

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

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation KTR-AdV

Version: 1.7.0 CC
Revision: 192694230737
Stand: 28.06.201930.04.2020
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_KTR-AdV

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	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
1.3.0	26.10.18		Einarbeitung Änderungsliste P15.10	gematik
	28.11.18		Einarbeitung Änderungsliste P15.11	gematik
1.4.0	18.12.18		Anh B - Leistungen der dezentralen TI-Plattform in eigenes Dokument [gemSpec_Systemprozesse_dezTI] ausgelagert	gematik
1.5.0	15.05.19		redaktionelle Anpassung (Referenzen auf AnhB), Einarbeitung Änderungsliste P18.1	gematik
1.6.0	28.06.19		Einarbeitung Änderungsliste P19.1	
1.7.0 CC	30.04.2020 28.06.19		freigegeben Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes	8
1.1 Zielsetzung	8
1.2 Zielgruppe	8
1.3 Geltungsbereich	8
1.4 Abgrenzungen	8
1.5 Methodik	9
2 Systemüberblick	10
2.1 Einordnung des Produkttyps in die Telematikinfrastruktur	10
2.2 Leistungen der TI-Plattform	11
3 Systemkontext	13
3.1 Akteure und Rollen	13
3.2 Nachbarsysteme	15
3.3 Ablaufumgebung	16
4 Zerlegung des Produkttyps	18
5 Übergreifende Festlegungen	22
5.1 Datenschutz und Sicherheit	22
5.1.1 Verarbeitung personenbezogener Daten	22
5.1.2 Absicherung der AdV-Komponenten	23
5.1.3 Verbindungsaufbau und Freischaltung eGK	25
5.1.4 Filterung von Kartenkommandos an die eGK	26
5.2 Logging	26
5.3 Nicht-funktionale Anforderungen	29
6 Funktionsmerkmale	30
6.1 Implementation der AdV-Anwendungsfälle	30
6.1.1 AdV-Sitzung des Versicherten	32
6.1.1.1 AdV-Sitzung initialisieren	32
6.1.1.2 AdV-Sitzung beenden	39
6.1.2 Übergreifende Vorbedingungen	39
6.1.3 Hinweistext zu Fachanwendung	42
6.1.4 Generische Anwendungsfälle	43
6.1.4.1 Anwendung auf eGK deaktivieren	43
6.1.4.2 Anwendung auf eGK reaktivieren	47
6.1.4.3 PIN-Verwaltung	51
6.1.4.3.1 PIN ändern	51
6.1.4.3.2 PIN auf eGK entsperren	54
6.1.4.3.3 PIN für Fachanwendung einschalten	57

67	6.1.4.3.4 PIN für Fachanwendung ausschalten.....	60
68	6.1.5 Verwaltung der eGK	64
69	6.1.5.1 VSD von eGK anzeigen.....	64
70	6.1.5.2 Zugriffsprotokoll anzeigen	67
71	6.1.5.3 Versicherten PIN ändern	70
72	6.1.5.4 Versicherten PIN entsperren	71
73	6.1.5.5 Datenübertragung bei Kartentausch	73
74	6.1.6 Verwaltung der NFD	80
75	6.1.6.1 NFD auf eGK verbergen.....	81
76	6.1.6.2 Verborgenen NFD auf eGK sichtbar machen	81
77	6.1.6.3 PIN für NFD einschalten	82
78	6.1.6.4 PIN für NFD ausschalten.....	83
79	6.1.7 Verwaltung des DPE	83
80	6.1.7.1 Persönliche Erklärung (DPE) von eGK anzeigen.....	83
81	6.1.7.2 Persönliche Erklärung (DPE) auf eGK ändern	86
82	6.1.7.3 Persönliche Erklärung (DPE) auf eGK löschen	90
83	6.1.7.4 PIN für DPE einschalten.....	93
84	6.1.7.5 PIN für DPE ausschalten.....	93
85	6.1.7.6 Persönliche Erklärung (DPE) auf eGK verbergen.....	94
86	6.1.7.7 Verborgene DPE auf eGK sichtbar machen	95
87	6.1.8 Verwaltung eMP/AMTS	96
88	6.1.8.1 AMTS Vertreter PIN ändern	96
89	6.1.8.2 AMTS Vertreter PIN entsperren.....	97
90	6.1.8.3 eMP/AMTS Datensatz verbergen.....	97
91	6.1.8.4 Verborgenen eMP/AMTS Datensatz sichtbar machen.....	98
92	6.1.8.5 PIN für AMTS einschalten	99
93	6.1.8.6 PIN für AMTS ausschalten.....	99
94	6.1.9 Fachanwendungsunabhängige Anwendungsfälle	100
95	6.1.9.1 Mit eGK verschlüsