK des Versicherten gelesene DPE soll dem Versicherten zur Anzeige gebracht werden. Dazu sollen sämtliche Inhalte in einer übersichtlichen und dem Versicherten verständlichen Darstellung angezeigt werden.

[&lt;=]

### 6.1.7.2 Persönliche Erklärung (DPE) auf eGK ändern

Mit der Umsetzung dieses Anwendungsfalls ändert der Versicherte eine oder mehrere Hinweise auf persönliche Erklärungen des auf der eGK gespeicherten Datensatzes Persönliche Erklärungen (DPE). Dem Ändern eines oder mehrerer Erklärungen muss ein



Lesen der DPE vorausgehen, da der DPE nur im Ganzen auf die Karte geschrieben werden kann.

Wenn noch kein DPE auf der eGK gespeichert ist, dann kann der Versicherte einen DPE anlegen.

Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall AdV-UC\_122: „DPE auf eGK ändern“ ausgeführt werden müssen.

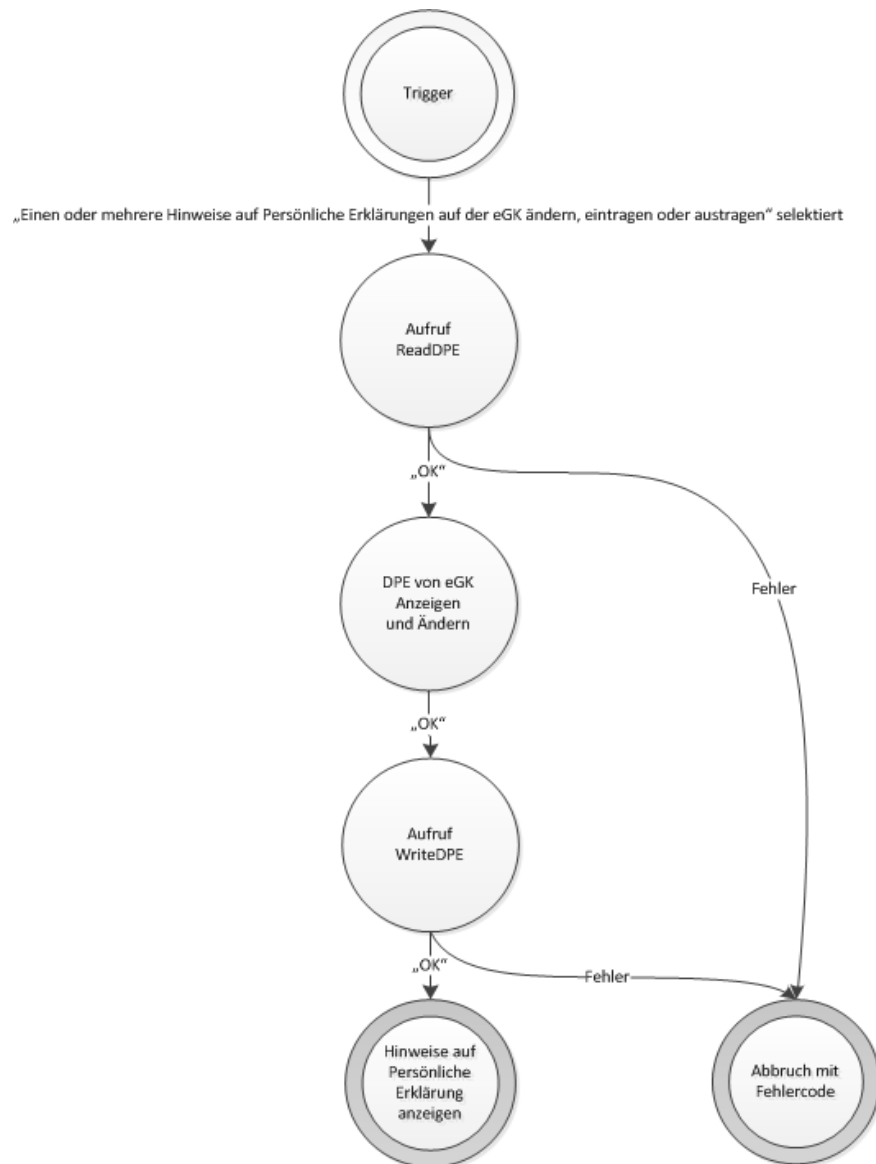


Abbildung 15: ABB\_ADV\_361 – Ablauf des AdV-UC\_122: „DPE auf eGK ändern“

#### AdV-A\_2475 - AdV-App: Persönliche Erklärung (DPE) auf eGK ändern

Die AdV-App MUSS den Anwendungsfall „Persönliche Erklärung (DPE) auf eGK ändern“ gemäß TAB\_ADV\_361 umsetzen.

**Tabelle 36: TAB\_ADV\_361 – DPE auf eGK ändern**

Benennung des Anwendungsfalls	„Hinweise auf Persönliche Erklärungen bearbeiten“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV013
Auslöser	Der Versicherte möchte eine oder mehrere Hinweise auf Persönliche Erklärungen im DPE auf seiner eGK ändern. Dazu wählt er eine Aktion in der AdV-App aus, die das Editieren der Hinweise auf Persönlichen Erklärungen am Terminal startet. Nach Eingabe aller gewünschten Änderungen bestätigt der Versicherte seine Eingaben, woraufhin die Daten auf die eGK des Versicherten geschrieben werden.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	Aktueller DPE auf der eGK wurde geschrieben.
Standardablauf	<p>Die Umsetzung ist in der Tabelle „TAB_ADV_362 – Ablaufaktivitäten – DPE auf eGK ändern“ beschrieben.</p> <ol style="list-style-type: none"> <li>1. DPE von eGK lesen und anzeigen</li> <li>2. Eintrag im DPE editieren</li> <li>3. DPE-SchreibRequest erzeugen</li> <li>4. PE-SchreibResponse verarbeiten</li> <li>5. Änderungsbestätigung und geänderte DPE anzeigen</li> </ol>
Diagramm	Abbildung ABB_ADV_361 – Ablauf des AdV-UC_122: „DPE auf eGK ändern“

**Tabelle 37: TAB\_ADV\_362 – Ablaufaktivitäten – DPE auf eGK ändern**

<b>1. DPE von eGK lesen und anzeigen</b>	
Hinweis zur Umsetzung	Das Lesen der DPE soll gemäß Tabelle "TAB_ADV_359 – DPE von eGK anzeigen" erfolgen.
<b>2. Persönliche Erklärung in DPE editieren</b>	
	Die AdV-App soll es dem Versicherten ermöglichen, einzelne Hinweise auf Persönliche Erklärungen des DPE zu ändern. Dabei sollen die übrigen Hinweise von der

	<p>Änderung nicht beeinflusst werden, d.h. das Ändern eines Elementes führt NICHT zum Ändern eines anderen Elementes. Editierbar sind die folgenden Elemente  DPE_Gewebe_Organspendeerklärung,  DPE_Vorsorgevollmacht und  DPE_Patientenverfügung des DPE-Dokuments. Editieren bedeutet im Zusammenhang mit dem vorliegenden Anwendungsfall auch das Anlegen eines der vorgenannten Elemente, sofern es im aktuellen Datensatz noch nicht vorhanden ist sowie das Löschen eines der genannten Elemente, sofern es im aktuellen Datensatz bereits vorhanden ist und diese Aktion vom Versicherten ausgelöst wurde.</p> <p>Die AdV-App muss die Eingaben des Versicherten gegen das Schema <code>DPE_Document.xsd</code> validieren. Der Versicherte muss auf invalide Daten hingewiesen werden. Es dürfen keine invaliden Daten akzeptiert und auf die eGK geschrieben werden.</p> <p>Zum Abschluss des Bearbeitens einer einzelnen persönlichen Erklärung soll der Versicherte seine Eingaben bestätigen.</p>
<b>3. DPE-SchreibRequest erzeugen</b>	
Operation	WriteDPE
<i>Eingangsdaten</i>	
DPEDocument	Auf die eGK des Versicherten zu schreibender DPE
<i>Beschreibung</i>	Der aktualisierte DPE muss als XML-Dokument gemäß <code>DPE_Document.xsd</code> strukturiert und valide sein. Dieses muss dann der Operation WriteDPE übergeben werden.
<b>4. DPE-SchreibResponse verarbeiten</b>	
<i>Rückgabedaten</i>	
Keine (bzw. Fehlermeldung)	Im Erfolgsfall werden keine Daten von der Operation zurückgegeben. Im Fehlerfall wird eine Fehlermeldung zurückgegeben.
<i>Beschreibung</i>	Das Schreiben des DPE basiert auf der parametrisierten Operation WriteDPE. Diese liefert eine Statusmeldung der Schreiboperation zurück. Im Fehlerfall wird

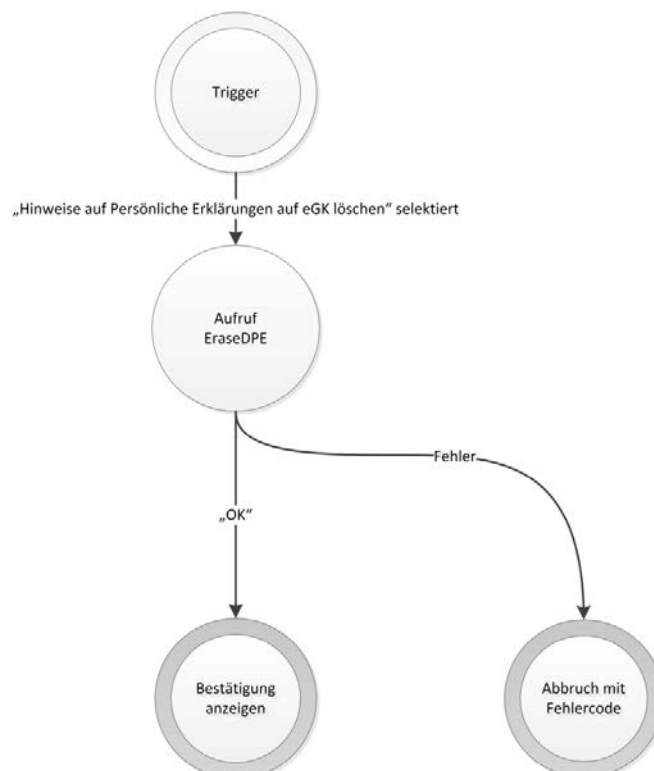
	eine Fehlermeldung mit entsprechenden Details der Fachanwendung <u>NFDM</u> zurückgegeben.
<b>5. DPE-Änderungsbestätigung anzeigen</b>	
<i>Hinweis an den Versicherten</i>	Der Status des DPE-Schreibresponse enthält Informationen über das erfolgreiche Schreiben des Datensatzes auf der eGK des Versicherten. Im Fehlerfall werden entsprechende Fehlerinformationen ausgegeben. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen.

[&lt;=]

### 6.1.7.3 Persönliche Erklärung (DPE) auf eGK löschen

Mit der Umsetzung dieses Anwendungsfalls löscht der Versicherte den gesamten Datensatz seiner persönlichen Erklärungen (DPE) auf der eGK.

Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall AdV-UC\_123: „DPE auf eGK löschen“ ausgeführt werden müssen.



**Abbildung 16: ABB\_ADV\_363 – Ablauf des AdV-UC\_123: „DPE auf eGK löschen“**

### AdV-A\_2476 - AdV-App: Persönliche Erklärung (DPE) auf eGK löschen

Die AdV-App MUSS den Anwendungsfall „Datensatz Persönliche Erklärung (DPE) auf eGK löschen“ gemäß TAB\_ADV\_363 umsetzen.

**Tabelle 38: TAB\_ADV\_363 – DPE auf eGK löschen**

Benennung des Anwendungsfalls	„Alle Hinweise auf Persönliche Erklärungen löschen“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV014
Auslöser	Der Versicherte möchte den Datensatz mit Hinweisen auf Persönlichen Erklärungen auf seiner eGK löschen. Dazu wählt er eine Aktion in der AdV-App aus, die den Anwendungsfall startet. Nach Bestätigung des Löschwunsches wird Datensatz DPE auf die eGK des Versicherten unwiederbringlich gelöscht.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	Der Datensatz der persönlichen Erklärungen im DPE ist auf der eGK nicht mehr vorhanden.
Standardablauf	<p>Die Umsetzung ist in der Tabelle TAB_ADV_364 – Ablaufaktivitäten – DPE auf eGK löschen beschrieben.</p> <ol style="list-style-type: none"> <li>1. Bestätigung des Löschwunsches vom Versicherten einholen</li> <li>2. DPE-LöschRequest erzeugen</li> <li>3. DPE-LöschResponse verarbeiten</li> <li>4. DPE Löschbestätigung anzeigen</li> </ol>
Diagramm	Abbildung ABB_ADV_363 – Ablauf des AdV-UC_123: „DPE auf eGK löschen“

**Tabelle 39: TAB\_ADV\_364 – Ablaufaktivitäten – DPE auf eGK löschen**

<b>1. Bestätigung des Löschwunsches vom Versicherten einholen</b>	
	Zum Starten der Löschaktion des Datensatzes der persönlichen Erklärungen soll der Versicherte seine Auswahl noch einmal bestätigen.
<b>2. DPE-LöschRequest erzeugen</b>	
Operation	EraseDPE
Eingangsdaten	

keine	Es wird der komplette DPE Datensatz gelöscht.
<b>3. DPE-LöschResponse verarbeiten</b>	
<i>Rückgabedaten</i>	
Keine (bzw. Fehlermeldung)	Im Erfolgsfall werden keine Daten von der Operation zurückgegeben. Im Fehlerfall wird eine Fehlermeldung zurückgegeben.
<i>Beschreibung</i>	Das Löschen des DPE basiert auf der parametrisierten Operation EraseDPE. Diese liefert im Fehlerfall eine Fehlermeldung mit entsprechenden Details der Fachanwendung <u>NFDM</u> zurück.
<b>4. DPE-Löschbestätigung anzeigen</b>	
<i>Hinweis an den Versicherten</i>	Der Status der DPE-LöschResponse enthält Informationen über das erfolgreiche Löschen des Datensatzes auf der eGK des Versicherten. Im Fehlerfall werden entsprechende Fehlerinformationen ausgegeben. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen.

[&lt;=]

#### 6.1.7.4 PIN für DPE einschalten

Mit diesem Anwendungsfall kann der Versicherte die technische Notwendigkeit der Verifikation der MRPIN.DPE einschalten.

##### Adv-A\_2477 - Adv-App: PIN für DPE einschalten

Die Adv-App MUSS den Anwendungsfall „PIN für DPE einschalten“ gemäß TAB\_ADV\_365 umsetzen.

**Tabelle 40: TAB\_ADV\_365 – PIN für DPE einschalten**

Benennung des Anwendungsfalls	„PIN-Schutz für Persönliche Erklärungen einschalten“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV017
Auslöser	Der Versicherte möchte MRPIN.DPE einschalten. Dazu wählt er eine Aktion in der Adv-App aus, die das Einschalten startet.
Akteure	Versicherter

Vorbedingung	Siehe übergreifende Vorbedingungen. Die MRPIN.DPE auf der eGK ist ausgeschaltet.
Nachbedingung	Die MRPIN.DPE auf der eGK ist eingeschaltet.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls AdV-UC_03 „PIN für Fachanwendung einschalten“ mit dem Parameter Identifikator = MRPIN.DPE

[&lt;=]

#### 6.1.7.5 PIN für DPE ausschalten

Mit diesem Anwendungsfall kann der Versicherte die technische Notwendigkeit der Verifikation der MRPIN.DPE ausgeschalten.

##### AdV-A\_2478 - AdV-App: PIN für DPE ausschalten

Die AdV-App MUSS den Anwendungsfall „PIN für DPE ausschalten“ gemäß TAB\_ADV\_366 umsetzen.

**Tabelle 41: TAB\_ADV\_366 – PIN für DPE ausschalten**

Benennung des Anwendungsfalls	„PIN-Schutz für Persönliche Erklärungen ausschalten“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV018
Auslöser	Der Versicherte möchte MRPIN.DPE ausschalten. Dazu wählt er eine Aktion in der AdV-App aus, die das Ausschalten startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen. Die MRPIN.DPE auf der eGK ist eingeschaltet.
Nachbedingung	Die MRPIN.DPE auf der eGK ist ausgeschaltet.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls AdV-UC_04 „PIN für Fachanwendung ausschalten“ mit dem Parameter Identifikator = MRPIN.DPE

[&lt;=]

#### 6.1.7.6 Persönliche Erklärung (DPE) auf eGK verbergen

Mit diesem Anwendungsfall kann der Versicherte den Datensatz Persönliche Erklärungen auf seiner eGK verbergen.

##### AdV-A\_2479 - AdV-App: Datensatz Persönliche Erklärungen (DPE) auf eGK verbergen

Die AdV-App MUSS den Anwendungsfall „Datensatz Persönliche Erklärungen (DPE) auf eGK verbergen“ gemäß TAB\_ADV\_367 umsetzen.

**Tabelle 42: TAB\_ADV\_367 – DPE auf eGK verbergen**

Benennung des Anwendungsfalls	„Hinweise auf Persönliche Erklärungen verbergen“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV015
Auslöser	Der Versicherte möchte die auf seiner eGK gespeicherten persönlichen Erklärungen verbergen. Dazu wählt er eine Aktion in der AdV-App aus, die das Verbergen des Datensatz Persönliche Erklärungen (DPE) auf der eGK startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	Persönliche Erklärungen sind auf der eGK verborgen.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls AdV-UC_14 „Anwendung auf eGK deaktivieren“ mit dem Parameter Identifikator = DF.DPE

[&lt;=]

**6.1.7.7 Verborgene DPE auf eGK sichtbar machen**

Mit diesem Anwendungsfall kann der Versicherte den verborgenen Datensatz Persönliche Erklärungen auf seiner eGK wieder sichtbar machen.

**AdV-A\_2480 - AdV-App: Verborgenen DPE auf eGK sichtbar machen**

Die AdV-App MUSS den Anwendungsfall „Verborgenen DPE auf eGK sichtbar machen“, gemäß TAB\_ADV\_368 umsetzen.

**Tabelle 43: TAB\_ADV\_368 – Verborgenen DPE auf eGK sichtbar machen**

Benennung des Anwendungsfalls	„Verborgene Hinweise auf Persönliche Erklärungen wieder anzeigen“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV016
Auslöser	Der Versicherte möchte den auf seiner eGK gespeicherten, verborgenen DPE sichtbar machen. Dazu wählt er eine Aktion in der AdV-App aus, die die Sichtbarkeit des DPE auf der eGK aktiviert.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	Datensatz Persönliche Erklärungen (DPE) ist auf der



	eGK wieder sichtbar.
Umsetzung	
1. DPE reaktivieren	Gemäß Beschreibung des Anwendungsfalls AdV-UC_15 „Anwendung auf eGK reaktivieren“ mit dem Identifikator = DF.DPE
2. DPE auslesen und anzeigen	<p>Ist das Sichtbarmachen des vorhandenen und verborgenen DPE erfolgreich, soll die AdV-App die Daten gemäß Anwendungsfall „Persönliche Erklärung (DPE) von eGK anzeigen“ auslesen und dem Versicherten anzeigen.</p> <p>Ist auf der eGK kein Datensatz Persönliche Erklärungen (DPE) vorhanden, so schlägt die Operation zum Sichtbarmachen der Anwendung fehl, ein entsprechender Fehlercode wird zurückgegeben. Im Fehlerfall ist der Versicherte über das Ergebnis der Operation zu informieren.</p>

[&lt;=]

### 6.1.8 Verwaltung eMP/AMTS

In diesem Abschnitt sind die Anwendungsfälle für die Verwaltung der Daten des elektronischen Medikationsplans und zur Prüfung der Arzneimitteltherapiesicherheit beschrieben. Ein Zugriff auf medizinische Daten ist nicht möglich.

#### 6.1.8.1 AMTS-Vertreter-PIN ändern

Mit der Umsetzung dieses Anwendungsfalls kann die AMTS-Vertreter-PIN auf der eGK gesetzt oder geändert werden.

Für die Umsetzung wird der in Kap. 6.1.4.3.1 PIN ändern beschriebene generische Anwendungsfall genutzt.

#### AdV-A\_2481 - AdV-App: AMTS-Vertreter-PIN ändern

Die AdV-App MUSS den Anwendungsfall „AMTS-Vertreter-PIN ändern“ gemäß TAB\_ADV\_369 umsetzen.

**Tabelle 44 TAB\_ADV\_369 – AMTS-Vertreter-PIN ändern**

Benennung des Anwendungsfalls	„Vertreter-PIN ändern“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV022
Auslöser	Der Versicherte möchte die PIN.AMTS_REP ändern. Dazu wählt er eine Aktion in der AdV-App aus, die das Ändern startet.

Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	Die PIN.AMTS_REP hat ein neues Geheimnis
Umsetzung	Gemäß Beschreibung des Anwendungsfalls AdV-UC_01: „PIN ändern“ mit dem Parameter Identifikator = PIN.AMTS_REP

[&lt;=]

### 6.1.8.2 AMTS-Vertreter-PIN entsperren

Mit diesem Anwendungsfall kann der Versicherte die gesperrten AMTS-Vertreter-PIN entsperren.

Für die Umsetzung wird der 6.1.4.3.2 PIN auf eGK entsperren beschriebene generische Anwendungsfall genutzt.

#### AdV-A\_2482 - AdV-App: AMTS-Vertreter-PIN entsperren

Die AdV-App MUSS den Anwendungsfall „AMTS-Vertreter-PIN entsperren“ gemäß TAB\_ADV\_370 umsetzen.

**Tabelle 45 TAB\_ADV\_370 – AMTS-Vertreter-PIN entsperren**

Benennung des Anwendungsfalls	„Vertreter-PIN entsperren“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV023
Auslöser	Der Versicherte möchte seine gesperrte PIN.AMTS_REP entsperren. Dazu wählt er eine Aktion in der AdV-App aus, die das Entsperren startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen. Die PIN.AMTS_REP auf der eGK ist gesperrt.
Nachbedingung	Die PIN.AMTS_REP auf der eGK ist entsperrt.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls AdV-UC_02: „PIN auf eGK entsperren“ mit dem Parameter Identifikator = PIN.AMTS_REP

[&lt;=]

### 6.1.8.3 eMP/AMTS Datensatz verbergen

Mit der Umsetzung dieses Anwendungsfalls soll der eMP/AMTS-Datensatz des Versicherten auf seiner eGK verborgen werden.

#### AdV-A\_2483 - AdV-App: eMP/AMTS-Datensatz verbergen

Die AdV-App MUSS den Anwendungsfall „eMP/AMTS-Datensatz auf eGK verbergen“ gemäß TAB\_ADV\_371 umsetzen.

**Tabelle 46: TAB\_ADV\_371 – eMP/AMTS-Datensatz auf eGK verbergen**

Benennung des Anwendungsfalls	„Medikationsplan verbergen“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV024
Auslöser	Der Versicherte möchte den auf seiner eGK gespeicherten eMP/AMTS-Datensatz verbergen. Dazu wählt er eine Aktion in der AdV-App aus, die die Sichtbarkeit des Datensatz auf der eGK deaktiviert.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen. eMP/AMTS ist auf der eGK sichtbar.
Nachbedingung	eMP/AMTS ist auf der eGK verborgen.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls AdV-UC_14 „Anwendung auf eGK deaktivieren“ mit dem Parameter Identifikator = DF.AMTS

[<=]

#### 6.1.8.4 Verborgenen eMP/AMTS Datensatz sichtbar machen

Mit der Umsetzung dieses Anwendungsfalls soll der verborgene eMP/AMTS-Datensatz des Versicherten auf seiner eGK sichtbar gemacht werden.

##### **AdV-A\_2484 - AdV-App: Verborgenen eMP/AMTS-Datensatz sichtbar machen**

Die AdV-App MUSS den Anwendungsfall „Verborgene eMP/AMTS-Datensatz auf eGK sichtbar machen“, gemäß TAB\_ADV\_372 umsetzen.

**Tabelle 47: TAB\_ADV\_372 – Verborgene eMP/AMTS-Datensatz auf eGK sichtbar machen**

Benennung des Anwendungsfalls	„Verborgenen Medikationsplan wieder anzeigen“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV025
Auslöser	Der Versicherte möchte den auf seiner eGK gespeicherten, verborgenen eMP/AMTS-Datensatz sichtbar machen. Dazu wählt er eine Aktion in der AdV-App aus, die die Sichtbarkeit des eMP/AMTS-Datensatzes auf der eGK aktiviert.
Akteure	Versicherter

Vorbedingung	Siehe übergreifende Vorbedingungen. eMP/AMTS ist auf der eGK verborgen.
Nachbedingung	eMP/AMTS-Datensatz ist auf der eGK wieder sichtbar.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls AdV-UC_15 „Anwendung auf eGK reaktivieren“ mit dem Parameter Identifikator = DF.AMTS

[&lt;=]

#### 6.1.8.5 PIN für AMTS einschalten

Mit diesem Anwendungsfall soll die technische Notwendigkeit der Verifikation der MRPIN.AMTS eingeschaltet werden.

##### AdV-A\_2485 - AdV-App: PIN für AMTS einschalten

Die AdV-App MUSS den Anwendungsfall „PIN für AMTS einschalten“ gemäß TAB\_ADV\_373 umsetzen.

**Tabelle 48: TAB\_ADV\_373 – PIN für AMTS einschalten**

Benennung des Anwendungsfalls	„PIN-Schutz für Medikationsplan einschalten“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV026
Auslöser	Der Versicherte möchte MRPIN.AMTS einschalten. Dazu wählt er eine Aktion aus, die das Einschalten startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen. Die MRPIN.AMTS auf der eGK ist ausgeschaltet (ab eGK G2.1)
Nachbedingung	Die MRPIN.AMTS auf der eGK ist eingeschaltet.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls AdV-UC_03 „PIN für Fachanwendung einschalten“ mit dem Parameter Identifikator = MRPIN.AMTS

[&lt;=]

#### 6.1.8.6 PIN für AMTS ausschalten

Mit diesem Anwendungsfall soll die technische Notwendigkeit der Verifikation der MRPIN.AMTS ausgeschaltet werden. Das Ausschalten der MRPIN.AMTS ist bei eGK ab der Generation G2.1 möglich.

##### AdV-A\_2486 - AdV-App: PIN für AMTS ausschalten

Die Adv-App MUSS den Anwendungsfall „PIN für AMTS ausschalten“ gemäß TAB\_ADV\_374 umsetzen.

**Tabelle 49: TAB\_ADV\_374 – PIN für AMTS ausschalten**

Benennung des Anwendungsfalls	„PIN-Schutz für Medikationsplan ausschalten“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV027
Auslöser	Der Versicherte möchte MRPIN.AMTS ausschalten. Dazu wählt er eine Aktion in der Adv-App aus, die das Ausschalten startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen. Die MRPIN.AMTS auf der eGK ist eingeschaltet. Die eGK zählt zur Generation G2.1 oder höher.
Nachbedingung	Die MRPIN.AMTS auf der eGK ist ausgeschaltet.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls Adv-UC_04 „PIN für Fachanwendung ausschalten“ mit dem Parameter Identifikator = MRPIN.AMTS

[<=]

### 6.1.9 Fachanwendungsunabhängige Anwendungsfälle

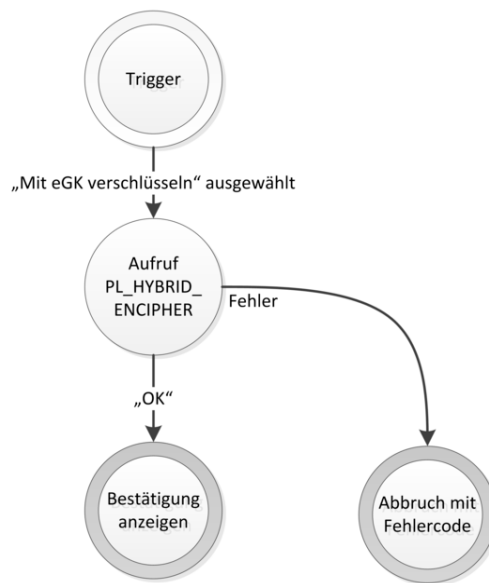
Dieses Kapitel beschreibt Anwendungsfälle, die keiner spezifischen Fachanwendung zugeordnet sind.

#### 6.1.9.1 Mit eGK verschlüsseln

Der Anwendungsfall ermöglicht es dem Versicherten, mit der Adv-App ein Dokument mit der eGK zu verschlüsseln.

Dieser Anwendungsfall zielt auf die @home-Umgebung, da der Versicherte dort auf einen Datenträger (z.B. USB-Stick oder lokale Festplatte) mit privaten Dokumenten zugreifen kann. In der @home-Umgebung kann in dem Anwendungsfall eine Datei auf einem lokalen Datenträger des Versicherten selektiert und der Ablageort für das Ergebnis definiert werden.

Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall Adv-UC\_25: „Mit eGK verschlüsseln“ ausgeführt werden müssen.



**Abbildung 17: ABB\_ADV\_322 – Ablauf des AdV-UC\_25: "Mit eGK verschlüsseln"**

**AdV-A\_2487 - AdV-App: AdV-UC\_25: „Mit eGK verschlüsseln“**

Die AdV-App KANN den Anwendungsfall AdV-UC\_25: „Mit eGK verschlüsseln“ gemäß TAB\_ADV\_375 umsetzen.

**Tabelle 50: TAB\_ADV\_375 – AdV-UC\_25: „Mit eGK verschlüsseln“**

Benennung des Anwendungsfalls	„Mit eGK verschlüsseln“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV030
Auslöser	Der Versicherte möchte ein Dokument mit dem öffentlichen Schlüssel seiner eGK verschlüsseln. Dazu wählt er eine Aktion in der AdV-App aus, die den Anwendungsfall startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	Als Rückgabewert wird das verschlüsselte Dokument zurückgegeben. (Das verschlüsselte Dokument ist zusammen mit dem verschlüsselten symmetrischen Schlüssel in dem zurückgegebenen CMS-Dokument enthalten)
Standardablauf	Die Umsetzung ist in der Tabelle TAB_ADV_376 – Ablaufaktivitäten – Mit eGK verschlüsseln beschrieben.

	<ol style="list-style-type: none"> <li>1. Eingangsdaten ermitteln</li> <li>2. PL_TUC_HYBRID_ENCIPHER aufrufen</li> <li>3. PL_TUC_HYBRID_ENCIPHER Ergebnis verarbeiten</li> <li>4. Ausgangsdaten zurückgeben und Ergebnis anzeigen</li> </ol>
Diagramm	Abbildung ABB_ADV_322 – Ablauf des AdV-UC_25: "Mit eGK verschlüsseln"

Tabelle 51: TAB\_ADV\_376 – Ablaufaktivitäten – Mit eGK verschlüsseln

<b>1. Eingangsdaten ermitteln</b>	
	Der Versicherte wählt das zu verschlüsselnde Dokument aus.
<b>2. PL_TUC_HYBRID_ENCIPHER aufrufen</b>	
Plattformbaustein	PL_TUC_HYBRID_ENCIPHER
<i>Eingangsdaten</i>	
Dokument	Vom Versicherten ausgewähltes Dokument.
Zertifikat	Zertifikat „C.CH.ENC“ gemäß PL_TUC_CARD_INFORMATION
<b>3. PL_TUC_HYBRID_ENCIPHER Ergebnis verarbeiten</b>	
<i>Rückgabedaten</i>	
OK + verschlüsseltes Dokument	Verschlüsselung erfolgreich. Das verschlüsselte Dokument wird zurückgegeben.
Fehler	Siehe Beschreibung PL_TUC_HYBRID_ENCIPHER und „TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine“ für die Behandlung in der AdV-App.
<i>Beschreibung</i>	Im Erfolgsfall wird das verschlüsselte Dokument zurückgegeben. Das symmetrisch verschlüsselte Dokument ist zusammen mit dem verschlüsselten symmetrischen Schlüssel in dem zurückgegebenen CMS-Dokument enthalten. Zum Verschlüsseln des symmetrischen Schlüssels wurde der öffentliche

	„C.CH.ENC“ Schlüssel genutzt.  Im Fehlerfall wird im Folgeschritt der Versicherte informiert.
<b>4. Ausgangsdaten zurückgeben und Ergebnis anzeigen</b>	
<i>Hinweis an den Versicherten</i>	Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige gebracht und das verschlüsselte Dokument zurückgegeben.  Im Fehlerfall werden dem Versicherten entsprechende Fehlerinformationen ausgegeben.

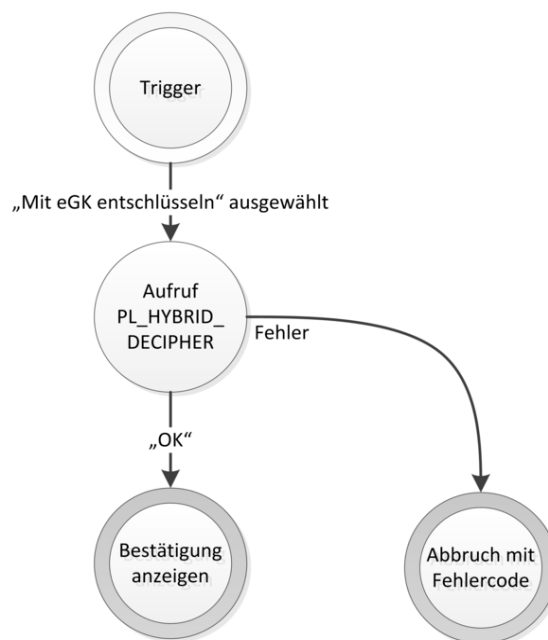
[&lt;=]

#### 6.1.9.2 Mit eGK entschlüsseln

Der Anwendungsfall ermöglicht es dem Versicherten, mit der AdV-App ein Dokument mit der eGK zu entschlüsseln.

Analog zum Anwendungsfall „Mit eGK verschlüsseln“ zielt dieser Anwendungsfall auf die @home-Umgebung, da der Versicherte dort auf seine privaten Dokumente zugreifen kann.

Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall AdV-UC\_26: „Mit eGK entschlüsseln“ ausgeführt werden müssen.



**Abbildung 18: ABB\_ADV\_324 – Ablauf des AdV-UC\_26: „Mit eGK entschlüsseln“**



**AdV-A\_2488 - AdV-App: AdV-UC\_26: „Mit eGK entschlüsseln“**

Die AdV-App KANN den Anwendungsfall AdV-UC\_26: „Mit eGK entschlüsseln“ gemäß TAB\_ADV\_377 umsetzen.

**Tabelle 52: TAB\_ADV\_377 – AdV-UC\_26: „Mit eGK entschlüsseln“**

Benennung des Anwendungsfalls	„Mit eGK entschlüsseln“
Hinweistext für den Versicherten	Anhang A6#TAB_ADV_473#ADV031
Auslöser	Der Versicherte möchte ein Dokument mit seiner eGK entschlüsseln. Dazu wählt er eine Aktion in der AdV-App aus, die den Anwendungsfall startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	Als Rückgabewert wird das entschlüsselte Dokument zurückgegeben.
Standardablauf	<p>Die Umsetzung ist in der Tabelle TAB_ADV_378 – Ablaufaktivitäten – Mit eGK entschlüsseln beschrieben.</p> <ol style="list-style-type: none"> <li>1. Eingangsdaten ermitteln</li> <li>2. PL_TUC_HYBRID_DECIPHER aufrufen</li> <li>3. PL_TUC_HYBRID_DECIPHER Ergebnis verarbeiten</li> <li>4. Ausgangsdaten zurückgeben und Ergebnis anzeigen</li> </ol>
Diagramm	Abbildung ABB_ADV_324 – Ablauf des AdV-UC_26: „Mit eGK entschlüsseln“

**Tabelle 53: TAB\_ADV\_378 – Ablaufaktivitäten – Mit eGK entschlüsseln**

<b>1. Eingangsdaten ermitteln</b>	
	Der Versicherte wählt das – mit seiner eGK - zu entschlüsselnde Dokument aus.
<b>2. PL_TUC_HYBRID_DECIPHER aufrufen</b>	
Plattformbaustein	PL_TUC_HYBRID_DECIPHER

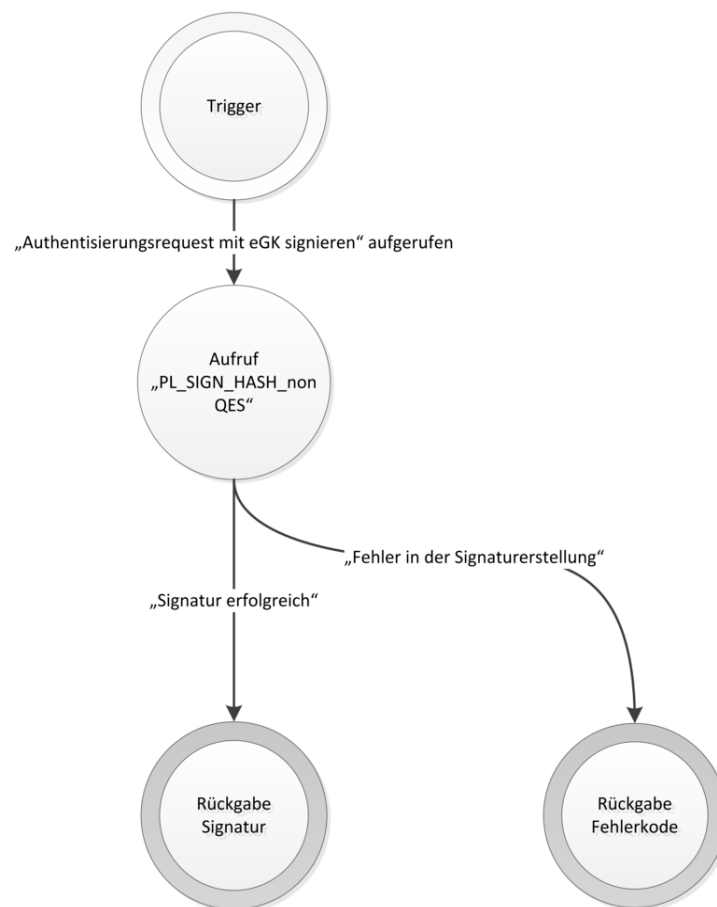
<i>Eingangsdaten</i>	
Dokument	Vom Versicherten ausgewähltes Dokument.
<b>3. PL_TUC_HYBRID_DECIPHER Ergebnis verarbeiten</b>	
<i>Rückgabedaten</i>	
OK + entschlüsseltes Dokument	Entschlüsselung erfolgreich. Das entschlüsselte Dokument wird zurückgegeben.
Fehler	Siehe Beschreibung PL_TUC_HYBRID_DECIPHER und „TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine“ für die Behandlung in der AdV-App.
<i>Beschreibung</i>	Im Erfolgsfall wird das entschlüsselte Dokument zurückgegeben. Im Fehlerfall wird im Folgeschritt der Versicherte informiert.
<b>4. Ausgangsdaten zurückgeben und Ergebnis anzeigen</b>	
<i>Hinweis an den Versicherten</i>	Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige gebracht und das entschlüsselte Dokument zurückgegeben. Im Fehlerfall werden dem Versicherten entsprechende Fehlerinformationen ausgegeben.

[&lt;=]

### 6.1.9.3 Authentisierungsrequest mit eGK signieren

Die Operation versieht unter Verwendung des AUT-Zertifikates der eGK eine Message (Binärstring/Hashwert) mit einer nicht-qualifizierten elektronischen Signatur. Die Operation verhält sich konform zu [TR-03112-4#3.5.5] (Crypto Services/Sign).

Die folgende Abbildung zeigt informativ, welche Schritte für Operation „Authentisierungsrequest mit eGK signieren“ ausgeführt werden müssen.



**Abbildung 19: ABB\_ADV\_379 – Ablauf des AdV-UC\_27 „Authentisierungsrequest mit eGK signieren“**

**AdV-A\_2489 - AdV-App: AdV-UC\_27: „Authentisierungsrequest mit eGK signieren“**

Die AdV-App KANN den Anwendungsfall AdV-UC\_27: „Authentisierungsrequest mit eGK signieren“ gemäß TAB\_ADV\_379 umsetzen.

**Tabelle 54: TAB\_ADV\_379 – Authentisierungsrequest mit eGK signieren**

Benennung des Anwendungsfalls	„Authentisierungsrequest mit eGK signieren“
Hinweistext für den Versicherten	-
Auslöser	Der Anwendungsfall wird ausgelöst, wenn der Versicherte sich mit seiner eGK authentisieren will (z.B. bei einem Fachdienst). Dieser Anwendungsfall wird nicht direkt vom Versicherten aufgerufen, sondern in Rahmen eines übergeordneten Anwendungsfalls (z.B. vom AdV-Terminal), welcher die benötigten Eingangsdaten bereitstellt.
Akteure	Versicherter

Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	Als Rückgabewert wird die erstellte Hashsignatur zurückgegeben.
Standardablauf	<p>Die Umsetzung ist in der Tabelle TAB_ADV_380 – Ablaufaktivitäten – Authentisierungsrequest mit eGK signieren beschrieben.</p> <ol style="list-style-type: none"> <li>1. PL_TUC_SIGN_HASH_nonQES aufrufen</li> <li>2. PL_TUC_SIGN_HASH_nonQES Ergebnis verarbeiten</li> <li>3. Ausgangsdaten zurückgeben</li> </ol>
Diagramm	Abbildung ABB_ADV_379 – Ablauf des AdV-UC_27 „Authentisierungsrequest mit eGK signieren“

**Tabelle 55: TAB\_ADV\_380 – Ablaufaktivitäten – Authentisierungsrequest mit eGK signieren**

<b>1. PL_TUC_SIGN_HASH_nonQES aufrufen</b>	
Plattformbaustein	PL_TUC_SIGN_HASH_nonQES
<i>Eingangsdaten</i>	
Hashwert	Der zu signierende Hash-Wert.
Identifikator	Der Identifikator des privaten Schlüssels (PrK.CH.AUT oder PrK.CH.AUTN) des in PL_TUC_CARD_INFORMATION gespeicherten AUT/AUTN-Zertifikats gemäß [gemSpec_CardProxy#Konfigurationstabelle CardProxy] und dem gewählten kryptografischen Verfahren R2048 bzw. E256
Signaturverfahren	Das Signaturverfahren (RSASSA-PKCS1-v1_5 oder ECDSA für TLS-Authentisierung, RSASSA-PSS für SAML).
<b>2. PL_TUC_SIGN_HASH_nonQES Ergebnis verarbeiten</b>	
<i>Rückgabedaten</i>	
OK + Hashsignatur	Signatur erfolgreich. Die Hashsignatur wird zurückgegeben.
Fehler	Siehe Beschreibung PL_TUC_SIGN_HASH_nonQES und „TAB_ADV_318 – Behandlung von Fehlercodes

	der Plattformbausteine“ für die Behandlung in der AdV-App.
<i>Beschreibung</i>	Im Erfolgsfall wird die erstellte Hashsignatur zurückgegeben. Im Fehlerfall wird im Folgeschritt der Fehlercode an den aufrufenden Anwendungsfall zurückgegeben.
<b>3. Ausgangsdaten zurückgeben</b>	
<i>Beschreibung</i>	Im Erfolgsfall wird die erstellte Hashsignatur an den aufrufenden Anwendungsfall zurückgegeben. Im Fehlerfall wird ein entsprechender Fehlercode an den aufrufenden Anwendungsfall zurückgegeben.

[&lt;=]

#### 6.1.9.4 Zertifikat von eGK lesen

Anwendungsfall AdV-UC\_24: Zertifikat von eGK lesen wird ausgelöst, wenn ein externes Programm oder Clientsystem von der eGK des Versicherten ein Zertifikat lesen will.

Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall AdV-UC\_24: Zertifikat von eGK lesen ausgeführt werden müssen.



Abbildung 20: ABB\_ADV\_381 – Ablauf AdV-UC\_24: Zertifikat von eGK lesen

**AdV-A\_2490 - AdV-App: AdV-UC\_24: Zertifikat von eGK lesen**

Die AdV-App KANN den Anwendungsfall AdV-UC\_24: „Zertifikat von eGK lesen“ gemäß TAB\_ADV\_381 umsetzen.

**Tabelle 56: TAB\_ADV\_381 – AdV-UC\_24: Zertifikat von eGK lesen**

Benennung des Anwendungsfalls	„Zertifikat von eGK lesen“
Hinweistext für den Versicherten	-
Auslöser	Dieser Anwendungsfall wird ausgelöst, wenn das Clientsystem von der eGK des Versicherten ein Zertifikat lesen will. Diese Operation wird nicht direkt vom Versicherten aufgerufen, sondern in Rahmen eines übergeordneten Anwendungsfalls einer Fachanwendung, welche die benötigten Eingangsdaten bereitstellt.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen. Der Identifikator des zu lesenden Zertifikates (C.CH.ENC oder C.CH.ENCV) wird in den Eingangsdaten übergeben.
Nachbedingung	Als Rückgabewert wird das Zertifikat im X.509-Format zurückgegeben.
Standardablauf	Die Umsetzung ist in der Tabelle TAB_ADV_382 – Ablaufaktivitäten – AdV-UC_24: Zertifikat von eGK lesen beschrieben. <ol style="list-style-type: none"> <li>1. Zertifikat in PL_TUC_CARD_INFORMATION auswählen (C.CH.ENC oder C.CH.ENCV)</li> <li>2. Zertifikat zurückgeben</li> </ol>
Diagramm	Abbildung ABB_ADV_381 – Ablauf AdV-UC_24: Zertifikat von eGK lesen

**Tabelle 57: TAB\_ADV\_382 – Ablaufaktivitäten – AdV-UC\_24: Zertifikat von eGK lesen**

<b>1. PL_TUC_CARD_INFORMATION auslesen</b>	
Plattformbaustein	PL_TUC_CARD_INFORMATION
<i>Eingangsdaten</i>	
Zertifikat	C.CH.ENC oder C.CH.ENCV als Identifikator des Zertifikats

<b>2. PL_TUC_CARD_INFORMATION Ergebnis verarbeiten</b>	
<i>Rückgabedaten</i>	
Zertifikat	Daten wurden erfolgreich gelesen. Das Zertifikat wird zurückgegeben.
<i>Beschreibung</i>	Das Zertifikat wurde bereits bei Start der eGK Sitzung gelesen und liegt in PL_TUC_CARD_INFORMATION vor. Das gewünschte Zertifikat wird aus PL_TUC_CARD_INFORMATION ausgelesen.
<b>3. Ausgangsdaten zurückgeben</b>	
<i>Beschreibung</i>	Das gewünschte Zertifikat wird an den aufrufenden Anwendungsfall zurückgegeben.

[&lt;=]

## 6.2 Realisierung der Leistungen der TI-Plattform

Der Produkttyp KTR-AdV realisiert die von den Fachanwendungen benötigten Leistungen der TI-Plattform, die in den fachlichen Anwendungsfällen der AdV genutzt werden. Die bereitgestellten Leistungen umfassen einen für die Fachanwendungen einheitlichen Zugriff auf die eGK des Versicherten, Leistungen der PKI der Telematikinfrastruktur, Kryptooperationen, etc. die in übergreifenden Spezifikationen der gematik festgelegt sind. Die Definition der Leistungen der TI-Plattform in der KTR-AdV finden sich in Anhang B.

Zusätzlich muss in der Realisierung der Leistung der Plattform – wie in 2.2 beschrieben – festgelegt werden, wie umgebungsspezifische Operationen an der Schnittstelle zu den Leistungen der TI-Plattform umgesetzt werden sollen. Diese Festlegungen werden in den folgenden Abschnitten festgelegt.

### 6.2.1 Transportschnittstelle für Kartenkommandos

Der hier beschriebene Produkttyp KTR-AdV ist als reines Softwareprodukt konzipiert. Als solches muss die KTR-AdV eine Schnittstelle zu Karten der TI über ein Kartenterminal herstellen. Diese Schnittstelle muss die von den Plattformprozessen erzeugten, kartenverständlichen APDUs an die Karte übertragen und wird im Folgenden als ENV\_TUC\_CARD\_APDU\_TRANSPORT bezeichnet. Neben proprietären Schnittstellentreibern von Kartenterminalherstellern existieren eine Reihe standardisierter Schnittstellen, die auch von verschiedenen Betriebssystemen zur Anbindung handelsüblicher Kartenterminals unterstützt werden.

#### AdV-A\_2492 - Transportschnittstelle für Kartenkommandos

Die KTR-AdV MUSS eine Transportschnittstelle für die Übertragung von SmartCard-APDUs gegen die Standards CT-API und PCSC implementieren.[<=]

#### **AdV-A\_2493 - Ergänzende Standards für Transportschnittstelle**

Die KTR-AdV KANN eine Transportschnittstelle für die Übertragung von SmartCard-APDUs auf Basis des SICCT-Protokolls, gegen den Standard CCID und gegen proprietäre Hardwaretreiber eines Kartenterminalherstellers implementieren.[<=]

#### **AdV-A\_2494 - Handbuch: Liste unterstützter Kartenterminals**

Der Hersteller der KTR-AdV MUSS im Handbuch ausweisen, welche Standards und Schnittstellen zu Kartenterminals die KTR-AdV unterstützt und MUSS eine Liste mit handelsüblichen Kartenterminals angeben, die nachweislich mit dieser Ausprägung der KTR-AdV funktionieren.[<=]

Auf Seiten des Versicherten können Kartenterminalvarianten der Sicherheitsklassen 1 (reine Kontaktiereinheit), 2 (Kartenterminal mit eigenem PIN-Pad) oder 3 (PIN-Pad plus Display) zum Einsatz kommen. Zusätzlich ist die Ausstattung des eingesetzten Kartenterminals (Klasse 1, 2 oder 3) mit einer NFC-Schnittstelle möglich. Der Hersteller der KTR-AdV muss die von den Varianten gebotenen Features geeignet nutzen.

#### **AdV-A\_2499 - PIN-Eingabe nicht speichern**

Die KTR-AdV DARF ein eingegebenes PIN-Geheimnis NICHT temporär und NICHT persistent speichern.[<=]

#### **AdV-A\_2562 - PIN-Geheimnis ausschließlich an Karte übermitteln**

Die KTR-AdV MUSS sicherstellen, dass das eingegebene PIN-Geheimnis ausschließlich an die Karte und nicht an andere Adressaten übermittelt wird.[<=]

Das temporäre Speichern bezieht sich bei der Verwendung eines Kartenterminals der Sicherheitsklasse 1 auf das Verwenden der PIN über den Anwendungsfall hinaus, für den die PIN-Eingabe erfolgt ist, z.B. Caching während einer Sitzung. Gelangt die KTR-AdV bei der Verwendung eines Kartenterminals der Sicherheitsklassen 2 und 3 ggfs. durch Fehlkonfiguration in Kenntnis der PIN, darf es diese ebenfalls nicht temporär und nicht persistent speichern.

Auf Seite der Komponente AdV-Server in einem Rechenzentrum sind zusätzliche Varianten der Einbeziehung der Identitäten der Kostenträger in die Kartenoperationen möglich, wie z.B. Nutzung einer Webservice-Schnittstelle zu einem HSM oder das SICCT-Protokoll zur Anbindung eines HSM-B.

### **6.2.1.1 Kartenterminals der Sicherheitsklasse 1**

Kartenterminals der Sicherheitsklasse 1 verfügen über keine Sicherheitsmerkmale, sie sind eine reine Kontaktiereinheit einer SmartCard. Sämtliche Geheimnis-Eingaben und Hinweistext-Ausgaben müssen über die KTR-AdV mittels Bildschirm und Tastatur/Maus erfolgen.

#### **AdV-A\_2495 - Klasse 1: PIN-Eingabe**

Die KTR-AdV MUSS die PIN-/PUK-Eingabe über ein angeschlossenes Eingabegerät entgegennehmen und in ein an die Karte adressiertes Kommando einbetten, wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet wird.[<=]

#### **AdV-A\_2496 - Klasse 1: PIN-Eingabe Geheimnis**

Die KTR-AdV DARF die eingegebene PIN/PUK Ziffernfolge NICHT auf dem Bildschirm darstellen, wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet wird.[<=]

#### **AdV-A\_2497 - Klasse 1: PIN-Eingabe Eingabefeedback**



Die KTR-AdV MUSS ein eingegebenes Zeichen einer Geheimniseingabe mit dem Zeichen „ \* “ (Wildcard) quittieren, wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet wird.[<=]

#### **AdV-A\_2498 - Klasse 1: PIN-Eingabe Eingabevalidierung**

Die KTR-AdV MUSS ein eingegebenes, neues PIN-Geheimnis durch eine erneute Abfrage des neuen PIN-Geheimnisses verifizieren, wenn das Geheimnis durch einen Anwendungsfall geändert werden soll und wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet wird.[<=]

### **6.2.1.2 Kartenterminals der Sicherheitsklasse 2**

Kartenterminals der Sicherheitsklasse 2 verfügen über eine Eingabeschnittstelle zur Eingabe eines Benutzergeheimnisses. Typischerweise werden Kartenterminals der Sicherheitsklasse 2 in Anwendungsfällen mit Eingabe einer PIN bzw. PUK so angesteuert, dass das vorbereitete Kartenkommando mit einem Platzhalter des PIN-Geheimnisses an das Kartenterminal geschickt wird. Das Kartenterminal nimmt die PIN über die Eingabeschnittstelle entgegen, ersetzt den Platzhalter durch das eingegebene Geheimnis und leitet das Kartenkommando anschließend weiter an die Karte.

#### **AdV-A\_2500 - Klasse 2: PIN-Eingabe**

Die KTR-AdV MUSS ein angeschlossenes Kartenterminal der Sicherheitsklasse 2 so ansteuern, dass ein Kartenkommando, das eine PIN-/PUK-Eingabe erfordert, an einem Kartenterminal um die Benutzereingabe ergänzt und anschließend direkt an die adressierte Karte weitergeleitet wird.[<=]

#### **AdV-A\_2501 - Klasse 2: PIN-Eingabe Fehlkonfiguration**

Die KTR-AdV MUSS alle Operationen mit einer eindeutigen Fehlermeldung abbrechen, in denen sie die Kenntnis eines PIN/PUK-Geheimnisses erlangt, das an einem PIN-Pad eines Klasse 2 Kartenterminals eingegeben wurde.[<=]

#### **AdV-A\_2502 - Klasse 2: PIN-Eingabe Eingabefeedback**

Die KTR-AdV MUSS während der Abfrage einer PIN/PUK an einem Kartenterminal der Sicherheitsklasse 2 einen Benutzerhinweis zur PIN-Eingabe am Kartenterminal an der Bildschirmausgabe ausgeben.[<=]

### **6.2.1.3 Kartenterminals der Sicherheitsklasse 3**

Kartenterminals der Sicherheitsklasse 3 verfügen über eine Eingabeschnittstelle zur Eingabe eines Benutzergeheimnisses und Ausgabeschnittstelle zur Anzeige kurzer Textmeldungen. Typischerweise werden Kartenterminals der Sicherheitsklasse 3 in Anwendungsfällen mit Eingabe einer PIN bzw. PUK so angesteuert, dass das vorbereitete Kartenkommando mit einem Platzhalter des PIN-Geheimnisses an das Kartenterminal geschickt wird. Das Kartenterminal nimmt die PIN über die Eingabeschnittstelle entgegen, ersetzt den Platzhalter durch das eingegebene Geheimnis und leitet das Kartenkommando anschließend weiter an die Karte.

Während des Wartens auf eine Benutzereingabe kann ein an das Kartenterminal übergebener Text angezeigt werden. Einzelne Eingaben durch einen Benutzer werden in der Regel durch „\*“-Zeichen quittiert. Ebenso besitzen Kartenterminals der Sicherheitsklasse 3 meist zusätzliche Logik, z.B. Eingaben zu verifizieren (siehe Anforderungen zum Ändern einer PIN mittels Klasse 1-Kartenterminal). Auf diese Logik soll hier nicht weiter eingegangen werden.

#### **AdV-A\_2503 - Klasse 3: PIN-Eingabe**

Die KTR-AdV MUSS ein angeschlossenes Kartenterminal der Sicherheitsklasse 3 so ansteuern, dass ein Kartenkommando, das eine PIN-/PUK-Eingabe erfordert, an einem

Kartenterminal um die Benutzereingabe ergänzt und anschließend direkt an die adressierte Karte weitergeleitet wird.[<=]

#### **AdV-A\_2504 - Klasse 3: PIN-Eingabe Fehlkonfiguration**

Die KTR-AdV MUSS alle Operationen mit einer eindeutigen Fehlermeldung abbrechen, in denen sie die Kenntnis eines PIN/PUK-Geheimnisses erlangt, das an einem PIN-Pad eines Klasse 3 Kartenterminals eingegeben wurde.[<=]

#### **AdV-A\_2505 - Klasse 3: PIN-Eingabe Eingabefeedback**

Die KTR-AdV MUSS während der Abfrage einer PIN/PUK an einem Kartenterminal der Sicherheitsklasse 3 einen Benutzerhinweis zur PIN-Eingabe am Kartenterminaldisplay ausgeben.[<=]

Die Anzeige eines Benutzerhinweises soll den Benutzer informieren zu welchem Zweck er eine Eingabe tätigen soll (z.B. alte Pin, neue PIN im Anwendungsfall PIN ändern) und welches konkretes Geheimnis abgefragt werden soll (PIN, PUK, PIN einer konkreten Anwendung).

### **6.2.2 Schnittstelle für PIN-Operationen und Anbindung der Karten der TI**

Anwendungsfälle zur PIN-Verwaltung, die Kartenfreischaltung und Anwendungsfälle weiterer Fachanwendungen können die Eingabe eines PIN- oder PUK-Geheimnisses durch den Versicherten erfordern. Der Zugriff auf Karten der TI erfolgt über die Systemprozesse PL\_TUC\_CARD\_\*. Die KTR-AdV als Realisierungs Umgebung der Systemprozesse muss ihrerseits die von der Plattform geforderten Schnittstellen ENV\_TUC\_CARD\_SECRET\_INPUT implementieren, um die Kommunikation der Plattform mit dem Benutzer über die Außenschnittstelle der KTR-AdV zu ermöglichen. Die Außenschnittstelle ist in Kapitel 6.2.1 Transportschnittstelle für Kartenkommandos beschrieben und umfasst das Kartenterminal, Eingabemedium und Hinweistexte an den Benutzer. Diese kann je nach Konfiguration an einem Gerät als Kartenterminal der Sicherheitsklasse 3 oder auch eine Kombination aus Bildschirmausgabe, Kartenterminal-PIN-Pad und/oder Tastatureingabe erfolgen.

#### **AdV-A\_2506 - Übergabeschnittstelle PIN/PUK-Geheimnis**

Die KTR-AdV MUSS eine Operation ENV\_TUC\_SECRET\_INPUT zur Eingabe eines PIN/PUK-Geheimnisses und Weiterleitung an eine SmartCard mit den Parametern

- Eingabeparameter:
  - Identifikator
  - Aktion
  - minLength
  - maxLength
  - commandApduPart
- Rückgabewerte
  - responseApdu

implementieren.[<=]

#### **AdV-A\_2507 - Umsetzung ENV\_TUC\_SECRET\_INPUT**

Die KTR-AdV MUSS 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

- wenn der Eingabeparameter `Aktion` die Eingabe eines Benutzerhinweises erfordert, 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.[<=]

#### **AdV-A\_2555 - Minimalprinzip Karteninteraktion**

Die KTR-AdV DARF ein Kartenkommando NICHT an eine angebundene Karte weiterleiten, dass nicht explizit im Kontext eines Anwendungsfalls (intendierte Kartenoperationen und Erhöhen des Sicherheitszustands der Karte falls erforderlich) erforderlich ist.[<=]

### **6.2.3 Schnittstelle zur Freischaltung der eGK**

Um dem Versicherten zur Verwaltung seiner eGK die notwendigen Zugriffsrechte einzuräumen, muss die eGK über ein Card-2-Card-Verfahren freigeschaltet werden. Die Systemprozesse der TI-Plattform benötigen dafür eine vertrauliche, integre und authentische Schnittstelle zum Austausch von eGK-Challenge und einer Signatur dieser Challenge durch die SM-B-Identität der Kostenträger, die die Echtheit des Zertifikats und den Besitz des privaten Schlüssels zu diesem Zertifikat bestätigt.

In der Realisierungsumgebung der KTR-AdV muss dazu ein gesicherter Kanal zwischen der AdV-App beim Versicherten und dem AdV-Server in einem Rechenzentrum hergestellt werden. Anforderungen an diese gesicherte Verbindung werden im Kapitel „5.1.2 Absicherung der AdV-Komponenten“ beschrieben.

#### **AdV-A\_2508 - Transportschnittstelle für Card-2-Card**

Die KTR-AdV MUSS eine Transportschnittstelle `ENV_TUC_CARD_TO_CARD` mit einer Kommunikationsschnittstelle zweier Karten der TI im Card-2-Card-Verfahren realisieren. Wird in einem Card-2-Card-Verfahren über `ENV_TUC_CARD_TO_CARD` die Signatur eines tokens verlangt, so MUSS dieses über den Plattformbaustein `PL_TUC_SIGN_HASH_nonQES`, in dessen Zugriff sich ein CardProxy mit einer passenden Freischaltkarte befindet, mit den folgenden Parametern erfolgen:

IDENTIFIKATOR des privaten Schlüsselobjekts	PrK.SMC.AUTR_CVC des in <code>PL_TUC_CARD_INFORMATION</code> gespeicherten CV-Zertifikats gemäß <code>[gemSpec_CardProxy#Konfigurationstabelle CardProxy SMC-B]</code> und dem gewählten kryptografischen Verfahren R2048 bzw. E256
SIGNATURVERFAHREN	<code>elcRoleAuthentication</code> , oder <code>rsaRoleAuthentication</code> gemäß dem gewählten kryptografischen Verfahren des in <code>PL_TUC_CARD_INFORMATION</code> gespeicherten CV-Zertifikats
HASHWERT	Weiterleiten des <i>tokens</i> , das an der Schnittstelle <code>ENV_TUC_CARD_TO_CARD</code>

	übergeben wurde
--	-----------------

Der Rückgabewert von PL\_TUC\_SIGN\_HASH\_nonQES ist als Antwort an die Aufrufschnittstelle von ENV\_TUC\_CARD\_TO\_CARD zurückzugeben.[<=]

#### 6.2.4 Schnittstelle zu Diensten der zentralen TI-Plattform

Über einen sicheren zentralen Zugangspunkt (SZZP) stehen dem AdV-Server Dienste der zentralen TI-Plattform zur Verfügung.

##### AdV-A\_2509 - Kapselung der Zugriffe auf Dienste der zentralen TI-Plattform

Die KTR-AdV MUSS den Zugriff auf Dienste der zentralen TI-Plattform in einem ConsumerAdapter der Komponente AdV-Server kapseln.[<=]

##### AdV-A\_2510 - Proxy-Funktion des ConsumerAdapters für die AdV-App

Die Komponente AdV-App der KTR-AdV MUSS für die Nutzung der Dienste der zentralen TI-Plattform die kapselnden Operationen des Consumer Adapters nutzen.[<=]

##### AdV-A\_2511 - Separierung der AdV-App von Diensten der TI

Die Komponente AdV-App der KTR-AdV DARF NICHT direkt auf die Dienste der zentralen TI-Plattform und Fachdienste der Fachanwendungen zugreifen.[<=]

##### AdV-A\_2512 - Consumer Adapter verwendet SZZP

Der Anbieter einer KTR-AdV MUSS den Zugriff des Consumer Adapters auf die TI über einen SZZP realisieren.[<=]

Über den Consumer Adapter werden die in ABB\_ADV\_302 und in TAB\_ADV\_301 dargestellten Schnittstellen zu Diensten der zentralen TI-Plattform und zu Fachdiensten bereitgestellt.

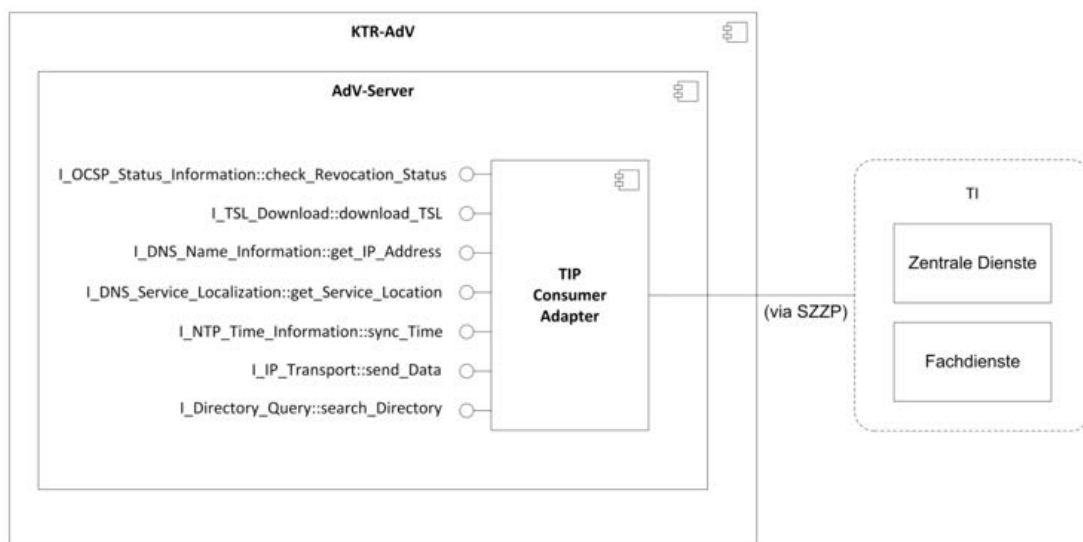


Abbildung 21: ABB\_ADV\_302 - Schnittstellen des TIP Consumer Adapters

**Tabelle 58: TAB\_AdV\_301 - Schnittstellen des Consumer Adapters**

<b>Bereitgestellte Schnittstellen</b>	
<b>Schnittstelle</b>	<b>Anbieter [Spezifikation]</b>
I_TSL_Download	TIP Consumer Adapter [gemSpec_TSL]
	Vom TSL-Dienst kann die aktuelle TSL heruntergeladen werden.
I_NTP_Time_Information	TIP Consumer Adapter [gemSpec_Net]
	Über den Zeitdienst wird innerhalb der TI die Zeit aller Komponenten synchronisiert.
I_DNS_Service_Localization	TIP Consumer Adapter [gemSpec_Net]
	Durch eine mit fachlichen Merkmalen parametrisierte Abfrage kann der URI eines Fachdienstes ermittelt werden.
I_DNS_Name_Resolution	TIP Consumer Adapter [gemSpec_Net]
	Durch eine mit fachlichen Merkmalen parametrisierte Abfrage kann der URI eines Fachdienstes ermittelt werden.
I_IP Transport	TIP Consumer Adapter [gemSpec_Net]
	Das Zentrale Netz TI stellt die Transportmechanismen in der zentralen TI bereit.
I_OCSP_Status_Information	TIP Consumer Adapter [gemSpec_PKI]
	Über den TSP X.509 nonQES des Zertifikatherausgebers wird bei Zertifikatsprüfungen der aktuelle Status des Zertifikats geprüft. Die Leistung zum Prüfen der zeitlichen und mathematischen Gültigkeit eines Zertifikats setzt die KTR-AdV in Plattformbausteinen (siehe. Anhang B) selbst um. Lediglich der Sperrstatus wird mittels I_OCSP_Status_Information an der zentralen TI-Plattform abgefragt.
<b>Benötigte Schnittstellen</b>	
<b>Schnittstelle</b>	<b>Anbieter [Spezifikation]</b>
(Zugang zur TI über einen SZZP)	Zentrale Dienste und Fachdienste [gemSpec_Net]
	Über den SZZP kann der TIP Consumer Adapter auf die TI zugreifen um die oben genannten Schnittstellen bereitzustellen.

## 6.3 Schnittstelle zwischen AdV-App und AdV-Server

Die Schnittstelle zwischen der AdV-App und dem AdV-Server liegt innerhalb des Produkttyps KTR-AdV. Es handelt sich daher um eine Innenschnittstelle. An diese werden keine inhaltlichen Anforderungen gestellt. Es werden jedoch Sicherheitsanforderungen im Kapitel 5.1.2 hierzu erhoben.

## 6.4 Identitäten der KTR-AdV

*In der Beschreibung der Leistungen der dezentralen TI-Plattform im Anhang sowie in der Plattformkomponente CardProxy erfolgt die Schnittstellendefinition für den Zugriff auf die SM-B-Identitäten und deren kryptografisches Schlüsselmaterial auf Basis einer SMC-B mit entsprechendem Objektsystem.*

*Mit der Verwendung eines HSM und einer herstellerspezifischen Schnittstelle für den HSM-Zugriff können sich sowohl die Schnittstellenoperationen als auch die Bezeichner der entsprechenden SM-B-Identitäten von denen in der Spezifikation der KTR-AdV unterscheiden. Diese Abweichung ist ausdrücklich zulässig, soweit die Realisierung protokollarische Vorgaben und das geforderte Sicherheitsniveau einhält.*

Die KTR-AdV benötigt zwei Rollen mit entsprechenden Identitäten zur Abbildung der oben genannten Anwendungsfälle. Als Kostenträgerorganisation soll sie dem Versicherten Zugriffsrechte auf seiner eGK zur Durchführung der AdV-Anwendungsfälle freischalten. Die Angaben zu dieser Kostenträgerorganisation werden auch zur Vervollständigung des obligatorischen eGK-Protokolleintrags verwendet.

Des Weiteren muss sich die KTR-AdV mit fachanwendungsspezifischen Fachdiensten verbinden können. Hierzu muss sie als Rechenzentrums-Consumer in einer passenden Rolle authentisiert werden.

Diese zwei Aspekte müssen in der KTR-AdV über Zertifikate abgebildet werden, deren zugehöriges kryptografisches, privates Schlüsselmaterial in der Realisierung der KTR-AdV integritätsgeschützt und vertraulich gespeichert werden muss.

### **AdV-A\_2513 - Privates Schlüsselmaterial in HSM speichern**

Die KTR-AdV MUSS privates Schlüsselmaterial zu Zertifikaten der Rollenauthentisierung gegenüber einer eGK und des Verbindungsaufbaus zu Diensten der TI in einem HSM integritätsgeschützt und vertraulich speichern, dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. 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.[<=]

Die Anbindung an den AdV-Server in einem Rechenzentrum kann über eine herstellerspezifische Schnittstelle mit einem handelsüblichen HSM erfolgen, die die oben genannten Sicherheitsziele erfüllt. Eine Anbindung eines HSM-Bs via SICCT ist nicht zwingend erforderlich.

Zum Zeitpunkt der Fertigstellung dieser Spezifikation erfüllt eine zugelassene SMC-B die oben genannte Anforderung und kann als HSM eingesetzt werden.

Falls keine SMC-B als HSM zum Einsatz kommt, müssen die Zertifikate auf sichere Weise in das HSM eingebracht werden. An dieser Stelle werden keine konkreten Technologien oder Prozessschritte vorgegeben, damit der Betreiber der KTR-AdV mit einem TSP ein geeignetes Verfahren etablieren kann.



**Tabelle 61: TAB\_ADV\_385 – Personalisierung eines HSM**

Aspekt	Beschreibung
Schlüsselmaterial der KTR-AdV	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.

**AdV-A\_2575 - Personalisierung des HSMs**

Falls der Betreiber der KTR-AdV keine SMC-B als HSM einsetzt, MUSS er einen sicheren Prozess zur Personalisierung des HSMs definieren und etablieren, der die in TAB\_ADV\_385 genannten Aspekte beinhaltet. [≤]

Falls für diesen Prozess nur eine geringe Anzahl an Instanzen erwartet wird, kann es sinnvoll sein, Teile dieses Prozesses rein organisatorisch umzusetzen. Anstelle einer technischen Schnittstelle kann dann ein papierbasiertes Verfahren eingesetzt werden.

**A\_15118 - CV-Zertifikat für PIN Status Prüfung**

Die KTR-AdV MUSS über ein CV-Zertifikat C.SMC.NULL\_CVC verfügen, mit dem in einem Authentisierungsverfahren ein Trusted Channel aufgebaut wird, jedoch keine Zugriffsrechte für KTR-AdV- Anwendungsfälle auf einer eGK freigeschaltet werden. [≤]

**AdV-A\_2514 - CV-Zertifikat für eGK-Freischaltung**

Die KTR-AdV MUSS über ein CV-Zertifikat C.SMC.AUTR\_CVC verfügen, mit dem auf einer eGK Zugriffsrechte für KTR-AdV-Anwendungsfälle in einem Authentisierungsverfahren freigeschaltet werden. [≤]

Abhängig von der Realisierung eines sicheren Zertifikatsspeichers in der KTR-AdV kann das Authentisierungsverfahren zur Freischaltung der eGK über ein Card-2-Card- oder auch Card-2-Server-Verfahren erfolgen.

**AdV-A\_2515 - X.509-Zertifikat für TLS-gesicherte Verbindung**

Die KTR-AdV MUSS über ein X.509-Zertifikat zum Zweck des TLS-Verbindungsaufbaus mit der Rolle `professionOID = OID <oid_adv_ktr>` gemäß [gemSpec\_OID] verfügen, um sich gegenüber einem Fachdienst zu authentisieren, welches als C.HCI.AUT identifiziert wird. [≤]

**AdV-A\_2516 - X.509-Zertifikat für eGK-Protokolleintrag**

Die KTR-AdV MUSS über ein X.509-Zertifikat mit einem CommonName entsprechend den Vorgaben des verantwortlichen Zertifikat-Herausgebers verfügen, um einen für den Versicherten lesbaren, nachvollziehbaren Protokolleintrag auf der eGK über die Nutzung der KTR-AdV erzeugen zu können. [≤]

**AdV-A\_2556 - nachvollziehbarer eGK-Protokolleintrag mit Bezug zum Anbieter**

Der Anbieter der KTR-AdV MUSS sicherstellen, dass auf der eGK des Versicherten ein lesbarer, nachvollziehbarer Protokolleintrag mit Bezug zum Anbieter der KTR-AdV erzeugt werden kann.[<=]

Der Anbieter ist in diesem Zusammenhang eine Krankenkasse, in deren Auftrag ein Betreiber die KTR-AdV eines spezifischen Herstellers den Versicherten zur Verfügung stellt. Da aus diesem Zertifikat lediglich der CommonName verwendet und kein privates Schlüsselmaterial zur Authentisierung verwendet wird, kann auf die Nutzung dieses Zertifikats verzichtet werden. Es muss jedoch sichergestellt werden, dass auf der eGK des Versicherten ein lesbarer, nachvollziehbarer Protokolleintrag mit Bezug zum Anbieter der KTR-AdV erzeugt wird.



---

## 7 Informationsmodell

---

Ein gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten wird nicht benötigt.

---

## 8 Verteilungssicht

---

Eine zusätzliche Darstellung der hardwareseitigen Verteilung des Produkttyps bzw. seiner Teilsysteme und der Einbettung in die physikalische Umgebung wird nicht benötigt.

## 9 Anhang A – Verzeichnisse

### 9.1 Abkürzungen

Abkürzung	Bedeutung
AdV	Anwendungen des Versicherten
AMTS	Fachanwendung Arzneimitteltherapiesicherheit
AUT-Zertifikat	Authentication-Zertifikat
C2C	Card-to-Card-Authentisierung
COS	Card Operating System, Betriebssystem einer Smartcard
CV-Zertifikat	Card Verifiable-Zertifikat
DF	Dedicated File im Objektsystem der eGK, Ordner
DPE	Datensatz ‚Persönliche Erklärungen‘
EF	Elementary File im Objektsystem der eGK, Datei
eGK	elektronische Gesundheitskarte
eMP	Elektronischer Medikationsplan
FLA	Fachlogik der Fachanwendungen auf Seite der AdV-App
FLS	Fachlogik der Fachanwendungen auf Seite des AdV-Servers
GDD	Gesundheitsdatendienst
GVD	Geschützte Versichertendaten
HBA	Heilberufsausweis
HCA	Health Care Application
HSM	Hardware Security Module
HSM-B	Hardware Security Module Typ B
ICCSN	Integrated Circuit Card Serial Number

IFD	Interface Device
ISM	Informationssicherheitsmanagement
KSR	Konfigurations- und Software-Repository
KTR	Kostenträger
KTR-AdV	AdV in einer Umgebung im Auftrag der Kostenträger
LE	Leistungserbringer
MRPIN	Multireferenz-PIN
NFD	Notfalldatensatz
NFDM	Notfalldatenmanagement
OSE	Organspendeerklärung
n/a	entfällt
PD	Persönliche Versichertendaten
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PT	Produkttyp
PUK	Personal Unblocking Key
SM-B	Sammelbegriff für SMC-B und HSM-B
SZZP	Sicherer Zentraler Zugangspunkt
TI	Telematikinfrastruktur
TIP	Telematikinfrastruktur-Plattform
TLS	Transport Layer Security
TSL	Trust-service Status List
VD	Allgemeine Versicherungsdaten
VSD	Versichertenstammdaten
VSDM	Versichertenstammdatenmanagement

## 9.2 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.
Gerät des Versicherten	Gerät bzw. Computer im Besitz des Versicherten, welches eine Ausführungsumgebung der AdV-App darstellt.

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

## 9.3 Abbildungsverzeichnis

Abbildung 1: ABB_ADV_300 – Überblick AdV in einer Umgebung im Auftrag der Kostenträger .....	9
Abbildung 2: ABB_ADV_304 – Zusammenhang Systemprozesse und Fachanwendung	11
Abbildung 3: ABB_ADV_301 – Kontextdiagramm .....	15
Abbildung 4: ABB_ADV_303 – Verteilungsdiagramm .....	15
Abbildung 5: ABB_ADV_329 – Komponentendiagramm der KTR-AdV .....	17
Abbildung 6 : ABB_ADV_333 Verbindungsaufbau und Freischaltung eGK .....	24
Abbildung 7: ABB_ADV_305 – Ablauf „Anwendung auf eGK deaktivieren“ .....	42
Abbildung 8: ABB_ADV_383 – Ablauf „Anwendung auf eGK reaktivieren“ .....	46
Abbildung 9: ABB_ADV_308 – Ablauf AdV-UC_03 „PIN für Fachanwendung einschalten“ .....	54
Abbildung 10: ABB_ADV_310 – Ablauf AdV-UC_04 „PIN für Fachanwendung ausschalten“ .....	57
Abbildung 11: ABB_ADV_317 - Ablauf des „VSD von eGK lesen“ .....	60
Abbildung 12: ABB_ADV_314 – Ablauf des AdV-UC_21: „Zugriffsprotokoll anzeigen“ ....	64
Abbildung 13: ABB_ADV_315 Standardablauf – Datenübertragung bei Kartentausch durchführen .....	71
Abbildung 14: ABB_ADV_359 – Ablauf des AdV-UC_121: „DPE von eGK anzeigen“ .....	79
Abbildung 15: ABB_ADV_361 – Ablauf des AdV-UC_122: „DPE auf eGK ändern“ .....	81
Abbildung 16: ABB_ADV_363 – Ablauf des AdV-UC_123: „DPE auf eGK löschen“ .....	84
Abbildung 17: ABB_ADV_322 – Ablauf des AdV-UC_25: "Mit eGK verschlüsseln" .....	94
Abbildung 18: ABB_ADV_324 – Ablauf des AdV-UC_26: „Mit eGK entschlüsseln“ .....	96
Abbildung 19: ABB_ADV_379 – Ablauf des AdV-UC_27 „Authentisierungsrequest mit eGK signieren“ .....	99
Abbildung 20: ABB_ADV_381 – Ablauf AdV-UC_24: Zertifikat von eGK lesen .....	101
Abbildung 21: ABB_ADV_302 - Schnittstellen des TIP Consumer Adapters .....	108

Abbildung 22: Systemprozesse der Basis-TI.....	127
Abbildung 23: Umgebungsspezifische Operationen.....	128

## 9.4 Tabellenverzeichnis

Tabelle 1: TAB_ADV_300 – Akteure und ihre Rollen .....	12
Tabelle 2: TAB_ADV_329 – Komponenten, Verantwortung und Funktionalitäten .....	17
Tabelle 3: TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine.....	29
Tabelle 4: TAB_ADV_303 – Starten einer AdV-Sitzung .....	31
Tabelle 5: TAB_ADV_304 – Ablaufaktivitäten - Starten einer AdV-Sitzung .....	32
Tabelle 6: TAB_ADV_320 – Übergreifende Vorbedingungen.....	38
Tabelle 7: TAB_ADV_384 – Zulässige Anwendungsfälle nach Status von Karte, Anwendung und PIN.....	39
Tabelle 8: TAB_ADV_461 – Benennung der Anwendungen und Hinweise am Terminal.....	41
Tabelle 9: TAB_ADV_305 – AdV-UC_14 „Anwendung auf eGK deaktivieren“ .....	42
Tabelle 10: TAB_ADV_306 – Ablaufaktivitäten – AdV-UC_14 .....	43
Tabelle 11: TAB_ADV_383 – AdV-UC_15 „Anwendung auf eGK reaktivieren“ .....	46
Tabelle 12: TAB_ADV_307 – Ablaufaktivitäten – AdV-UC_15 .....	47
Tabelle 13: TAB_ADV_312 – PIN der eGK ändern .....	49
Tabelle 14: TAB_ADV_313 – Ablaufaktivitäten – PIN der eGK ändern .....	50
Tabelle 15: TAB_ADV_316 – PIN der eGK entsperren .....	52
Tabelle 16: TAB_ADV_317 – Ablaufaktivitäten – PIN der eGK entsperren .....	52
Tabelle 17: TAB_ADV_308 – AdV-UC_03 „PIN für Fachanwendung einschalten“ .....	54
Tabelle 18: TAB_ADV_309 – Ablaufaktivitäten – AdV-UC_03 .....	55
Tabelle 19: TAB_ADV_310 – AdV-UC_04 „PIN für Fachanwendung ausschalten“ .....	57
Tabelle 20: TAB_ADV_311 – Ablaufaktivitäten – AdV-UC_04 .....	58
Tabelle 21: TAB_ADV_314 – VSD von eGK anzeigen.....	60
Tabelle 22: TAB_ADV_315 – Ablaufaktivitäten – VSD von eGK anzeigen .....	61
Tabelle 23: TAB_ADV_350 – Zugriffsprotokoll anzeigen.....	64
Tabelle 24: TAB_ADV_351 – Ablaufaktivitäten – Zugriffsprotokoll anzeigen.....	65
Tabelle 25: TAB_ADV_352 – Versicherten-PIN der eGK ändern .....	67
Tabelle 26: TAB_ADV_353 – Versicherten-PIN entsperren .....	67
Tabelle 27: TAB_ADV_354 – Ablaufaktivitäten – Versicherten-PIN entsperren .....	68
Tabelle 28: TAB_ADV_324 – Datenübertragung bei Kartentausch durchführen .....	71

Tabelle 29: TAB_ADV_325 – Ablaufaktivitäten – Datenübertragung bei Kartentausch durchführen .....	72
Tabelle 30: TAB_ADV_355 – NFD auf eGK verbergen .....	75
Tabelle 31: TAB_ADV_356 – Verborgene NFD auf eGK sichtbar machen.....	76
Tabelle 32: TAB_ADV_357 – PIN für NFD einschalten .....	77
Tabelle 33: TAB_ADV_358 – PIN für NFD ausschalten .....	77
Tabelle 34: TAB_ADV_359 – DPE von eGK anzeigen.....	79
Tabelle 35: TAB_ADV_360 – Ablaufaktivitäten – DPE von eGK anzeigen .....	80
Tabelle 36: TAB_ADV_361 – DPE auf eGK ändern .....	82
Tabelle 37: TAB_ADV_362 – Ablaufaktivitäten – DPE auf eGK ändern .....	82
Tabelle 38: TAB_ADV_363 – DPE auf eGK löschen.....	85
Tabelle 39: TAB_ADV_364 – Ablaufaktivitäten – DPE auf eGK löschen .....	85
Tabelle 40: TAB_ADV_365 – PIN für DPE einschalten .....	86
Tabelle 41: TAB_ADV_366 – PIN für DPE ausschalten .....	87
Tabelle 42: TAB_ADV_367 – DPE auf eGK verbergen .....	88
Tabelle 43: TAB_ADV_368 – Verborgenen DPE auf eGK sichtbar machen.....	88
Tabelle 44: TAB_ADV_369 – AMTS-Vertreter-PIN ändern .....	89
Tabelle 45: TAB_ADV_370 – AMTS-Vertreter-PIN entsperren .....	90
Tabelle 46: TAB_ADV_371 – eMP/AMTS-Datensatz auf eGK verbergen .....	91
Tabelle 47: TAB_ADV_372 – Verborgene eMP/AMTS-Datensatz auf eGK sichtbar machen.....	91
Tabelle 48: TAB_ADV_373 – PIN für AMTS einschalten .....	92
Tabelle 49: TAB_ADV_374 – PIN für AMTS ausschalten .....	93
Tabelle 50: TAB_ADV_375 – Adv-UC_25: „Mit eGK verschlüsseln“ .....	94
Tabelle 51: TAB_ADV_376 – Ablaufaktivitäten – Mit eGK verschlüsseln .....	95
Tabelle 52: TAB_ADV_377 – Adv-UC_26: „Mit eGK entschlüsseln“ .....	97
Tabelle 53: TAB_ADV_378 – Ablaufaktivitäten – Mit eGK entschlüsseln .....	97
Tabelle 54: TAB_ADV_379 – Authentisierungsrequest mit eGK signieren .....	99
Tabelle 55: TAB_ADV_380 – Ablaufaktivitäten – Authentisierungsrequest mit eGK signieren .....	100
Tabelle 56: TAB_ADV_381 – Adv-UC_24: Zertifikat von eGK lesen.....	102
Tabelle 57: TAB_ADV_382 – Ablaufaktivitäten – Adv-UC_24: Zertifikat von eGK lesen .....	102
Tabelle 58: TAB_AdV_301 - Schnittstellen des Consumer Adapters .....	109
Tabelle 59: TAB_ADV_473 – Hinweistexte für den Versicherten .....	121

## 9.5 Referenzierte Dokumente

### 9.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemKPT_Test]	gematik: Testkonzept der TI
[gemSpec_CardProxy]	gematik: AdV Baustein Card Proxy
[gemSpec_FLA_NFDM]	gematik: Spezifikation Fachlogik der Fachanwendung NFDM in KTR-AdV
[gemSpec_FM_VSDM]	gematik: Spezifikation Fachmodul VSDM
[gemSpec_Karten_Fach_TIP]	gematik: Befüllvorschriften für die Plattformanteile der Karten der TI
[gemSpec_eGK_ObjSys]	gematik: Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_KTR-AdV-Terminal]	gematik: Spezifikation KTR-AdV-Terminal
[gemSpec_NET]	gematik: Übergreifende Spezifikation Netzwerk
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_PKI]	gematik: Spezifikation PKI



[gemSpec_SST_FD_VSDM]	gematik: Schnittstellenspezifikation Fachdienste (UFS/VSDD/CMS)
[gemSpec_SST_VSDM]	gematik: Schnittstellenspezifikation Transport VSDM
[gemSysL_VSDM]	gematik: Systemspezifisches Konzept Versichertenstammdaten-management (VSDM)

### 9.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI TR AdV-App]	Technische Richtlinie BSI TR Anwendungen des Versicherten - AdV-App

## 9.6 Hinweistexte der Fachanwendungen

Tabelle 59: TAB\_ADV\_473 – Hinweistexte für den Versicherten

ID	Bezeichnung Anwendungsfal l	Hinweistext für Versicherten
<b>Verwaltung der eGK durch den Versicherten</b>		
AdV001	Versichertendaten anzeigen	Sie können die auf Ihrer Gesundheitskarte gespeicherten Versichertendaten einsehen. Haben Sie Ihrer Krankenkasse eine Änderung zu Ihrem Versicherungsverhältnis gemeldet, werden die Daten auf der Karte automatisch aktualisiert.
AdV002	Zugriffsprotokoll anzeigen	Sie können die Protokolldaten der letzten 50 Zugriffe auf Daten Ihrer Gesundheitskarte einsehen, die im Rahmen einer ärztlichen Behandlung, Arzneimittelabgabe in einer Apotheke oder in einer AdV-Umgebung getätigt worden sind.
AdV003	Versicherten-PIN ändern	Sie können Ihre Versicherten-PIN auf der Gesundheitskarte ändern.

AdV004	Versicherten-PIN entsperren	Sie können Ihre gesperrte Versicherten-PIN auf der Gesundheitskarte durch Eingabe der PUK entsperren und eine neue Versicherten-PIN vergeben.
AdV005	Datenübertragung bei Kartentausch	Sie können Ihre Hinweise auf Persönliche Erklärungen von Ihrer alten Gesundheitskarte auf Ihre neue Gesundheitskarte übertragen. Nach dem Kopieren der Daten wird die Anwendung auf der alten Gesundheitskarte verborgen. Falls auf der neuen Gesundheitskarte bereits Daten einer Anwendung vorhanden sind, werden diese nicht überschrieben.
<b>Verwaltung der NFD</b>		
AdV008	Notfalldaten verbergen	Sie können die auf Ihrer Gesundheitskarte gespeicherten Notfalldaten verbergen. Die Notfalldaten werden dabei nicht gelöscht. Wenn Sie die Notfalldaten verbergen, können sie auch im Notfall nicht gelesen werden.
AdV009	Verborgene Notfalldaten wieder anzeigen	Sie können die auf Ihrer Gesundheitskarte verborgenen Notfalldaten wieder sichtbar machen, sodass diese durch einen Arzt wieder eingesehen oder bearbeitet werden können.
AdV010	PIN-Schutz für Notfalldaten einschalten	Sie können den PIN-Schutz für das Lesen und Schreiben Ihrer Notfalldaten auf der Gesundheitskarte einschalten. Bei eingeschaltetem PIN-Schutz ist ein Lesen und Schreiben Ihrer Notfalldaten beim Arzt nur mit Ihrer vorherigen PIN-Eingabe möglich. Das Lesen der Notfalldaten im Notfall erfolgt immer ohne eine PIN-Eingabe.

AdV011	PIN-Schutz für Notfalldaten ausschalten	Sie können den PIN-Schutz für das Lesen und Schreiben Ihrer Notfalldaten auf der Gesundheitskarte ausschalten. Bei ausgeschaltetem PIN-Schutz ist ein Lesen und Schreiben Ihrer Notfalldaten beim Arzt ohne Ihre vorherige PIN-Eingabe möglich. Das Lesen der Notfalldaten im Notfall erfolgt immer ohne eine PIN-Eingabe.
<b>Verwaltung des DPE</b>		
AdV012	Hinweise auf Persönliche Erklärungen anzeigen	Sie können die auf Ihrer Gesundheitskarte gespeicherten Hinweise auf Aufbewahrungsorte zu persönlichen Erklärungen (Patientenverfügung, Vorsorgevollmacht, Erklärung zur Organ- und Gewebespende (Organspendeausweis)) einsehen.
AdV013	Hinweise auf Persönliche Erklärungen bearbeiten	Sie können Ihre Hinweise auf Aufbewahrungsorte Ihrer persönlichen Erklärungen (Patientenverfügung, Vorsorgevollmacht, Erklärung zur Organ- und Gewebespende (Organspendeausweis)) auf der Gesundheitskarte eintragen, ändern oder austragen.
AdV014	Alle Hinweise auf Persönliche Erklärungen löschen	Sie können alle auf Ihrer Gesundheitskarte gespeicherten Hinweise auf persönliche Erklärungen löschen. Sie können jederzeit neue Hinweise auf persönliche Erklärungen auf Ihrer Gesundheitskarte eintragen. Wenn Sie nur einen einzelnen Hinweis löschen möchten, wählen Sie "Hinweise auf persönliche Erklärungen bearbeiten".

AdV015	Hinweise auf Persönliche Erklärungen verbergen	Sie können die auf Ihrer Gesundheitskarte gespeicherten Hinweise auf persönliche Erklärungen verbergen. Die Hinweise werden dabei nicht gelöscht. Wenn Sie die Hinweise verbergen, können sie auch im Notfall nicht gelesen werden.
AdV016	Verborgene Hinweise auf Persönliche Erklärungen wieder anzeigen	Sie können die auf Ihrer Gesundheitskarte verborgenen Hinweise auf persönliche Erklärungen wieder sichtbar machen, sodass Sie oder ein Arzt diese wieder einsehen oder bearbeiten kann.
AdV017	PIN-Schutz für Persönliche Erklärungen einschalten	Sie können den PIN-Schutz für das Lesen und Schreiben Ihrer Hinweise auf persönliche Erklärungen auf der Gesundheitskarte einschalten. Bei eingeschaltetem PIN-Schutz ist ein Lesen und Schreiben Ihrer Hinweise auf persönliche Erklärungen beim Arzt nur mit Ihrer vorherigen PIN-Eingabe möglich. Das Lesen der Hinweise im Notfall erfolgt immer ohne eine PIN-Eingabe.
AdV018	PIN-Schutz für Persönliche Erklärungen ausschalten	Sie können den PIN-Schutz für das Lesen und Schreiben Ihrer Hinweise auf persönliche Erklärungen auf der Gesundheitskarte ausschalten. Bei ausgeschaltetem PIN-Schutz ist ein Lesen und Schreiben Ihrer Hinweise auf persönliche Erklärungen beim Arzt ohne Ihre vorherige PIN-Eingabe möglich. Das Lesen der Hinweise im Notfall erfolgt immer ohne eine PIN-Eingabe.
<b>Verwaltung eMP / AMTS</b>		
AdV022	Vertreter-PIN ändern	Sie können eine Vertreter-PIN für den Medikationsplan / die arzneimitteltherapiesicherheitsrelevante n Daten auf Ihrer Gesundheitskarte vergeben, wenn Sie einen Vertreter zur Erledigung von Arzt- beziehungsweise Apothekenbesuchen beauftragen möchten.

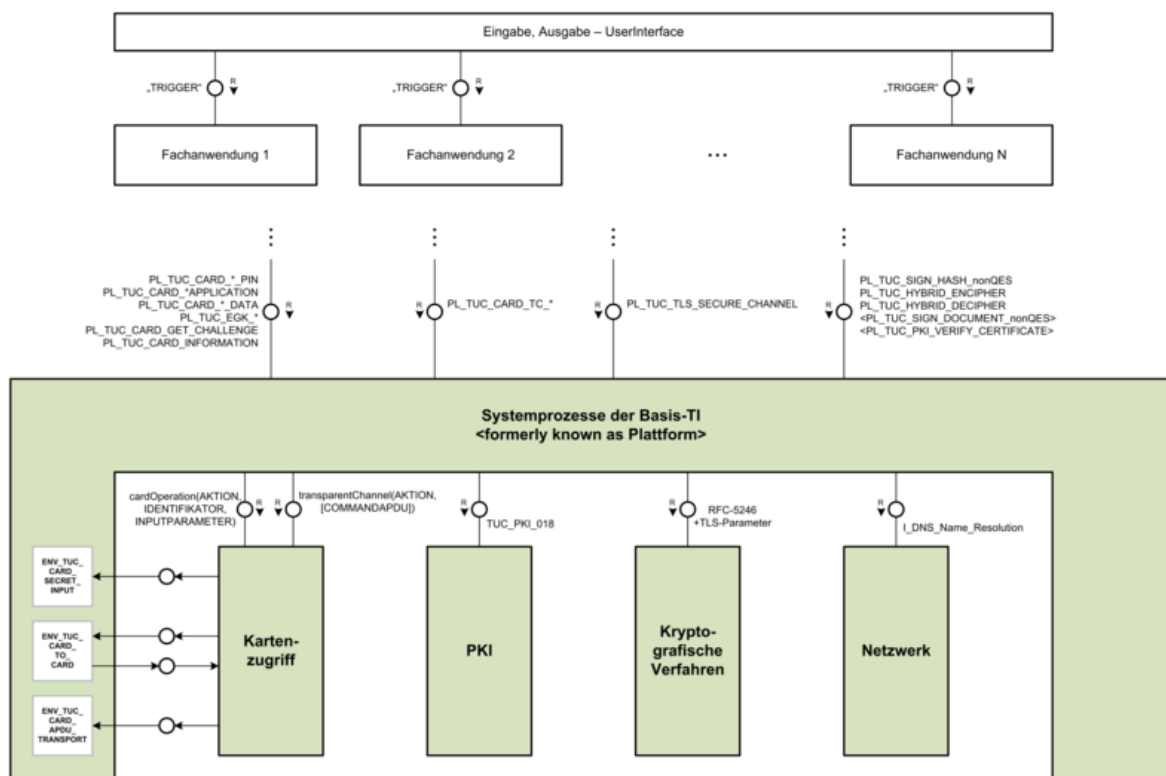
AdV023	Vertreter-PIN entsperren	Sie können die gesperrte Vertreter-PIN für den Medikationsplan/die arzneimitteltherapiesicherheitsrelevanten Daten auf Ihrer Gesundheitskarte durch die Eingabe Ihrer Versicherten-PIN entsperren und eine neue Vertreter-PIN vergeben.
AdV024	Medikationsplan verbergen	Sie können den auf Ihrer Gesundheitskarte gespeicherten Medikationsplan/die arzneimitteltherapiesicherheitsrelevanten Daten samt Einwilligungsdaten verbergen. Der Medikationsplan/die arzneimitteltherapiesicherheitsrelevanten Daten werden dabei nicht gelöscht.
AdV025	Verborgenen Medikationsplan wieder anzeigen	Sie können die auf Ihrer Gesundheitskarte gespeicherten, verborgenen Medikationsplan/die arzneimitteltherapiesicherheitsrelevanten Daten samt Einwilligungsdaten wieder sichtbar machen, sodass ein Arzt oder Apotheker diesen wieder einsehen oder bearbeiten kann.
AdV026	PIN-Schutz für Medikationsplan einschalten	Sie können den PIN-Schutz für das Lesen und Schreiben Ihres Medikationsplans/die arzneimitteltherapiesicherheitsrelevanten Daten auf der Gesundheitskarte einschalten. Bei eingeschaltetem PIN-Schutz ist ein Lesen und Schreiben der Daten beim Arzt oder Apotheker nur mit Ihrer vorherigen PIN-Eingabe möglich.
AdV027	PIN-Schutz für Medikationsplan ausschalten	Sie können den PIN-Schutz für das Lesen und Schreiben Ihres Medikationsplans/der arzneimitteltherapiesicherheitsrelevanten Daten auf der Gesundheitskarte ausschalten. Bei ausgeschaltetem PIN-Schutz ist ein Lesen und Schreiben der Daten beim Arzt oder Apotheker ohne Ihre vorherige PIN-Eingabe möglich.
<b>Fachanwendungsunabhängige Anwendungsfälle</b>		

AdV030	Mit eGK verschlüsseln	Sie können mit Ihrer Gesundheitskarte Daten verschlüsseln.
AdV031	Mit eGK entschlüsseln	Sie können mit Ihrer Gesundheitskarte verschlüsselte Daten wieder entschlüsseln.

## 10 Anhang B – Leistungen der dezentralen TI-Plattform

Im Folgenden werden Leistungen der TI-Plattform beschrieben und als Systemprozesse deklariert. Diese Systemprozesse beschreiben wie mit Produkttypen der TI zu verfahren ist, um eine Plattformleistung für Fachanwendungen der TI zu erbringen. Diese Lösung hat das Ziel, Basisleistungen der TI-Plattform einheitlich und produkttyp unabhängig zu definieren.

Durch das Zusammenschalten von Operationen und Bausteinen der verschiedenen Fachdomänen der TI-Plattform (Kartenzugriff, PKI, Kryptografische Verfahren) entstehen höherwertige Plattformbausteine mit einer vereinheitlichten Syntax für den Zugriff auf produkttypübergreifende Plattformleistungen („**PL\_TUC\_\***“). Den Zusammenhang der verschiedenen Domänen und den damit komponierten höherwertigen Systemprozessen verdeutlicht die folgende Abbildung als *technische Dokumentenlandkarte* (in der Darstellung grün markiert).



**Abbildung 22: Systemprozesse der Basis-TI**

Die Beschreibung dieser Systemprozesse der TI erfolgt normativ, es wird jedoch auf eine prozedurale Ablaufbeschreibung verzichtet. Es erfolgt eine Festlegung, was zu tun ist, um eine vorgegebene Plattformleistung zu erbringen. Die konkrete Realisierung dieser Leistung eines Systemprozesses ist abhängig von Umgebungsannahmen und muss unter bestimmten Bedingungen um umgebungsspezifische Operationen und Festlegungen ergänzt werden. Sie sorgen für einen umgebungsspezifischen Zuschnitt (tayloring) der Systemprozesse, um eine TI-übergreifend spezifizierte Leistung in einer konkreten Ablaufumgebung von einem konkreten Produkttypen oder Dienst einer Fachanwendung zu erbringen.

Die umgebungsspezifischen Operationen, Umgebungsannahmen oder -parameter müssen von der Realisierungs Umgebung („ENV\_TUC\_“\*) normativ festgelegt werden. Der Produkttyp, der die hier spezifizierten Plattformleistungen nutzt, muss Festlegungen treffen, wie diese umgebungsabhängigen Schnittstellen zu implementieren sind. Damit ergibt sich für die Realisierung der Systemprozesse in einer konkreten Fachanwendung für eine konkrete Realisierungs Umgebung ein Spezifikationsanteil, der in der folgenden Abbildung orange gekennzeichnet ist.

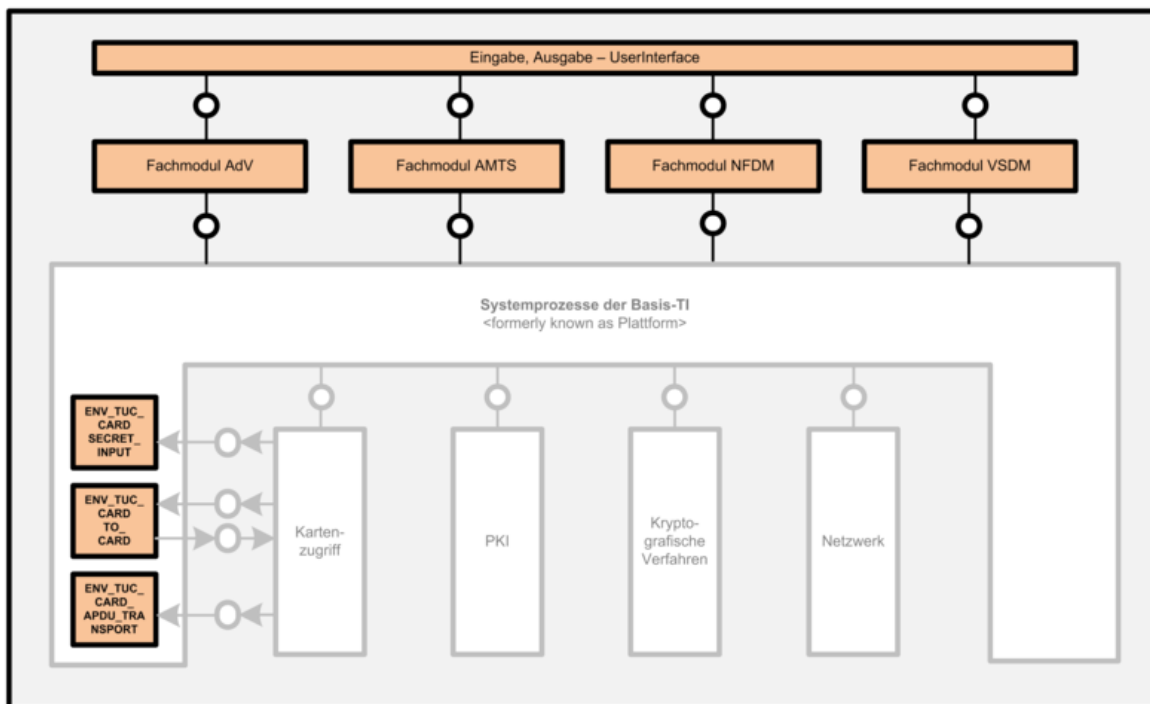


Abbildung 23: Umgebungsspezifische Operationen

## 10.1 Systemprozesse für den Zugriff auf Smartcards der TI

Der Zugriff auf Smartcards der TI wird durch einen CardProxy gemäß [gemSpec\_CardProxy] gekapselt. Dieser kommuniziert pro Instanz mit einer einzelnen eGK, SM-B, mit einem HBA oder einer anderen entsprechenden Karte. Der CardProxy stellt Anwendungen eine höherwertige Schnittstelle für den Zugriff auf eine Karte zur Verfügung und übersetzt die parametrisierbaren Operationen in kartenverständliche APDU-Sequenzen. Der CardProxy verwaltet intern den Freischaltstatus der Karte und organisiert bei technischer Notwendigkeit einer PIN-Eingabe oder Freischaltung durch eine weitere Karte auf Basis von Zugriffsregeln und dem aktuellen Freischaltzustand eines Artefakts auf der Karte.

Die Kommunikation mit dem CardProxy wird durch die hier beschriebenen Plattformbausteine gekapselt. Die Plattformbausteine leiten die Aufrufe an den CardProxy weiter der zum einen eine höherwertige Kartenoperationen als *cardOperation* bereitstellt und zum anderen eine direkte, bei Bedarf auf eine verschlüsselte, Kommunikation mit der Karte über *APDU*-Sequenzen erlaubt. In der Schnittstelle zur *cardOperation* sind sämtliche kartenspezifischen Aspekte gekapselt, jede Aktion auf und mit der Karte wird auf die jeweils angegebenen Rückgabewerte abgebildet. In der direkten Kommunikation



über einen transparenten Kanal erfolgt keine Auswertung der zur und von der Karte übertragenen APDU-Kommandos.

### 10.1.1 Die Realisierungsumgebung des CardProxy

Der CardProxy benötigt einen Zugriff auf Umgebungsschnittstellen, die je nach Einsatzumgebung der Karten unterschiedlich ausgeprägt sind. Der CardProxy benötigt eine Transportschnittstelle der physischen Anbindung zur Karte, einen Kommunikationskanal zu einem Remote-CardProxy mit einer zweiten Karte für eine Freischaltung nach dem Zwei-Schlüssel-Prinzip (Card-2-Card) und eine Schnittstelle zur Eingabe eines PIN-Geheimnisses.

#### 10.1.1.1 ENV\_TUC\_CARD\_SECRET\_INPUT – Realisierung Eingabe PIN-Geheimnis

Das System zur Umsetzung der Plattformleistungen zur Anbindung der Karte muss für seine konkrete Realisierungsumgebung festlegen, wie PIN- bzw. PUK-Geheimnisse von einem Benutzerinterface an die Karte gelangen.

##### TIP1-A\_6889 - Eingabeschnittstelle für PIN

Das System zur Umsetzung der Plattformleistungen PL\_TUC\_CARD\_\* MUSS eine Eingabeschnittstelle definieren, mittels der die Eingabe eines PIN-Geheimnisses an der Schnittstelle CardProxy und Kartenterminal gemäß [gemSpec\_CardProxy#Schnittstelle CardProxy und Kartenleser] übergeben wird.[<=]

##### TIP1-A\_6890 - Eingabeschnittstelle für PUK

Das System zur Umsetzung der Plattformleistungen PL\_TUC\_CARD\_\* MUSS eine Eingabeschnittstelle definieren, mittels der die Eingabe eines PUK-Geheimnisses an der Schnittstelle CardProxy und Kartenterminal gemäß [gemSpec\_CardProxy#Schnittstelle CardProxy und Kartenleser] übergeben wird.[<=]

##### TIP1-A\_6891 - Eingabeschnittstelle für newPIN

Das System zur Umsetzung der Plattformleistungen PL\_TUC\_CARD\_\* MUSS eine Eingabeschnittstelle definieren, mittels der die Eingabe eines neuen PIN-Geheimnisses an der Schnittstelle CardProxy und Kartenterminal gemäß [gemSpec\_CardProxy#Schnittstelle CardProxy und Kartenleser] übergeben wird.[<=]

##### TIP1-A\_7017 - Statusinformationen im Rahmen der PIN-Verifikation

Produkttypen und Dienste der TI die eine PIN/PUK-Eingabe mittels ENV\_TUC\_CARD\_SECRET\_INPUT umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy#Sicherheitszustand] zurückmelden:

1. ErrorUserVerification „Fehler im Authentisierungsprotokoll“
2. OK „Sicherheitszustand passend gesetzt“

[<=]

#### 10.1.1.2 ENV\_TUC\_CARD\_TO\_CARD – Realisierung Card-2-Card

Das System zur Umsetzung der Plattformleistungen zur Anbindung der Karte muss für seine konkrete Realisierungsumgebung festlegen, wie der Datentransport innerhalb einer Card-2-Card-Freischaltung zwischen zwei beteiligten Karten erfolgt.

##### TIP1-A\_6892 - Umgebungsschnittstelle für Card-2-Card

Das System zur Umsetzung der Plattformleistungen PL\_TUC\_CARD\_\* MUSS eine Transportschnittstelle „Umgebung“ definieren, mittels welcher der Datenaustausch von Challenge und Response im Card-2-Card-Verfahren zwischen zwei CardProxy-Instanzen

von CardProxy\_A an CardProxy\_B gemäß  
[gemSpec\_CardProxy#Sicherheitszustand#Card-2-Card] realisiert wird.[<=]

#### **TIP1-A\_7018 - Statusinformationen im Rahmen von Card-2-Card**

Produkttypen und Dienste der TI die eine Card-2-Card-Freischaltung mittels  
ENV\_TUC\_CARD\_TO\_CARD umsetzen, MÜSSEN das Ergebnis gemäß  
[gemSpec\_CardProxy#Sicherheitszustand] zurückmelden:

1. ErrorAuthentication „Fehler im Authentisierungsprotokoll“
2. ErrorImportCVC „Fehler im CV-Zertifikatimport“
3. OK „Sicherheitszustand passend gesetzt“
4. WrongEndEntityCVC „Das End-Entity-CV-Zertifikat enthält nicht die Rechte,  
die nötig sind um die Aktion freizuschalten“

[<=]

#### **10.1.1.3 ENV\_TUC\_CARD\_APDU\_TRANSPORT – Realisierung APDU-Transport**

Das System zur Umsetzung der Plattformleistungen zur Anbindung der Karte muss für  
seine konkrete Realisierungsumgebung festlegen, wie die elektrische Schnittstelle  
zwischen CardProxy und Karte als Kartenkontaktiereinheit IFD realisiert wird.

#### **TIP1-A\_6893 - Umgebungsschnittstelle für Kartenkommandos**

Das System zur Umsetzung der Plattformleistungen PL\_TUC\_CARD\_\* MUSS eine  
Schnittstelle realisieren, mittels welcher der Transport der APDU-Kommandos zwischen  
CardProxy und Karte gemäß [gemSpec\_CardProxy Konzept der Komponente  
Kartenterminal Proxy] über eine Kartenkontaktiereinheit gemäß [ISO7816-3] realisiert  
wird.[<=]

### **10.1.2 Konfiguration und Statusinformationen**

Um die korrekte Funktionsweise einer CardProxy-Instanz in einer konkreten  
Realisierungsumgebung sicherzustellen, ist eine Konfiguration und Initialisierung des  
CardProxies erforderlich. Es muss festgelegt werden, welchen Kartentyp eine jeweilige  
CardProxy-Instanz unterstützen soll und welche Operation auf welchen Objekten der  
jeweiligen Karte in einer Anwendung zulässig sind.

#### **10.1.2.1 Konfiguration des CardProxy**

##### **TIP1-A\_6894 - Konfiguration des Kartenzugriffs**

Das System zur Umsetzung der Kartenzugriffe mittels CardProxy MUSS für seine  
Realisierungsumgebung eine Konfigurationstabelle gemäß  
[gemSpec\_CardProxy#Konfigurationstabelle CardProxy] für jeden unterstützten  
Kartentyp einer SmartCard der TI definieren.[<=]

Die Konfigurationstabelle legt die zulässigen Operationen für jeden unterstützten  
Kartentyp in einer konkreten Realisierungsumgebung fest. Um eine Eindeutigkeit in der  
Auswahl einer passenden Zugriffsregel eines Objektes auf der Karte zu erhalten, muss  
der Nutzer der Plattformleistung festlegen, in welchen Rollen ein Akteur in  
Anwendungsfällen mit Bezug zu einer Karte der TI interagieren kann.

##### **TIP1-A\_7019 - Konfiguration der Rollen des Benutzers einer Karte**

Das System zur Umsetzung der Plattformleistungen für Systemprozesse der TI-Plattform  
MUSS für seine Realisierungsumgebung festlegen, welche Rollen ein Benutzer in  
Anwendungsfällen mit Bezug auf eine Karte der TI einnehmen darf.[<=]

**TIP1-A\_6895 - Festlegung des Zugriffsprofils zur Rollenauthentisierung gegenüber einer eGK**

Das System zur Umsetzung der Plattformleistungen für Systemprozesse der TI-Plattform MUSS festlegen, welche Zugriffe eine SmartCard (HBA, SM-B) bei der Rollenauthentisierung gegenüber einer eGK in seiner konkreten Realisierungsumgebung freischalten darf. [≤]

Mit dieser Anforderung wird sichergestellt, dass die zum Einsatz kommenden Karten über die entsprechenden Zertifikate zur Rollenauthentisierung gegenüber einer eGK verfügen. Diese Rollen bilden Zugriffsrechte auf der eGK ab, die in der Konfigurationstabelle für den CardProxy verzeichnet sind.

**10.1.2.2 Initialisierung CardProxy für eGK**

Bei der Initialisierung des CardProxy in dessen Zugriff sich eine eGK befindet, soll die komplette CV-Zertifikatskette einer in der Realisierungsumgebung vorgehaltenen SM-B, die für die Freischaltung der eGK vorgesehen ist, übergeben werden. Daraus ergibt sich, dass die in der Realisierungsumgebung eingesetzte SM-B bereits über einen initialisierten CardProxy adressiert werden kann. Die Instanz des CardProxy mit eGK muss mit der Referenz der SM-B der übergebenen SM-B-CV-Zertifikatskette und dem bei der Initialisierung des SM-B-CardProxy ausgelesenen X.509-AUT-Zertifikats assoziiert werden.

**TIP1-A\_6896 - Initialisierung CardProxy für eGK**

Das System zur Umsetzung der Plattformleistungen für Systemprozesse der TI-Plattform MUSS bei der Initialisierung des CardProxies mit Zugriff auf eine eGK

- die gesamte CV-Zertifikatskette einer für die Freischaltung vorgesehenen SM-B-Identität der Realisierungsumgebung an den eGK-CardProxy übergeben
- die vorgesehene SM-B mit diesem eGK-CardProxy für die Dauer des Zugriffs auf die eGK assoziieren und zu dieser Verbindung das C.HCI.AUT-Zertifikat der SM-B temporär speichern.
- die in PL\_TUC\_CARD\_INFORMATION gelisteten Informationen zu dieser Karte mittels CardProxy aus der Karte auslesen.

[≤]

**10.1.2.3 Initialisierung CardProxy für SM-B**

Bei der Initialisierung des CardProxy in dessen Zugriff sich eine SM-B befindet, soll die SM-B mittels PIN-Eingabe freigeschaltet werden sowie das CV- und das X.509-AUT-Zertifikat ausgelesen werden.

**TIP1-A\_6897 - Initialisierung CardProxy für SM-B**

Das System zur Umsetzung der Plattformleistungen für Systemprozesse der TI-Plattform MUSS bei der Initialisierung des CardProxies mit Zugriff auf eine SM-B

- eine Benutzerverifikation durchführen mittels PL\_TUC\_CARD\_VERIFY\_PIN und dem IDENTIFIKATOR *PIN.SMC* gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy für SMC-B]
- die in PL\_TUC\_CARD\_INFORMATION gelisteten Informationen zu Karte mittels CardProxy aus der Karte auslesen
- das CV-CA-Zertifikat zum C.SMC.AUTR\_CVC-Zertifikat der im Zugriff befindlichen SM-B und sofern vorhanden alle dazugehörigen Cross-Zertifikate der CVC-Root aus der TSL auslesen.

[≤]

#### 10.1.2.4 PL\_TUC\_CARD\_INFORMATION – Gesammelte Statusinformationen zu einer Karte

Der Systemprozess PL\_TUC\_CARD\_INFORMATION sammelt Statusinformationen zu einer SmartCard, die über eine umgebungsspezifische Schnittstelle an das System angebundene wird und stellt diese zum Abruf durch andere Systemprozesse bereit. Die Informationen umfassen zum einen Auskünfte über Kartentyp und Kartengeneration bzw. –version und zum anderen Statusinformationen über auf der Karte vorhandene Anwendungen und PINs.

##### TIP1-A\_6898 - Leistung zu Statusinformationen zu einer Karte

Produkttypen und Dienste der TI mit Zugriff auf Smartcards der TI MÜSSEN eine Plattformleistung PL\_TUC\_CARD\_INFORMATION realisieren und mit Statusinformationen einer SmartCard befüllen, die über die Umgebungsschnittstelle ENV\_TUC\_CARD\_APDU\_TRANSPORT mit dem System verbunden wird.[<=]

##### TIP1-A\_6899 - Liste verfügbarer Informationen zu einer SmartCard

Produkttypen und Dienste der TI die eine Plattformleistung PL\_TUC\_CARD\_INFORMATION umsetzen, MÜSSEN die folgenden Informationen zum Status einer angebotenen SmartCard sammeln, bei Änderung aktualisieren und für die Dauer der Verbindung zu dieser SmartCard zum Abruf bereitstellen.

Statusdatum	
<ul style="list-style-type: none"> <li>• Kartentyp</li> <li>• ICCSN</li> <li>• Produkttypversion des COS</li> <li>• Produkttypversion des Objektsystems</li> <li>• Echtheit der Karte</li> </ul>	Diese Informationen werden vom CardProxy bei der Initialisierung der Karte selbstständig erfasst
Informationen bei Kartentyp = eGK	
Status der Anwendungen auf der eGK: <ul style="list-style-type: none"> <li>• DF.HCA</li> <li>• DF.AMTS</li> <li>• DF.NFD</li> <li>• DF.DPE</li> </ul>	Aufruf der Cardproxy-cardOperation mit dem <i>Identifikator der Fachanwendung (siehe links)</i> gemäß [gemSpec_CardProxy#Konfigurationstabelle CardProxy eGK G2] und dem Aktionsparameter <i>SELECT</i> Abbildung der Rückgabewerte von cardOperation je Fachanwendung wie folgt: OK → AVAILABLE FileDeactivated → HIDDEN ObjectNotFound → ABSENT ObjectTerminated → TERMINATED

Status der PINs der eGK: <ul style="list-style-type: none"> <li>• PIN.CH</li> <li>• MRPIN.AMTS</li> <li>• PIN.AMTS_REP</li> <li>• MRPIN.NFD</li> <li>• MRPIN.DPE</li> </ul>	Aufruf der Cardproxy-cardOperation mit dem Identifikator der PIN (siehe links) gemäß [gemSpec_CardProxy#Konfigurationstabelle CardProxy eGK G2] und dem Aktionsparameter <i>GETSTATUS</i> Abbildung der Rückgabewerte von cardOperation je Fachanwendung wie folgt: PasswordProtected → TransportProtected PasswordDisabled → PasswordDisabled RetryCounter.0 → PasswordBlocked Wenn X > 0 RetryCounter.X → PasswordEnabledNotVerified.X OK → PasswordEnabledVerified
Authentisierungszertifikat der eGK C.CH.AUT	Auslesen des Zertifikats mittels PL_TUC_CARD_READ_FILE und dem IDENTIFIKATOR = EF.C.CH.AUT.R2048 oder IDENTIFIKATOR = EF.C.CH.AUT.E256, in Abhängigkeit des zum aktuellen Zeitpunkt PL_TUC_NET_SYNC_TIME zulässigen kryptografischen Verfahren gemäß [gemSpec_Krypt#2.1 Identitäten] gemäß [gemSpec_CardProxy#Konfigurationstabelle CardProxy eGK G2] Transformation der ausgelesenen Daten in die X.509-Zertifikatstruktur
Authentisierungszertifikat der eGK (pseudonymisiert) C.CH.AUTN	Auslesen des Zertifikats mittels PL_TUC_CARD_READ_FILE und dem IDENTIFIKATOR = EF.C.CH.AUTN.R2048 oder IDENTIFIKATOR = EF.C.CH.AUTN.E256, in Abhängigkeit des zum aktuellen Zeitpunkt PL_TUC_NET_SYNC_TIME zulässigen kryptografischen Verfahren gemäß [gemSpec_Krypt#2.1 Identitäten] gemäß [gemSpec_CardProxy#Konfigurationstabelle CardProxy eGK G2] Transformation der ausgelesenen Daten in die X.509-Zertifikatstruktur

Verschlüsselungszertifikat der eGK für elektronische Dokumente C.CH.ENC	Auslesen des Zertifikats mittels PL_TUC_CARD_READ_FILE und dem IDENTIFIKATOR = EF.C.CH.ENC.R2048 oder IDENTIFIKATOR = EF.C.CH.ENC.E256, in Abhängigkeit des zum aktuellen Zeitpunkt PL_TUC_NET_SYNC_TIME zulässigen kryptografischen Verfahren gemäß [gemSpec_Krypt#2.1 Identitäten] gemäß [gemSpec_CardProxy#Konfigurationstabelle CardProxy eGK G2] Transformation der ausgelesenen Daten in die X.509-Zertifikatstruktur
Verschlüsselungszertifikat der eGK für elektronische Verordnungen C.CH.ENCV	Auslesen des Zertifikats mittels PL_TUC_CARD_READ_FILE und dem IDENTIFIKATOR = EF.C.CH.ENCV.R2048 oder IDENTIFIKATOR = EF.C.CH.ENCV.E256, in Abhängigkeit des zum aktuellen Zeitpunkt PL_TUC_NET_SYNC_TIME zulässigen kryptografischen Verfahren gemäß [gemSpec_Krypt#2.1 Identitäten] gemäß [gemSpec_CardProxy#Konfigurationstabelle CardProxy eGK G2] Transformation der ausgelesenen Daten in die X.509-Zertifikatstruktur
<b>Informationen bei Kartentyp = SM-B</b>	
Status der PINs der SM-B PIN.SMC	Aufruf der Cardproxy-cardOperation mit dem <i>Identifikator der PIN</i> gemäß [gemSpec_CardProxy#Konfigurationstabelle CardProxy SMC-B] und dem Aktionsparameter <i>GETSTATUS</i> Abbildung der Rückgabewerte von <i>cardOperation</i> je Fachanwendung wie folgt: PasswordProtected → TransportProtected PasswordDisabled → PasswordDisabled RetryCounter.0 → PasswordBlocked Wenn X > 0 RetryCounter.X → PasswordEnabledNotVerified.X OK → PasswordEnabledVerified



Authentisierungszertifikat der SM-B gegenüber der eGK C.SMC.AUTR_CVC	Auslesen des Zertifikats EF.C.SMC.AUTR_CVC.R2048 oder EF.C.SMC.AUTR_CVC.E256 , in Abhängigkeit des zum aktuellen Zeitpunkt PL_TUC_NET_SYNC_TIME zulässigen kryptografischen Verfahren gemäß [gemSpec_Krypt#2.1 Identitäten] aus dem CV-CertificateStore des CardProxy gemäß [gemSpec_CardProxy#Bausteine innerhalb von CardProxy]
Authentisierungszertifikat der SM-B gegenüber der eGK für die PIN Status Prüfung C.SMC.NULL_CVC	Einlesen des Zertifikates vom Speicherort.
Authentisierungszertifikat der SM-B gegenüber Fachdiensten mit TLS C.HCI.AUT	Auslesen des Zertifikats mittels PL_TUC_CARD_READ_FILE und dem IDENTIFIKATOR = EF.C.HCI.AUT.R2048 oder IDENTIFIKATOR = EF.C.HCI.AUT.E256, in Abhängigkeit des zum aktuellen Zeitpunkt PL_TUC_NET_SYNC_TIME zulässigen kryptografischen Verfahren gemäß [gemSpec_Krypt#2.1 Identitäten] gemäß [gemSpec_CardProxy#Konfigurationstabelle CardProxy SMC-B] Transformation der ausgelesenen Daten in die X.509-Zertifikatstruktur
Zertifikat für einen lesbaren eGK-Protokolleintrag <optional vorhanden>	Auslesen des Zertifikats mittels PL_TUC_CARD_READ_FILE und dem IDENTIFIKATOR gemäß der Festlegung in [gemSpec_CardProxy#Konfigurationstabelle CardProxy SMC-B] und den Vorgaben zur Erzeugung eines Protokolleintrags auf der eGK Transformation der ausgelesenen Daten in die X.509-Zertifikatstruktur

[&lt;=]

#### 10.1.2.5 PL\_TUC\_EGK\_STATUS – Gültigkeit der eGK prüfen

Der Systemprozess PL\_TUC\_EGK\_STATUS fasst Leistungen verschiedener Domänen unter Einbeziehung einer elektronischen Gesundheitskarte zu einer höherwertigen Plattformleistung zusammen. Mit dieser wird eine Gültigkeitsprüfung der eGK durchgeführt, die zum einen Prüfschritte direkt auf der Karte durchführt und andererseits die Legitimität der Karte mittels Onlineabfrage beim Kartenherausgeber prüft.

#### TIP1-A\_6901 - Prüfkriterien der Gültigkeit der eGK

Produkttypen und Dienste der TI mit Zugriff auf eine elektronische Gesundheitskarte mittels CardProxy MÜSSEN eine Plattformleistung PL\_TUC\_EGK\_STATUS zur Prüfung des Status einer eGK umsetzen, die die eGK den folgenden Prüfkriterien unterzieht:

Prüfkriterium	Prüfergebnis
Abbildung des Werts zur Echtheit der Karte in <i>PL_TUC_CARD_INFORMATION.Echtheit</i> auf den Wahrheitswert <b>ja</b> wenn die Karte für echt befunden wurde, sonst <b>nein</b> .	Echtheit: <b>ja / nein</b>
Abbildung des Status der Gesundheitsanwendung auf der eGK in <i>PL_TUC_CARD_INFORMATION.DF.HCA</i> auf den Wert „ <b>aktiv</b> “, wenn Status = AVAILABLE „ <b>nicht aktiv</b> “, wenn Status ungleich AVAILABLE	Gesundheitsanwendung: <b>aktiv / nicht aktiv / Prüffehler</b>
Prüfung der Gültigkeit des Zertifikats der Karteninhaberidentität C.CH.AUTN der eGK aus <i>PL_TUC_CARD_INFORMATION</i> mittels <i>PL_TUC_PKI_VERIFY_CERTIFICATE</i> unter Verwendung der folgenden Parameter: <ul style="list-style-type: none"> <li>• Zu prüfendes Zertifikat: C.CH.AUTN</li> <li>• Referenzzeitpunkt: „jetzt“ (aktuelle gesetzliche Zeit)</li> <li>• PolicyList: &lt;oid_egk_autn&gt;</li> <li>• KeyUsage: „digitalSignature“</li> <li>• ExtendedKeyUsage: „id-kp-clientAuth“</li> <li>• OCSP-Graceperiod: NULL oder default</li> <li>• Offline-Modus: „nein“</li> <li>• OCSP-Response: NULL</li> <li>• Timeout: default</li> <li>• TOLERATE_OCSP_FAILURE: „ja“</li> </ul>	Gültigkeit zu Referenzzeitpunkt: <b>„zeitlich gültig / ungültig“ / Prüffehler</b>  Mathematische Gültigkeit: <b>„mathematisch gültig / ungültig“ / Prüffehler</b>  OCSP-Prüfung: <b>„Online gültig / Online gesperrt / nicht geprüft / Prüffehler“</b>

[<=]

#### TIP1-A\_6902 - Prüfergebnis der Echtheit und Gültigkeit der eGK

Produkttypen und Dienste der TI MÜSSEN zur Realisierung von PL\_EGK\_STATUS über das Ergebnis jedes Prüfkriteriums der Echtheit- und Gültigkeitsprüfung der eGK informieren und mit einem Status die erfolgreiche Prüfung aller Kriterien mitteilen.

- Echtheit => „**ja / nein / Prüffehler**“
- Gesundheitsanwendung => „**aktiv / nicht aktiv / Prüffehler**“
- Karteninhaberzertifikat => „**zeitlich gültig / ungültig / Prüffehler**“  
 „**mathematisch gültig / ungültig / Prüffehler**“  
 „**Online gültig / Online gesperrt / Onlinestatus unbekannt / Prüffehler**“

[<=]



### 10.1.2.6 PL\_TUC\_CARD\_RESET – Rücksetzen einer Karte

Mit dem Systemprozess PL\_TUC\_CARD\_RESET soll der logische Kanal einer im Zugriff eines CardProxy befindlichen SmartCard der TI auf den Initialisierungsstand zurückgesetzt werden.

#### TIP1-A\_7020 - Leistung zum Rücksetzen einer Karte

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Rücksetzen des logischen Kanals einer SmartCard als Plattformleistung PL\_TUC\_CARD\_RESET gemäß [gemSpec\_CardProxy] *cardOperation* mit dem Aktionsparameter *RESETCHANNEL* und dem IDENTIFIKATOR „\*“ (Wildcard) umsetzen und das Abschließen dieser Aktion mit dem Rückgabewert OK bestätigen.[<=]

### 10.1.3 Zugriff auf Smartcards der TI

Der folgende Abschnitt definiert Systemprozesse für den Zugriff auf Smartcards der TI als funktionale Abläufe. Voraussetzung für die korrekte Funktionsweise sind zum einen umgebungsspezifische Abläufe an den Außenschnittstellen, die von der jeweiligen Realisierungsumgebung festgelegt werden müssen. Zum anderen muss für die jeweils durch einen CardProxy adressierbaren Karten eine Konfigurationstabelle der zulässigen Kartenoperationen definiert werden.

#### 10.1.3.1 PL\_TUC\_CARD\_CHANGE\_PIN – PIN Ändern

Durch den Systemprozess PL\_TUC\_CARD\_CHANGE\_PIN wird das PIN-Geheimnis einer referenzierten PIN auf einer SmartCard der TI geändert.

##### TIP1-A\_6903 - Leistung zur Änderung einer PIN

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Ändern einer PIN auf einer SmartCard als Plattformleistung PL\_TUC\_CARD\_CHANGE\_PIN gemäß [gemSpec\_CardProxy] *cardOperation* für *Passwortobjekte* mit dem Aktionsparameter *CHANGE* umsetzen.[<=]

##### TIP1-A\_6904 - Aufrufparameter zum Ändern einer PIN

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_CHANGE\_PIN umsetzen, MÜSSEN vom Nutzenden den IDENTIFIKATOR des Passwortobjektes gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy] entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

##### TIP1-A\_6905 - Ergebnis der Änderung einer PIN

Produkttypen und Dienste der TI die eine Plattformleistung PL\_TUC\_CARD\_CHANGE\_PIN umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

- |                               |                               |
|-------------------------------|-------------------------------|
| 1. OK                         | „PIN erfolgreich geändert“    |
| 2. CardTerminated             | „Karte nicht mehr verwendbar“ |
| 3. MemoryFailure              | „Karte defekt“                |
| 4. ObjectNotFound             | „IDENTIFIKATOR ungültig“      |
| 5. PasswordBlocked            | „PIN gesperrt“                |
| 6. PasswordProtected          | „PIN mit Transportschutz“     |
| 7. SecurityStatusNotSatisfied | „Aktion nicht erlaubt“        |
| 8. WrongSecretWarning.X       | „PIN falsch, noch X Versuche“ |

9. WrongLength „neue PIN hat die falsche Länge“  
 [<=]

### 10.1.3.2 PL\_TUC\_CARD\_ENABLE\_PIN – PIN-Schutz einschalten

Mit dem Systemprozess PL\_TUC\_CARD\_ENABLE\_PIN wird die PIN-Verifikation der referenzierten PIN eingeschaltet.

#### TIP1-A\_6906 - Leistung zum Einschalten einer PIN

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Einschalten einer PIN auf einer SmartCard als Plattformleistung PL\_TUC\_CARD\_ENABLE\_PIN gemäß [gemSpec\_CardProxy] *cardOperation* für *Passwortobjekte* mit dem Aktionsparameter *ENABLE* umsetzen.[<=]

#### TIP1-A\_6907 - Aufrufparameter zum Einschalten einer PIN

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_ENABLE\_PIN umsetzen, MÜSSEN vom Nutzenden den *IDENTIFIKATOR* des Passwortobjektes gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy] entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

#### TIP1-A\_6908 - Ergebnis des Einschaltens einer PIN

Produkttypen und Dienste der TI die eine Plattformleistung PL\_TUC\_CARD\_ENABLE\_PIN umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK „PIN erfolgreich eingeschaltet“
2. CardTerminated „Karte nicht mehr verwendbar“
3. MemoryFailure „Karte defekt“
4. ObjectNotFound „IDENTIFIKATOR ungültig“
5. PasswordBlocked „PIN gesperrt“
6. PasswordProtected „PIN mit Transportschutz“
7. SecurityStatusNotSatisfied „Aktion nicht erlaubt“
8. WrongSecretWarning.X „PIN falsch, noch X Versuche“

[<=]

### 10.1.3.3 PL\_TUC\_CARD\_DISABLE\_PIN – PIN-Schutz abschalten

Mit dem Systemprozess PL\_TUC\_CARD\_DISABLE\_PIN wird die PIN-Verifikation einer referenzierten PIN abgeschaltet. Objekte auf einer SmartCard mit Zugriffsbedingungen, die die referenzierte PIN enthalten, sind bei abgeschalteter PIN weniger geschützt.

#### TIP1-A\_6909 - Leistung zum Abschalten einer PIN

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Abschalten einer PIN auf einer SmartCard als Plattformleistung PL\_TUC\_CARD\_DISABLE\_PIN gemäß [gemSpec\_CardProxy] *cardOperation* für *Passwortobjekte* mit dem Aktionsparameter *DISABLE* umsetzen.[<=]

#### TIP1-A\_6910 - Aufrufparameter zum Abschalten einer PIN

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_DISABLE\_PIN umsetzen, MÜSSEN vom Nutzenden den *IDENTIFIKATOR* des Passwortobjektes gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy] entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

**TIP1-A\_6911 - Ergebnis des Abschaltens einer PIN**

Produkttypen und Dienste der TI die eine Plattformleistung

PL\_TUC\_CARD\_DISABLE\_PIN umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

- |                               |                                |
|-------------------------------|--------------------------------|
| 1. OK                         | „PIN erfolgreich abgeschaltet“ |
| 2. CardTerminated             | „Karte nicht mehr verwendbar“  |
| 3. MemoryFailure              | „Karte defekt“                 |
| 4. ObjectNotFound             | „IDENTIFIKATOR ungültig“       |
| 5. PasswordBlocked            | „PIN gesperrt“                 |
| 6. PasswordProtected          | „PIN mit Transportschutz“      |
| 7. SecurityStatusNotSatisfied | „Aktion nicht erlaubt“         |
| 8. WrongSecretWarning.X       | „PIN falsch, noch X Versuche“  |

[<=]

**10.1.3.4 PL\_TUC\_CARD\_UNBLOCK\_PIN – PIN mit PUK entsperren**

Mit dem Systemprozess PL\_TUC\_CARD\_UNBLOCK\_PIN wird eine gesperrte PIN entsperrt. Das Entsperrn kann mit gleichzeitigem Setzen einer neuen PIN oder ohne das setzen einer neuen PIN erfolgen. Der Modus der Entsperrung erfolgt auf Grundlage der Festlegungen in der Konfiguration des CardProxies für einen bestimmten Kartentypen.

**TIP1-A\_6912 - Leistung zum Entsperrn einer PIN mittels PUK**

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Entsperrn einer PIN auf einer SmartCard als Plattformleistung

PL\_TUC\_CARD\_UNBLOCK\_PIN gemäß [gemSpec\_CardProxy] *cardOperation* für Passwortobjekte mit dem Aktionsparameter UNBLOCK umsetzen.[<=]

**TIP1-A\_6913 - Aufrufparameter zum Entsperrn einer PIN mittels PUK**

Produkttypen und Dienste der TI, die eine Plattformleistung

PL\_TUC\_CARD\_UNBLOCK\_PIN umsetzen, MÜSSEN vom Nutzenden den IDENTIFIKATOR des Passwortobjektes gemäß

[gemSpec\_CardProxy#Konfigurationstabelle CardProxy] entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

**TIP1-A\_6914 - Ergebnis der Entsperrung einer PIN mittels PUK**

Produkttypen und Dienste der TI die eine Plattformleistung

PL\_TUC\_CARD\_UNBLOCK\_PIN umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

- |                               |                                  |
|-------------------------------|----------------------------------|
| 1. OK                         | „PIN erfolgreich entsperrt“      |
| 2. CardTerminated             | „Karte nicht mehr verwendbar“    |
| 3. MemoryFailure              | „Karte defekt“                   |
| 4. ObjectNotFound             | „IDENTIFIKATOR ungültig“         |
| 5. PasswordBlocked            | „PUK gesperrt“                   |
| 6. PasswordProtected          | „PIN mit Transportschutz“        |
| 7. SecurityStatusNotSatisfied | „Aktion nicht erlaubt“           |
| 8. WrongSecretWarning.X       | „PUK falsch, noch X Versuche“    |
| 9. WrongLength                | „neue PIN hat die falsche Länge“ |

[<=]

#### 10.1.3.5 PL\_TUC\_CARD\_VERIFY\_PIN – Benutzer verifizieren

Der Systemprozess PL\_TUC\_CARD\_VERIFY\_PIN führt eine kartenbasierte Benutzerverifikation durch. Dazu wird auf einer SmartCard der TI eine PIN-Eingabe angestoßen, über die sich ein Benutzer als Besitzer des Kartengeheimnisses authentifiziert.

##### TIP1-A\_6915 - Leistung zur Benutzerverifikation

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN eine Benutzerverifikation mittels PIN als Plattformleistung PL\_TUC\_CARD\_VERIFY\_PIN gemäß [gemSpec\_CardProxy] *cardOperation für Passwortobjekte* mit dem Aktionsparameter *VERIFY* umsetzen.[<=]

##### TIP1-A\_6916 - Aufrufparameter der Benutzerverifikation

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_VERIFY\_PIN umsetzen, MÜSSEN vom Nutzenden den *IDENTIFIKATOR* des Passwortobjektes gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy] entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

##### TIP1-A\_6917 - Ergebnis der Leistung zur Eingabe einer PIN

Produkttypen und Dienste der TI die eine Plattformleistung PL\_TUC\_CARD\_VERIFY\_PIN umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK „PIN erfolgreich verifiziert“
2. PasswordBlocked „PIN gesperrt“
3. PasswordProtected „PIN mit Transportschutz“
4. SecurityStatusNotSatisfied „Aktion nicht erlaubt“
5. WrongSecretWarning.X „PIN falsch, noch X Versuche“
6. ObjectNotFound „IDENTIFIKATOR ungültig“
7. CardTerminated „Karte nicht mehr verwendbar“
8. MemoryFailure „Karte defekt“

[<=]

#### 10.1.3.6 PL\_TUC\_CARD\_ACTIVATE\_APPLICATION – Anwendung aktivieren

Der Systemprozess PL\_TUC\_CARD\_ACTIVATE\_APPLICATION schaltet eine verborgene Anwendung auf einer SmartCard sichtbar.

##### TIP1-A\_6918 - Leistung zum Aktivieren einer Anwendung

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Sichtbarmachen einer Anwendung auf einer SmartCard als Plattformleistung PL\_TUC\_CARD\_ACTIVATE\_APPLICATION gemäß [gemSpec\_CardProxy] *cardOperation für Ordner* mit dem Aktionsparameter *ACTIVATE* umsetzen.[<=]

##### TIP1-A\_6919 - Aufrufparameter zum Aktivieren einer Anwendung

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_ACTIVATE\_APPLICATION umsetzen, MÜSSEN vom Nutzenden den *IDENTIFIKATOR* der Anwendung gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy] entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

##### TIP1-A\_6920 - Ergebnis der Leistung zur Aktivieren einer Anwendung

Produkttypen und Dienste der TI die eine Plattformleistung PL\_TUC\_CARD\_ACTIVATE\_APPLICATION umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK „Anwendung erfolgreich aktiviert“
2. ObjectNotFound „IDENTIFIKATOR ungültig“
3. CardTerminated „Karte nicht mehr verwendbar“
4. MemoryFailure „Karte defekt“
5. ObjectTerminated „Objekt nicht mehr verwendbar“
6. SecurityStatusNotSatisfied „Aktion nicht erlaubt“
7. UpdateRetryWarning „Aktion erfolgreich, Speicher mglw. defekt“

[&lt;=]

#### 10.1.3.7 PL\_TUC\_CARD\_DEACTIVATE\_APPLICATION – Anwendung deaktivieren

Mit dem Systemprozess PL\_CAR\_DEACTIVATE\_APPLICATION wird eine Anwendung auf einer SmartCard verborgen.

##### TIP1-A\_6921 - Leistung zum Deaktivieren einer Anwendung

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Verbergen einer Anwendung auf einer SmartCard als Plattformleistung

PL\_TUC\_CARD\_DEACTIVATE\_APPLICATION gemäß [gemSpec\_CardProxy] *cardOperation* für Ordner mit dem Aktionsparameter DEACTIVATE umsetzen.[<=]

##### TIP1-A\_6922 - Aufrufparameter zum Deaktivieren einer Anwendung

Produkttypen und Dienste der TI, die eine Plattformleistung

PL\_TUC\_CARD\_DEACTIVATE\_APPLICATION umsetzen, MÜSSEN vom Nutzenden den IDENTIFIKATOR der Anwendung gemäß

[gemSpec\_CardProxy#Konfigurationstabelle CardProxy] entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

##### TIP1-A\_6923 - Ergebnis der Leistung zur Deaktivieren einer Anwendung

Produkttypen und Dienste der TI die eine Plattformleistung

PL\_TUC\_CARD\_DEACTIVATE\_APPLICATION umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK „Anwendung erfolgreich deaktiviert“
2. ObjectNotFound „IDENTIFIKATOR ungültig“
3. CardTerminated „Karte nicht mehr verwendbar“
4. MemoryFailure „Karte defekt“
5. ObjectTerminated „Objekt nicht mehr verwendbar“
6. SecurityStatusNotSatisfied „Aktion nicht erlaubt“
7. UpdateRetryWarning „Aktion erfolgreich, Speicher mglw. defekt“

[&lt;=]

#### 10.1.3.8 PL\_TUC\_CARD\_GET\_CHALLENGE – Auslesen einer Zufallszahl

Mit dem Systemprozess PL\_TUC\_CARD\_GET\_CHALLENGE kann eine Zufallszahl aus einer SmartCard ausgelesen werden. Ist die verwendete Karte eine elektronische Gesundheitskarte genügt die Qualität der Zufallszahl zur Ableitung ephemerer Schlüsselparameter.

##### TIP1-A\_6924 - Leistung zum Auslesen einer Zufallszahl

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das

Auslesen einer Zufallszahl von einer SmartCard als Plattformleistung

PL\_TUC\_CARD\_GET\_CHALLENGE gemäß [gemSpec\_CardProxy] *cardOperation* für



*Ordner* mit dem Aktionsparameter *GETRANDOM* und dem IDENTIFIKATOR „\*“ (Wildcard) umsetzen.[<=]

#### **TIP1-A\_6925 - Aufrufparameter für das Auslesen einer Zufallszahl**

Produkttypen und Dienste der TI, die eine Plattformleistung *PL\_TUC\_CARD\_GET\_CHALLENGE* umsetzen, MÜSSEN vom Nutzenden die Längenangabe *LENGTH* der auszulesenden Zufallszahl gemäß [gemSpec\_CardProxy] entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

#### **TIP1-A\_6926 - Ergebnis des Auslesens einer Zufallszahl**

Produkttypen und Dienste der TI die eine Plattformleistung *PL\_TUC\_CARD\_GET\_CHALLENGE* umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK + Daten                      „Aktion erfolgreich ausgeführt“

[<=]

### **10.1.3.9 PL\_TUC\_CARD\_READ\_FILE – Lesen von Daten aus einer SmartCard**

Mit dem Systemprozess *PL\_TUC\_CARD\_READ\_FILE* werden Daten aus einer transparenten Datei einer SmartCard gelesen. Über die Parameter Offset und Length kann gesteuert werden, ab welcher Position in der Datei eine festgelegte Anzahl Bytes gelesen werden. Fehlen diese Parameter, wird der komplette Dateiinhalt ausgelesen.

#### **TIP1-A\_6927 - Leistung zum Lesen einer Datei**

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Lesen des Inhalts einer Datei auf einer SmartCard als Plattformleistung *PL\_TUC\_CARD\_READ\_FILE* gemäß [gemSpec\_CardProxy] *cardOperation* für *transparente Elementary Files* mit dem Aktionsparameter *READ* umsetzen.[<=]

#### **TIP1-A\_6928 - Aufrufparameter für das Lesen einer Datei**

Produkttypen und Dienste der TI, die eine Plattformleistung *PL\_TUC\_CARD\_READ\_FILE* umsetzen, MÜSSEN vom Nutzenden den *IDENTIFIKATOR* der zu lesenden Datei gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy] entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

#### **TIP1-A\_6929 - Optionale Parameter für das Lesen einer Datei**

Produkttypen und Dienste der TI, die eine Plattformleistung *PL\_TUC\_CARD\_READ\_FILE* umsetzen, MÜSSEN die vom Nutzenden optional bereitgestellten Parameter *OFFSET* und *LENGTH* bei Vorhandensein entgegennehmen und diese in der Umsetzung von [gemSpec\_CardProxy] *cardOperation* verwenden, um die zu lesende Datenmenge zu beschränken.[<=]

#### **TIP1-A\_6930 - Ergebnis des Lesens des Inhalts einer Datei**

Produkttypen und Dienste der TI die eine Plattformleistung *PL\_TUC\_CARD\_READ\_FILE* umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK + Dateiinhalt                      „Daten wurden erfolgreich gelesen“
2. OffsetTooBig                      „OFFSET ungültig“
3. CorruptDataWarning + Dateiinhalt    „Daten gelesen, Speicher mglw. defekt“
4. ObjectNotFound                      „IDENTIFIKATOR ungültig“
5. CardTerminated                      „Karte nicht mehr verwendbar“
6. SecurityStatusNotSatisfied            „Aktion nicht erlaubt“

[<=]

### 10.1.3.10 PL\_TUC\_CARD\_WRITE\_FILE – Schreiben von Daten auf eine SmartCard

Mit dem Systemprozess PL\_TUC\_CARD\_WRITE\_FILE werden Binärdaten in eine transparente Datei einer SmartCard geschrieben. Die Schreiboperation fügt die neuen Daten an eventuell vorhandene Daten an.

#### TIP1-A\_6931 - Leistung zum Schreiben von Daten in eine transparente Datei

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Schreiben von Daten in eine transparente Datei auf einer SmartCard als Plattformleistung PL\_TUC\_CARD\_WRITE\_FILE gemäß [gemSpec\_CardProxy] *cardOperation für transparente Elementary Files* mit dem Aktionsparameter *UPDATE* und dem *OFFSET = 0* umsetzen.[<=]

#### TIP1-A\_6932 - Aufrufparameter für das Schreiben einer transparenten Datei

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_WRITE\_FILE umsetzen, MÜSSEN vom Nutzenden den *IDENTIFIKATOR* der zu schreibenden Datei gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy] sowie *NEWDATA* entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

#### TIP1-A\_6933 - Ergebnis des Schreibens von Datei in eine transparente Datei

Produkttypen und Dienste der TI die eine Plattformleistung PL\_TUC\_CARD\_WRITE\_FILE umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK „Daten erfolgreich geschrieben“
2. DataTooBig „Länge von NEWDATA ungültig“
3. MemoryFailure „Karte defekt“
4. ObjectNotFound „IDENTIFIKATOR ungültig“
5. CardTerminated „Karte nicht mehr verwendbar“
6. SecurityStatusNotSatisfied „Aktion nicht erlaubt“
7. UpdateRetryWarning „Daten geschrieben, Speicher mglw. defekt“

[<=]

### 10.1.3.11 PL\_TUC\_CARD\_UPDATE\_FILE – Aktualisieren von Daten in einer transparenten Datei einer SmartCard

Mit dem Systemprozess PL\_TUC\_CARD\_UPDATE\_FILE werden Binärdaten in eine transparente Datei einer SmartCard geschrieben, so dass vorhandene Daten überschrieben werden. Über den Parameter Offset kann gesteuert werden, ab welcher Position in der Datei die neuen Daten geschrieben werden. Fehlt dieser Parameter, beginnt die Schreiboperation am Anfang der Datei.

#### TIP1-A\_6934 - Leistung zum Aktualisieren von Daten in einer transparenten Datei

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Aktualisieren von Daten in einer transparenten Datei auf einer SmartCard als Plattformleistung PL\_TUC\_CARD\_UPDATE\_FILE gemäß [gemSpec\_CardProxy] *cardOperation für transparente Elementary Files* mit dem Aktionsparameter *UPDATE* umsetzen.[<=]

#### TIP1-A\_6935 - Aufrufparameter zum Aktualisieren von Daten in einer transparenten Datei

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_UPDATE\_FILE umsetzen, MÜSSEN vom Nutzenden den *IDENTIFIKATOR* der zu aktualisierenden Datei gemäß

[gemSpec\_CardProxy#Konfigurationstabelle CardProxy] sowie *NEWDATA* entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

#### **TIP1-A\_6936 - Optionaler Parameter für das Aktualisieren von Datei in einer transparenten Datei**

Produkttypen und Dienste der TI, die eine Plattformleistung *PL\_TUC\_CARD\_READ\_FILE* umsetzen, MÜSSEN den vom Nutzenden optional bereitgestellten Parameter *OFFSET* bei Vorhandensein entgegennehmen und diesen in der Umsetzung von [gemSpec\_CardProxy] *cardOperation* verwenden, um die Startposition der Schreiboperation innerhalb der Datei festzulegen.[<=]

#### **TIP1-A\_6937 - Ergebnis der Aktualisierung von Daten einer transparenten Datei**

Produkttypen und Dienste der TI die eine Plattformleistung *PL\_TUC\_CARD\_UDPATE\_FILE* umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK „Daten erfolgreich geschrieben“
2. DataTooBig „Länge von NEWDATA ungültig“
3. OffsetTooBig „OFFSET ungültig“
4. MemoryFailure „Karte defekt“
5. ObjectNotFound „IDENTIFIKATOR ungültig“
6. CardTerminated „Karte nicht mehr verwendbar“
7. SecurityStatusNotSatisfied „Aktion nicht erlaubt“
8. UpdateRetryWarning „Daten geschrieben, Speicher mglw. defekt“

[<=]

#### **10.1.3.12 PL\_TUC\_CARD\_DELETE\_FILE – Löschen von Daten auf einer SmartCard**

Der Systemprozess *PL\_TUC\_CARD\_DELETE\_FILE* entfernt eine transparente Datei auf einer SmartCard samt Dateinhalt. Die gelöschte Datei ist im Anschluss nicht mehr adressierbar.

#### **TIP1-A\_6938 - Leistung des Löschens einer transparenten Datei**

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Löschen einer transparenten Datei auf einer SmartCard als Plattformleistung *PL\_TUC\_CARD\_DELETE\_FILE* gemäß [gemSpec\_CardProxy] *cardOperation für transparente Elementary Files* mit dem Aktionsparameter *DELETE* umsetzen.[<=]

#### **TIP1-A\_6939 - Aufrufparameter zum Löschen einer transparenten Datei**

Produkttypen und Dienste der TI, die eine Plattformleistung *PL\_TUC\_CARD\_DELETE\_FILE* umsetzen, MÜSSEN vom Nutzenden den *IDENTIFIKATOR* der zu löschenden Datei gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy] entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

#### **TIP1-A\_6940 - Ergebnis der Löschoperation einer transparenten Datei**

Produkttypen und Dienste der TI die eine Plattformleistung *PL\_TUC\_CARD\_DELETE\_FILE* umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK „Datei erfolgreich gelöscht“
2. MemoryFailure „Karte defekt“
3. ObjectNotFound „IDENTIFIKATOR ungültig“



4. CardTerminated „Karte nicht mehr verwendbar“
5. SecurityStatusNotSatisfied „Aktion nicht erlaubt“
6. UpdateRetryWarning „Aktion erfolgreich, Speicher mglw. defekt“

[&lt;=]

#### 10.1.3.13 PL\_TUC\_CARD\_ERASE\_FILE – Rücksetzen des Inhalts einer transparenten Datei

Der Systemprozess PL\_TUC\_CARD\_ERASE\_FILE entfernt den Inhalt einer transparenten Datei. Die adressierte Datei ist weiterhin verwendbar.

##### TIP1-A\_6941 - Leistung zum Rücksetzen einer transparenten Datei

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Rücksetzen des Dateiinhalts einer transparenten Datei auf einer SmartCard als Plattformleistung PL\_TUC\_CARD\_ERASE\_FILE gemäß [gemSpec\_CardProxy] *cardOperation für transparente Elementary Files* mit dem Aktionsparameter *ERASE* umsetzen.[<=]

##### TIP1-A\_6942 - Aufrufparameter zum Rücksetzen einer transparenten Datei

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_ERASE\_FILE umsetzen, MÜSSEN vom Nutzenden den IDENTIFIKATOR der zurückzusetzenden Datei gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy] entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

##### TIP1-A\_6943 - Optionaler Parameter für das Rücksetzen des Inhalts einer transparenten Datei

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_ERASE\_FILE umsetzen, MÜSSEN den vom Nutzenden optional bereitgestellten Parameter *OFFSET* bei Vorhandensein entgegennehmen und dieses in der Umsetzung von [gemSpec\_CardProxy] *cardOperation* verwenden, um die Startposition der Operation innerhalb der Datei festzulegen.[<=]

##### TIP1-A\_6944 - Ergebnis des Rücksetzens einer transparenten Datei

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_ERASE\_FILE umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK „Daten erfolgreich gelöscht“
2. OffsetTooBig „OFFSET ungültig“
3. MemoryFailure „Karte defekt“
4. ObjectNotFound „IDENTIFIKATOR ungültig“
5. CardTerminated „Karte nicht mehr verwendbar“
6. SecurityStatusNotSatisfied „Aktion nicht erlaubt“
7. UpdateRetryWarning „Daten gelöscht, Speicher mglw. defekt“

[&lt;=]

#### 10.1.3.14 PL\_TUC\_CARD\_READ\_RECORD – Lesen von Daten aus einer strukturierten Datei

Mit dem Systemprozess PL\_TUC\_CARD\_READ\_RECORD werden Daten aus einer strukturierten Datei auf einer SmartCard ausgelesen. Über die optionale Angabe der *recordNumber* wird gesteuert, ob nur ein einzelner Record oder alle Records der strukturierten Datei gelesen werden sollen.

**TIP1-A\_6945 - Leistung zum Lesen einer strukturierten Datei**

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Lesen einer strukturierten Datei auf einer SmartCard als Plattformleistung PL\_TUC\_CARD\_READ\_RECORD gemäß [gemSpec\_CardProxy] *cardOperation für strukturierte Elementary Files* mit dem Aktionsparameter *READ* umsetzen.[<=]

**TIP1-A\_6946 - Aufrufparameter für das Lesen einer strukturierten Datei**

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_READ\_RECORD umsetzen, MÜSSEN vom Nutzenden den IDENTIFIKATOR der zu lesenden Datei gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy] entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

**TIP1-A\_6947 - Optionale Parameter für das Lesen einer strukturierten Datei**

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_READ\_RECORD umsetzen, MÜSSEN den vom Nutzenden optional bereitgestellten Parameter *RECORDNUMBER* bei Vorhandensein entgegennehmen und diese in der Umsetzung von [gemSpec\_CardProxy] *cardOperation* verwenden, um die zu lesende Datenmenge zu beschränken.[<=]

**TIP1-A\_6948 - Ergebnis des Lesens einer strukturierten Datei**

Produkttypen und Dienste der TI die die Plattformleistung PL\_TUC\_CARD\_READ\_RECORD umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK +Recordliste           „Daten wurden erfolgreich gelesen“
2. CorruptDataWarning +Recordliste   „Daten gelesen, Speicher mglw. defekt “
3. ObjectNotFound           „IDENTIFIKATOR ungültig“
4. RecordNotFound           „RECORDNUMBER ungültig“
5. RecordDeactivated       „Datensatz[RECORDNUMBER] deaktiviert“
6. CardTerminated          „Karte nicht mehr verwendbar“
7. SecurityStatusNotSatisfied   „Aktion nicht erlaubt“

[<=]

**10.1.3.15 PL\_TUC\_EGK\_READ\_PROTOCOL – Auslesen des Zugriffsprotokolls der eGK**

Mit dem Systemprozess PL\_TUC\_EGK\_READ\_PROTOCOL wird das gesamte Zugriffsprotokoll auf der elektronischen Gesundheitskarte ausgelesen. Im Gegensatz zur generischen Leseoperation eines strukturierten Elementary Files wird in diesem Baustein der Zugriff auf die Karte durch die Kartenzugriffsschicht CardProxy optimiert und es werden alle Log-Einträge (maximal 50) in einer Liste zurückgegeben.

**TIP1-A\_6949 - Leistung zum Lesen des Zugriffsprotokolls auf der eGK**

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Auslesen des Zugriffsprotokolls auf der eGK als Plattformleistung PL\_TUC\_EGK\_READ\_PROTOCOL gemäß [gemSpec\_CardProxy] *cardOperation für strukturiertes Elementary File* mit dem Aktionsparameter *READ* und dem IDENTIFIKATOR *EF.Logging* gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy eGK G2] umsetzen.[<=]

**TIP1-A\_6996 - Aufbereitung Zugriffsprotokolleinträge**

Produkttypen und Dienste der TI, die die Plattformleistung PL\_TUC\_EGK\_READ\_PROTOCOL umsetzen, MÜSSEN alle aus der Karte gelesenen, binär-codierten Zugriffsprotokolleinträge gemäß

[gemSpec\_Karten\_Fach\_TIP#Tab\_Karten\_Fach\_TIP\_010\_StrukturEF.Logging] in ein strukturiertes Format überführen und die Werte entsprechend des angegebenen Datentyps decodieren.[<=]

#### **TIP1-A\_6950 - Ergebnis des Auslesens des Zugriffsprotokolls der eGK**

Produkttypen und Dienste der TI, die die Plattformleistung

PL\_TUC\_EGK\_READ\_PROTOCOL umsetzen, MÜSSEN das Ergebnis gemäß

[gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK + Liste/Zugriffsprotokoll „Daten wurden erfolgreich gelesen“
2. CorruptDataWarning + Liste „Daten gelesen, Speicher mglw. defekt“
3. ObjectNotFound „IDENTIFIKATOR ungültig“
4. CardTerminated „Karte nicht mehr verwendbar“
5. SecurityStatusNotSatisfied „Aktion nicht erlaubt“

[<=]

#### **10.1.3.16 PL\_TUC\_CARD\_WRITE\_RECORD – Schreiben von Daten in eine strukturierte Datei**

Der Systemprozess PL\_TUC\_CARD\_WRITE\_RECORD schreibt einen Datensatz in einen Record einer strukturierten Datei auf einer SmartCard. Enthält der zu schreibende Record bereits Daten, wird der alte Datensatz mit dem neuen Wert überschrieben.

#### **TIP1-A\_6951 - Leistung zum Schreiben von Daten in eine strukturierte Datei**

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das

Schreiben eines Records einer strukturierten Datei auf einer SmartCard als

Plattformleistung PL\_TUC\_CARD\_WRITE\_RECORD gemäß [gemSpec\_CardProxy]

*cardOperation für strukturierte Elementary Files* mit dem Aktionsparameter *UPDATE* umsetzen.[<=]

#### **TIP1-A\_6952 - Aufrufparameter zum Schreiben von Daten in eine strukturierte Datei**

Produkttypen und Dienste der TI, die eine Plattformleistung

PL\_TUC\_CARD\_WRITE\_RECORD umsetzen, MÜSSEN vom Nutzenden den

*IDENTIFIKATOR* der zu aktualisierenden Datei gemäß

[gemSpec\_CardProxy#Konfigurationstabelle CardProxy], die *RECORDNUMBER* sowie *NEWDATA* entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

#### **TIP1-A\_6953 - Ergebnis der Schreiboperation in einer strukturierten Datei**

Produkttypen und Dienste der TI die die Plattformleistung

PL\_TUC\_CARD\_WRITE\_RECORD umsetzen, MÜSSEN das Ergebnis gemäß

[gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK „Datensatz erfolgreich geschrieben“
2. UpdateRetryWarning „Daten geschrieben, Speicher mglw. defekt“
3. WrongRecordLength „Länge von NEWDATA ungültig“
4. ObjectNotFound „IDENTIFIKATOR ungültig“
5. RecordNotFound „RECORDNUMBER ungültig“
6. RecordDeactivated „Datensatz[RECORDNUMBER] deaktiviert“
7. CardTerminated „Karte nicht mehr verwendbar“
8. SecurityStatusNotSatisfied „Aktion nicht erlaubt“
9. OutOfMemoryError „Speicherplatz in Zieldatei zu klein“
10. MemoryFailure „Karte defekt“
11. BufferTooSmall „Kartenkommando zu lang“

[&lt;=]

### 10.1.3.17 PL\_TUC\_CARD\_APPEND\_RECORD – Anfügen von Daten an eine strukturierte Datei

Mit dem Systemprozess PL\_TUC\_CARD\_APPEND\_RECORD wird ein Datensatz als neuer Record in einer strukturierten Datei an das Ende angefügt.

#### TIP1-A\_6954 - Leistung zum Anfügen von Daten in einer strukturierten Datei

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Anfügen eines Records in einer strukturierten Datei auf einer SmartCard als Plattformleistung PL\_TUC\_CARD\_APPEND\_RECORD gemäß [gemSpec\_CardProxy] *cardOperation für strukturierte Elementary Files* mit dem Aktionsparameter *APPEND* umsetzen.[<=]

#### TIP1-A\_6955 - Aufrufparameter zum Anfügen von Daten in einer strukturierten Datei

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_APPEND\_RECORD umsetzen, MÜSSEN vom Nutzenden den *IDENTIFIKATOR* der zu aktualisierenden Datei gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy] sowie *RECORDDATA* entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

#### TIP1-A\_6956 - Ergebnis der Anfügeoperation in einer strukturierten Datei

Produkttypen und Dienste der TI, die die Plattformleistung PL\_TUC\_CARD\_APPEND\_RECORD umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK „Datensatz erfolgreich angefügt“
2. UpdateRetryWarning „Daten angefügt, Speicher mglw. defekt“
3. WrongRecordLength „Länge von RECORDDATA ungültig“
4. ObjectNotFound „IDENTIFIKATOR ungültig“
5. FullRecordList „Kein zusätzlicher Record in Zieldatei zulässig“
6. CardTerminated „Karte nicht mehr verwendbar“
7. SecurityStatusNotSatisfied „Aktion nicht erlaubt“
8. OutOfMemoryError „Speicherplatz in Zieldatei zu klein“
9. MemoryFailure „Karte defekt“
10. BufferTooSmall „Kartenkommando zu lang“

[&lt;=]

### 10.1.3.18 PL\_TUC\_EGK\_APPEND\_PROTOCOL – Zugriff auf der eGK protokollieren

Mit dem Systemprozess PL\_TUC\_EGK\_APPEND\_PROTOCOL wird ein höherwertiger Baustein für das Schreiben eines Zugriffsprotokoll-Eintrags auf die eGK definiert. Nutzern dieser Plattformleistung genügt es, beim Aufruf den Identifikator der zu protokollierenden Fachanwendung mit der Art des durch die Fachanwendung erfolgten Zugriffs mitzuteilen. Der Systemprozess erzeugt aus diesen Daten zusammen mit den Angaben des Karteninhabers der SM-B-AUT-Identität, der diese eGK in einem Card-2-Card-Verfahren mit einem CV-Zertifikat freigeschaltet hat, einen Protokolldatensatz. Für das Protokollieren auf der eGK nutzt der Systemprozess die Schreiboperation des CardProxy der eGK.

#### TIP1-A\_6957 - Leistung zum Protokollieren des eGK-Zugriffs

Produkttypen und Dienste, welche Systemprozesse der TI mit Zugriff auf die eGK realisieren, MÜSSEN das Hinzufügen eines Protokolleintrags auf der eGK als Plattformleistung PL\_TUC\_EGK\_APPEND\_PROTOCOL umsetzen.[<=]

#### TIP1-A\_6958 - Aufrufparameter der Zugriffsprotokollierung

Produkttypen und Dienste der TI, die die Plattformleistung PL\_TUC\_EGK\_APPEND\_PROTOCOL umsetzen, MÜSSEN vom Nutzenden die Protokollparameter

1. DATATYPE [1 Byte] „Identifikator der Fachanwendung“
2. ACCESTYPE [1 Byte] „Identifikator der Zugriffsart“

entgegennehmen.[<=]

#### TIP1-A\_6959 - Hinzufügen eines Protokolleintrags auf die eGK

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_EGK\_APPEND\_PROTOCOL umsetzen, MÜSSEN die Schritte zum Hinzufügen eines Protokolleintrags auf der eGK in der angegebenen Reihenfolge durchführen:

	Teilschritt Hinzufügen eines Protokolleintrags	Teilergebnis
1	Auslesen des <code>commonName</code> , <code>surName</code> und <code>givenName</code> aus dem zur Erzeugung eines Protokolleintrags auf der eGK vorgesehenen Zertifikats in PL_TUC_CARD_INFORMATION, sofern vorhanden; alternativ: Auslesen des <code>commonName</code> , <code>surName</code> und <code>givenName</code> des C.HCI.AUT-Zertifikats in PL_TUC_CARD_INFORMATION der zur Initialisierung des eGK-CardProxy verwendeten SM-B-Identität gemäß [CommonPKI] und [gemSpec_PKI# Tab_PKI_229]	
2	Auslesen der ICCSN aus den Kartenstammdaten PL_TUC_CARD_INFORMATION der zur Initialisierung des eGK-CardProxy verwendeten SM-B-Identität	
3	Zusammenfügen der folgenden Informationen zu einem Protokolldatensatz gemäß [gem_Spec_Karten_Fach_TIP#4.1 – Tabelle 11: Tab_Karten_Fach_TIP_010_StrukturEF.Logging – Struktur der Rekords der Datei EF.Logging] <i>RECORDDATA</i> := Timestamp ("jetzt" aktuelle gesetzliche Zeit) + DATATYPE + ACCESTYPE + ICCSN + ActorName als [ <code>commonName</code>   ( <code>surname</code> , <code>givenname</code> )]	

4	Schreiben des Protokolleintrags auf die eGK mittels PL_TUC_CARD_APPEND_RECORD mit IDENTIFIKATOR = <i>EF.Logging</i> gemäß [gemSpec_CardProxy#Konfigurationstabelle CardProxy eGK G2] <i>RECORDDATA</i> = Protokolldatensatz aus Schritt 3	OK => <b>OK</b> UpdateRetryWarning WrongRecordLength ObjectNotFound FullRecordList CardTerminated SecurityStatusNotSatisfied OutOfMemoryError MemoryFailure BufferTooSmall NotEnoughMemorySpace => <b>Fehler</b>
5	Rückmeldung an den Nutzenden <b>OK</b> „Datensatz erfolgreich geschrieben“ <b>Fehler</b> „Keine passende Freischaltkarte oder eGK-Fehler“	

[&lt;=]

#### 10.1.3.19 PL\_TUC\_CARD\_DELETE\_RECORD – Löschen von Daten in einer strukturierten Datei

Mit dem Systemprozess PL\_TUC\_CARD\_DELETE\_RECORD wird ein einzelner Record einer strukturierten Datei oder werden alle Records einer strukturierten Datei auf einer SmartCard gelöscht. Beim Löschen eines einzelnen Records reduziert sich die Anzahl der Records in der strukturierten Datei um eins. Werden alle Records gelöscht, ist die Anzahl der Records nach erfolgreichem Abschluss der Operation null. Die strukturierte Datei ist weiterhin adressierbar.

##### TIP1-A\_6960 - Leistung zum Löschen von Daten in einer strukturierten Datei

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Löschen von Daten einer strukturierten Datei auf einer SmartCard als Plattformleistung PL\_TUC\_CARD\_DELETE\_RECORD gemäß [gemSpec\_CardProxy] *cardOperation für strukturierte Elementary Files* mit dem Aktionsparameter *DELETERECORD* umsetzen.[<=]

##### TIP1-A\_6961 - Aufrufparameter zum Löschen von Daten in einer strukturierten Datei

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_DELETE\_RECORD umsetzen, MÜSSEN vom Nutzenden den *IDENTIFIKATOR* der betroffenen Datei gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy] entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

##### TIP1-A\_6962 - Optionale Parameter für das Löschen von Daten einer strukturierten Datei

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_DELETE\_RECORD umsetzen, MÜSSEN den vom Nutzenden optional bereitgestellten Parameter *RECORDNUMBER* bei Vorhandensein entgegennehmen und



diese in der Umsetzung von [gemSpec\_CardProxy] *cardOperation* verwenden, um die zu löschende Datenmenge auf einen einzelnen Record zu beschränken.[<=]

#### **TIP1-A\_6963 - Ergebnis der Löschoperation in einer strukturierten Datei**

Produkttypen und Dienste der TI, die die Plattformleistung

PL\_TUC\_CARD\_DELETE\_RECORD umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK „Datensatz erfolgreich gelöscht“
2. UpdateRetryWarning „Daten gelöscht, Speicher mglw. defekt“
3. ObjectNotFound „IDENTIFIKATOR ungültig“
4. RecordNotFound „RECORDNUMBER ungültig“
5. RecordDeactivated „Datensatz[RECORDNUMBER] deaktiviert“
6. CardTerminated „Karte nicht mehr verwendbar“
7. SecurityStatusNotSatisfied „Aktion nicht erlaubt“
8. MemoryFailure „Karte defekt“

[<=]

#### **10.1.3.20 PL\_TUC\_CARD\_ERASE\_RECORD – Rücksetzen eines Datensatzes in einer strukturierten Datei**

Der Systemprozess PL\_TUC\_CARD\_ERASE\_RECORD löscht den Inhalt eines einzelnen der strukturierten Datei auf einer SmartCard. Der Record sowie die gesamte strukturierte Datei bleiben dabei erhalten. Der zurückgesetzte Record sowie die strukturierte Datei sind weiterhin adressierbar.

#### **TIP1-A\_6964 - Leistung zum Rücksetzen eines Datensatzes in einer strukturierten Datei**

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Rücksetzen eines Records einer strukturierten Datei auf einer SmartCard als Plattformleistung PL\_TUC\_CARD\_ERASE\_RECORD gemäß [gemSpec\_CardProxy] *cardOperation für strukturierte Elementary Files* mit dem Aktionsparameter *ERASE* umsetzen.[<=]

#### **TIP1-A\_6965 - Aufrufparameter zum Rücksetzen eines Datensatzes in einer strukturierten Datei**

Produkttypen und Dienste der TI, die eine Plattformleistung

PL\_TUC\_CARD\_ERASE\_RECORD umsetzen, MÜSSEN vom Nutzenden den

*IDENTIFIKATOR* der zu betroffenen strukturierten Datei gemäß

[gemSpec\_CardProxy#Konfigurationstabelle CardProxy] sowie die *RECORDNUMBER* des zurückzusetzenden Datensatzes entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

#### **TIP1-A\_6966 - Ergebnis des Rücksetzens eines Datensatzes in einer strukturierten Datei**

Produkttypen und Dienste der TI die die Plattformleistung

PL\_TUC\_CARD\_DELETE\_RECORD umsetzen, MÜSSEN das Ergebnis gemäß

[gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK „Datensatz erfolgreich zurückgesetzt“
2. UpdateRetryWarning „Daten zurückgesetzt, Speicher mglw. defekt“
3. ObjectNotFound „IDENTIFIKATOR ungültig“
4. RecordNotFound „RECORDNUMBER ungültig“
5. RecordDeactivated „Datensatz[RECORDNUMBER] deaktiviert“

- 6. CardTerminated „Karte nicht mehr verwendbar“
- 7. SecurityStatusNotSatisfied „Aktion nicht erlaubt“
- 8. MemoryFailure „Karte defekt“

[&lt;=]

#### 10.1.4 Transparenter Zugriff auf eine SmartCard

Mit dem Zugriff auf eine SmartCard über einen transparenten Kanal ist es möglich, von entfernter Stelle mit der Karte zu interagieren. Über den CardProxy werden Kartenkommandos direkt an die Karte weitergeleitet und deren Antwort-APDU zurückgegeben. Weder die kapselnden Systemprozesse noch CardProxy werten den Inhalt der an die Karte gesendeten und von dort empfangenen APDUs aus. Im speziellen Fall einer verschlüsselten Kommunikation (trusted channel) zwischen der Karte und einem Server in Card-to-Server-Kommunikation ist dies ohnehin nicht möglich.

##### 10.1.4.1 PL\_TUC\_CARD\_TC\_OPEN

Der Systemprozess PL\_TUC\_CARD\_TC\_OPEN öffnet einen transparenten Kommunikationskanal zu einer SmartCard. Mit der Nutzung dieses Plattformbausteins findet kein direkter Zugriff auf die Karte statt, es aktiviert in der Kartenzugriffsschicht eine exklusive Nutzung der Karte für diesen transparenten Kanal. Während dieser geöffnet ist, sind ausschließlich Aktionen mit den Systemprozessen PL\_TUC\_CARD\_TC\_SEND und \_CLOSE möglich.

##### TIP1-A\_6967 - Leistung zum Öffnen eines transparenten Kanals

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Öffnen eines transparenten Kanals zu einer SmartCard als Plattformleistung PL\_TUC\_CARD\_TC\_OPEN gemäß [gemSpec\_CardProxy] *Funktion transparentChannel* mit dem Aktionsparameter *OPEN* umsetzen.[<=]

##### TIP1-A\_6968 - Ergebnis des Öffnens eines transparenten Kanals

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_TC\_OPEN umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *Funktion transparentChannel* zurückmelden:

- 1. OK „Aktion erfolgreich ausgeführt“
- 2. TransparentChannelAlreadyOpen „Transparenter Kanal bereits offen“

[&lt;=]

##### 10.1.4.2 PL\_TUC\_CARD\_TC\_SEND

Mittels des Systemprozesses PL\_TUC\_CARD\_TC\_SEND wird ein Kartenkommando zu einer Karte weitergeleitet, ohne den Inhalt auszuwerten. Gelangt das Kartenkommando erfolgreich zur Karte wird immer das Response-Kommando der Karte zurückgegeben.

##### TIP1-A\_6969 - Leistung der transparenten Kommunikation zur Karte

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Senden von transparenten Kartenkommandos an eine SmartCard als Plattformleistung PL\_TUC\_CARD\_TC\_SEND gemäß [gemSpec\_CardProxy] *Funktion transparentChannel* mit dem Aktionsparameter *SENDAPDU* umsetzen.[<=]

##### TIP1-A\_6970 - Aufrufparameter zur transparenten Kommunikation zur Karte

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_CARD\_TC\_SEND umsetzen, MÜSSEN vom Nutzenden die *COMMANDAPDU*, welche an die Karte



weitergeleitet werden soll, entgegennehmen und in der Umsetzung der *Funktion transparentChannel* verwenden.[<=]

#### **TIP1-A\_6971 - Ergebnis der transparenten Kommunikation zur Karte**

Produkttypen und Dienste der TI die eine Plattformleistung PL\_TUC\_CARD\_TC\_SEND umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *Funktion transparentChannel* zurückmelden:

1. OK plus responseAPDU „Aktion erfolgreich ausgeführt“
2. MissingAPDU „Fehlendes Kartenkommando“
3. TransparentChannelNotOpen „Transparenter Kanal nicht offen“

[<=]

#### **10.1.4.3 PL\_TUC\_CARD\_TC\_CLOSE**

Der Systemprozess PL\_TUC\_CARD\_TC\_CLOSE schließt einen transparenten Kommunikationskanal zu einer SmartCard und gibt diese als Ressource für andere Plattformleistungen wieder frei. Mit der Nutzung dieses Plattformbausteins findet kein direkter Zugriff auf die Karte statt, es deaktiviert in der Kartenzugriffsschicht die exklusive Nutzung der Karte für diesen transparenten Kanal.

#### **TIP1-A\_6972 - Leistung zum Schließen eines transparenten Kanals**

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN das Schließen eines transparenten Kanals zu einer SmartCard als Plattformleistung PL\_TUC\_CARD\_TC\_CLOSE gemäß [gemSpec\_CardProxy] *Funktion transparentChannel* mit dem Aktionsparameter *CLOSE* umsetzen.[<=]

#### **TIP1-A\_6973 - Ergebnis des Schließens eines transparenten Kanals**

Produkttypen und Dienste der TI die eine Plattformleistung PL\_TUC\_CARD\_TC\_CLOSE umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *Funktion transparentChannel* zurückmelden:

1. OK „Aktion erfolgreich, Karte zurückgesetzt“
2. TransparentChannelNotOpen „Transparenter Kanal nicht offen“

[<=]

## **10.2 Kommunikation und Vernetzung**

### **10.2.1 PL\_TUC\_TLS\_SECURE\_CHANNEL – Kartenbasierte TLS-Verbindung**

Der Systemprozess PL\_TUC\_TLS\_SECURE\_CHANNEL baut eine verschlüsselte Verbindung von einem Clientsystem auf Basis einer Kartenidentität auf einer SmartCard der TI zu einem Zielsystem her. Dazu erfolgt eine **gegenseitige Authentisierung** zwischen dem Zielsystem und der verwendeten SmartCard und werden symmetrische Sitzungsschlüssel, für die verschlüsselte Kommunikation zwischen Client- und Zielsystem, ausgehandelt.

#### **TIP1-A\_6974 - Leistung zur kartenbasierten TLS-Verbindung**

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN eine Plattformleistung PL\_TUC\_TLS\_SECURE\_CHANNEL für den Aufbau einer kartenidentitätsbasierten TLS-Verbindung umsetzen.[<=]

#### **TIP1-A\_6975 - Aufrufparameter zur kartenbasierten TLS-Verbindung**

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_TLS\_SECURE\_CHANNEL umsetzen, MÜSSEN vom Nutzenden den *URI* des Zielsystems und den *ROLLENBEZEICHNER* der erwarteten Rolle des Zielsystems als Parameter entgegennehmen und diese im Verbindungsaufbau verwenden.[<=]

#### **TIP1-A\_6976 - Aufbau der kartenbasierten TLS-Verbindung**

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_TLS\_SECURE\_CHANNEL umsetzen, MÜSSEN die Schritte zum Aufbau einer kartenbasierten TLS-Verbindung in der angegebenen Reihenfolge durchführen:

	<b>Teilschritt kartenbasierter TLS-Verbindungsaufbau</b>	<b>Teilergebnis</b>
1	Auflösung des FQDN in der URI der Adresse des Zielsystems über PL_TUC_NET_NAME_RESOLUTION	Der FQDN kann nicht aufgelöst werden <b>=&gt; Fehler</b>

2	<p>Aufbau einer TLS-Verbindung vom Client- zum Zielsystem gemäß der Festlegungen des TLS-Protokolls in [RFC-5246] und den gematik-spezifischen Ergänzungen in [gemSpec_Krypt#TLS-Verbindungen]          Folgende zusätzliche Festlegungen gelten für den Verbindungsaufbau gemäß TLS-Protokoll in [RFC-5246]:</p> <ul style="list-style-type: none"> <li>Falls erforderlich, Auslesen einer Zufallszahl aus einer im Zugriff befindlichen Karte gemäß Systemprozess PL_TUC_CARD_GET_CHALLENGE</li> <li>Prüfung des vom Zielsystem bereitgestellten Serverzertifikat C.FD.TLS-S auf Gültigkeit mittels PL_TUC_PKI_VERIFY_CERTIFICATE mit folgenden Parametern:             <ul style="list-style-type: none"> <li>Zu prüfendes Zertifikat: C.FD.TLS-S</li> <li>Referenzzeitpunkt: „jetzt“ (aktuelle gesetzliche Zeit)</li> <li>PolicyList: oid_fd_tls_s</li> <li>KeyUsage: mindestens digitalSignature</li> <li>ExtendedKeyUsage: id-kp-serverAuth</li> <li>OCSP-Graceperiod: NULL oder default</li> <li>Offline-Modus: „nein“</li> <li>OCSP-Response NULL</li> <li>Timeout: default</li> <li>TOLERATE_OCSP_FAILURE: default</li> </ul> </li> <li>Wird vom Nutzenden ein ROLLENBEZEICHNER gemäß [gemSpec_OID] übergeben, Abgleich zwischen diesem und der von PL_TUC_PKI_VERIFY_CERTIFICATE zurückgegebenen Rolle des C.FD.TLS-S-Zertifikats des Zielsystems</li> <li>Clientauthentisierung gegenüber dem Zielsystem mit der Karteninhaberidentität C.HCI.AUT der SM-B-Identität aus PL_TUC_CARD_INFORMATION</li> <li>Signatur der ephemeren Schlüssel im TLS-Protokoll (Kontext: Diffie-Hellman Schlüssel signieren) mittels PL_TUC_SIGN_HASH_nonQES, dem IDENTIFIKATOR des privaten Schlüssels PrK.HCI.AUT des in PL_TUC_CARD_INFORMATION gespeicherten C.HCI.AUT-Zertifikats gemäß [gemSpec_CardProxy#Konfigurationstabelle CardProxy SMC-B] und dem gewählten kryptografischen Verfahren R2048 bzw. E256 sowie dem entsprechenden SIGNATURVERFAHREN</li> </ul>	<p>Ist das Zielsystem nicht erreichbar, schlägt der Verbindungsaufbau fehl =&gt; <b>Fehler</b>          Ist das Serverzertifikat gemäß TUC_PKI_018 <b>mathematisch</b> oder <b>zeitlich ungültig</b> oder meldet die erfolgreiche <b>Onlineprüfung</b> die <b>Sperrung</b> des Zertifikats („revoked“), wird der Verbindungsaufbau <b>wird abgelehnt</b>          =&gt; <b>Fehler</b>  <b>ROLLENBEZEICHNER und Rolle des Serverzertifikats</b> passen nicht zueinander, der Verbindungsaufbau wird abgelehnt          =&gt; <b>Fehler</b>          Gegenseitige Authentisierung fehlgeschlagen, Verbindungsaufbau abgebrochen          =&gt; <b>Fehler</b></p>
---	---	--

3	Rückmeldung an den Nutzenden <b>OK</b> „Verbindungsaufbau erfolgreich“ <b>Fehler</b> „Verbindungsaufbau nicht erfolgreich“	
---	--	--

[&lt;=]

### 10.2.2 PL\_TUC\_NET\_NAME\_RESOLUTION

Mit dem Systemprozess PL\_TUC\_NET\_NAME\_RESOLUTION wird ein URI einer Netzwerkkomponente der TI mittels des Namensdienstes der zentralen TI-Plattform in eine IP-Adresse aufgelöst.

#### TIP1-A\_6977 - Auflösen von URI in IP-Adresse

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, **SOLLEN** eine Auflösung von Netzwerk-URI in IP-Adresse als Plattformleistung PL\_TUC\_NET\_NAME\_RESOLUTION über die Schnittstelle I\_DNS\_Name\_Resolution zum TI-Namensdienst gemäß [gemSpec\_Net#Namensdienst] anbieten.[<=]

### 10.2.3 PL\_TUC\_NET\_SYNC\_TIME

Über den Systemprozess PL\_TUC\_NET\_SYNC\_TIME können sich Dienste und Komponenten der Telematikinfrastruktur mit dem Zeitserver der zentralen TI-Plattform synchronisieren.

#### TIP1-A\_6978 - Synchronisierung mit Zeitdienst

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, **MÜSSEN** eine Zeitsynchronisation als Plattformleistung PL\_TUC\_NET\_SYNC\_TIME über die Schnittstelle I\_NTP\_Time\_Informationen zum Zeitdienst der Telematikinfrastruktur gemäß [gemSpec\_Net#Zeitdienst] umsetzen und diese TI-Zeit als gültige, gesetzliche Zeit betrachten.[<=]

## 10.3 Vertraulichkeit, Authentizität, Integrität

### 10.3.1 PL\_TUC\_SIGN\_HASH\_nonQES – mit Karten-Identität signieren

Der Systemprozess PL\_TUC\_SIGN\_HASH\_nonQES versieht einen übergebenen Hash-Wert mit einer kartenbasierten digitalen nonQES Signatur. Dazu wird unter Verwendung der Karteninhaberidentität einer SmartCard der TI ein Binärwert von der entsprechenden Karte als Identitätsträger signiert.

#### TIP1-A\_6979 - Leistung der kartenbasierten elektronischen Signatur

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, **MÜSSEN** das Signieren eines Hashwertes mit einer Kartenidentität als Plattformleistung PL\_TUC\_SIGN\_HASH\_nonQES gemäß [gemSpec\_CardProxy] *cardOperation für private Schlüsselobjekte* umsetzen.[<=]

#### TIP1-A\_6980 - Aufrufparameter der kartenbasierten elektronischen Signatur

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_SIGN\_HASH\_nonQES umsetzen, **MÜSSEN** vom Nutzenden den *IDENTIFIKATOR* des privaten Schlüssels der Kartenidentität gemäß [gemSpec\_CardProxy#Konfigurationstabelle CardProxy], das SIGNATURVERFAHREN gemäß [gemSpec\_CardProxy] (RSASSA-PKCS1-v1\_5 oder ECDSA für TLS-

Authentisierung, RSASSA-PSS für SAML) als Aktionsparameter sowie den zu signierenden *HASHWERT* als Eingangsparameter entgegennehmen und in der Umsetzung von *cardOperation* verwenden.[<=]

#### **TIP1-A\_6981 - Ergebnis der kartenbasierten elektronischen Signatur**

Produkttypen und Dienste der TI die eine Plattformleistung

PL\_TUC\_SIGN\_HASH\_nonQES umsetzen, MÜSSEN das Ergebnis gemäß [gemSpec\_CardProxy] *cardOperation* zurückmelden:

1. OK + Hashsignatur „Signatur erfolgreich erstellt“
2. SecurityStatusNotSatisfied „Aktion nicht erlaubt“
3. ObjectNotFound „IDENTIFIKATOR ungültig“
4. KeyInvalid „Schlüsselobjekt nicht verwendbar“
5. CardTerminated „Karte nicht mehr verwendbar“
6. WrongToken „Übergabeparameter fehlerhaft“

[<=]

### **10.3.2 PL\_TUC\_HYBRID\_ENCIPHER – Hybrid verschlüsseln**

Der Systemprozess PL\_TUC\_HYBRID\_ENCIPHER führt eine hybride Verschlüsselung eines Dokuments durch. Dazu muss zunächst ein symmetrischer Schlüssel erzeugt werden, mit dem das Eingabedokument verschlüsselt wird. Dieser symmetrische Schlüssel wird anschließend mit dem öffentlichen Schlüsselmaterial des Dokumentenempfängers (bereitgestellt über ein X.509v3-Zertifikat) verschlüsselt und an das Dokument angefügt.

#### **TIP1-A\_6982 - Leistung zum hybriden Verschlüsseln**

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN eine Plattformleistung PL\_TUC\_HYBRID\_ENCIPHER zum hybriden Verschlüsseln eines Dokuments umsetzen.[<=]

#### **TIP1-A\_6983 - Aufrufparameter zum hybriden Verschlüsseln**

Produkttypen und Dienste der TI, die die Plattformleistung PL\_TUC\_HYBRID\_ENCIPHER umsetzen, MÜSSEN vom Nutzenden die Aufrufparameter

1. Doc „das zu verschlüsselnde Dokument“
2. Cert „das Empfänger-/Ziel-Zertifikat“

entgegennehmen.[<=]

#### **TIP1-A\_6984 - Ablauf der hybriden Verschlüsselung eines Dokuments**

Produkttypen und Dienste der TI, die eine Plattformleistung

PL\_TUC\_HYBRID\_ENCIPHER umsetzen, MÜSSEN die Schritte zum Verschlüsseln eines gegebenen Dokuments in der angegebenen Reihenfolge durchführen:

	Teilschritt der hybriden Verschlüsselung	Teilergebnis
1	Erzeugung eines symmetrischen Schlüssels gemäß BSI-TR-03116-1#3.5 Schlüsselerzeugung] und den Festlegungen in [gemSpec_Krypt#3.5.1 Hybride Verschlüsselung] ->S <sub>symm</sub>	Symmetrischer Schlüssel kann nicht erzeugt werden <b>=&gt; Fehler</b>

2	Dokument mit symmetrischem Schlüssel $S_{\text{symm}}$ verschlüsseln -> $\text{Doc}_{\text{enc}}$	
3	Schlüssel $S_{\text{symm}}$ mit öffentlichem Schlüssel $S_{\text{public}}$ der Empfängeridentität (liegt in Zertifikat Cert) verschlüsseln -> $(S_{\text{symm}})_{\text{enc}}$	
4	<p>Den verschlüsselten Dokumentenschlüssel und das verschlüsselte Dokument gemäß [RFC-5083] und [RFC-5084] zu einem CMS-Dokument [RFC-5652#6.1 EnvelopedData] zusammenfügen:  <math>\text{Doc}_{\text{enc}} + (S_{\text{symm}})_{\text{enc}} + \text{Attribute} \rightarrow D</math></p> <p>Bei Verschlüsselung des „content-encryption key“ wird „key transport“ verwendet</p> <p>Für den Empfänger wird eine KeyTransRecipientInfo erzeugt, für RecipientIdentifier wird die Option IssuerAndSerialNumber verwendet</p> <p>ContentType = OID {... authEnvelopedData}        = 1.2.840.113549.1.9.16.1.23</p>	
5	<p>Rückmeldung an den Aufrufenden, entweder</p> <ol style="list-style-type: none"> <li>1. OK + verschlüsseltes Dokument D, oder</li> <li>2. Fehler</li> </ol>	

[&lt;=]

### 10.3.3 PL\_TUC\_HYBRID\_DECIPHER – Hybrid entschlüsseln

Der Systemprozess PL\_TUC\_HYBRID\_DECIPHER entschlüsselt ein hybrid verschlüsseltes Dokument. Dazu wird zunächst der verschlüsselte Dokumentenschlüssel aus dem Eingabedokument extrahiert und mit einem privaten Schlüssel auf einer im Zugriff befindlichen SmartCard entschlüsselt. Mit diesem wiederhergestellten Dokumentenschlüssel wird anschließend das Dokument in einem symmetrischen Verfahren entschlüsselt.

#### TIP1-A\_6985 - Leistung zum hybriden Entschlüsseln

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN eine Plattformleistung PL\_TUC\_HYBRID\_DECIPHER zum hybriden Entschlüsseln eines Dokuments umsetzen.[<=]

#### TIP1-A\_6986 - Aufrufparameter zum hybriden Entschlüsseln

Produkttypen und Dienste der TI, die die Plattformleistung PL\_TUC\_HYBRID\_DECIPHER umsetzen, MÜSSEN vom Nutzenden den Aufrufparameter

1. D „das verschlüsselte Dokument“

entgegennehmen.[&lt;=]

#### TIP1-A\_6987 - Ablauf der hybriden Entschlüsselung eines Dokuments

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_HYBRID\_DECYPHER umsetzen, MÜSSEN die Schritte zum Entschlüsseln eines verschlüsselten Dokuments in der angegebenen Reihenfolge durchführen:

	Teilschritt der hybriden Entschlüsselung	Teilergebnis
1	<p>Einlesen der übergebenen Daten und Identifikation der verschiedenen Komponenten und Parameter gemäß [RFC-5652#6.1 EnvelopData]:  <math>D \rightarrow Doc_{enc} + (S_{symm})_{enc} + \text{Attribute}</math>, insbesondere werden die RecipientInfos als KeyTransRecipientInfo-Angaben benötigt</p>	<p>Verschlüsseltes Dokument, verschlüsselter Dokumentenschlüssel oder Empfängeridentität kann nicht bestimmt werden  <b>=&gt; Fehler</b></p>
2	<p>Entschlüsselung des Dokumentenschlüssels mittels CardProxy [gemSpec_CardProxy] <i>cardOperation für private Schlüsselobjekte</i> mit dem Aktionsparameter entweder</p> <ul style="list-style-type: none"> <li>• rsaDecipherOaep, oder</li> <li>• rsaDecipherPKCS1_V1_5</li> </ul> <p>entsprechend der Angabe des Schlüsselverschlüsselungsalgorithmus in [RFC-5652#6.2.1 KeyTransRecipientInfo::KeyEncryptionAlgorithmIdentifier] und dem Cryptogram als verschlüsselter Dokumentenschlüssel gemäß [RFC-5652#6.2.1 KeyTransRecipientInfo::EncryptedKey], welcher in der Liste der Dokumentenempfänger anhand der KeyTransRecipientIdentifier::IssuerAndSerialNumber des Empfänger-Zertifikats identifiziert wird          Das Empfängerzertifikat kann über IssuerAndSerialNumber gegen das ENC.Zertifikat in den Kartenstammdaten in PL_TUC_CARD_INFORMATION geprüft werden, der dazugehörige private Schlüssel muss gemäß [gemSpec_CardProxy#Konfigurationstabelle] als IDENTIFIKATOR übergeben werden  <math>(S_{symm})_{enc} \rightarrow S_{symm}</math></p>	<p>Auf der Karte befindet sich kein ENC.Zertifikat des angegebenen Empfängers mit zugehörigem privaten Schlüssel  <b>=&gt; Fehler</b></p>
3	<p>Dokument mit entschlüsseltem symmetrischem Schlüssel <math>S_{symm}</math> entschlüsseln  <math>Doc_{enc} \rightarrow Doc</math></p>	



4	Rückmeldung an den Aufrufenden, entweder <ol style="list-style-type: none"> <li>1. OK + unverschlüsseltes Dokument, oder</li> <li>2. Fehler</li> </ol>	
---	--	--

[&lt;=]

### 10.3.4 PL\_TUC\_SIGN\_DOCUMENT\_nonQES – Dokument signieren

Auf der eGK ist nach aktueller Spezifikationslage kein kryptografisches Schlüsselmaterial für eine Content-Signatur vorhanden.

## 10.4 Leistungen der PKI

### 10.4.1 PL\_TUC\_PKI\_VERIFY\_CERTIFICATE – Prüfung eines Zertifikats der TI

Der Systemprozess PL\_TUC\_PKI\_VERIFY\_CERTIFICATE kapselt die Prüfung eines X.509-Zertifikats der PKI der Telematikinfrastruktur. Es wird die zeitliche Gültigkeit zu einem Referenzzeitpunkt sowie die mathematische Gültigkeit geprüft. Zusätzlich kann via Parameter eine Online-Prüfung des Sperrstatus des Zertifikats verlangt werden.

#### TIP1-A\_6991 - Leistung zur Prüfung eines Zertifikats in der TI

Produkttypen und Dienste, welche Systemprozesse der TI realisieren, MÜSSEN eine Zertifikatsprüfung als Plattformleistung PL\_TUC\_PKI\_VERIFY\_CERTIFICATE gemäß [gemSpec\_PKI#TUC\_PKI\_018] umsetzen.[<=]

#### TIP1-A\_6992 - Aufrufparameter der Zertifikatsprüfung in der TI

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_PKI\_VERIFY\_CERTIFICATE umsetzen, MÜSSEN vom Nutzenden die folgenden Parameter entgegennehmen und in der Zertifikatsprüfung in TUC\_PKI\_018 verwenden:

1. Zu prüfendes Zertifikat      ein Zertifikat der PKI der TI
2. Referenzzeitpunkt          Prüfung auf Gültigkeit zu Referenzzeitpunkt
3. PolicyList                  zulässige Zertifikatstyp-OIDs
4. KeyUsage                  Anwendungsfall für kryptografisches Material
5. ExtendedKeyUsage      Anwendungsfall für kryptografisches Material
6. OCSP-Graceperiod      default: 10 Min
7. Offline-Modus            ja/nein (wenn nein, dann Prüfmodus: OCSP)
8. OCSP-Response          optional
9. Timeout:                  default: 10 Sek.
10. TOLERATE\_OCSP\_FAILURE:    ja/nein, default: „nein“

[&lt;=]

#### TIP1-A\_6993 - Ergebnis der Zertifikatsprüfung in der TI

Produkttypen und Dienste der TI, die eine Plattformleistung PL\_TUC\_PKI\_VERIFY\_CERTIFICATE umsetzen, MÜSSEN das Ergebnis jedes Prüfkriteriums und Fehler in der Zertifikatsprüfung in TUC\_PKI\_018 zurückmelden:



Gültigkeit zu Referenzzeitpunkt:	<b>„zeitlich gültig / ungültig / Prüffehler“</b>
Mathematische Gültigkeit:	<b>„mathematisch gültig / ungültig / Prüffehler“</b>
OCSP-Prüfung:	<b>„Online gültig / Online gesperrt / Onlinestatus unbekannt / Prüffehler“</b>

Fehler in der Verarbeitung beeinflussen die Prüfergebnisse des TUC\_PKI\_018 wie folgt:

1. CERT\_READ\_ERROR, das Zertifikat kann nicht geprüft werden
2. CA\_CERT\_MISSING oder AUTHORITYKEYID\_DIFFERENT, das Zertifikat darf nicht als gültig betrachtet werden, da kein gültiges Ausstellerzertifikat gefunden wurde.
3. OCSP\_CERT\_MISSING oder OCSP\_SIGNATURE\_ERROR, die Legitimität einer OCSP-Response kann nicht verifiziert werden, die OCSP-Prüfung muss abgebrochen werden und das Zertifikat ist nicht online-gültig
4. CERTHASH\_EXTENSION\_MISSING, CERTHASH\_MISMATCH, WARNING\_CERT\_UNKNOWN, die OCSP-Prüfung ist nicht erfolgreich und das Zertifikat ist nicht online-gültig

[<=]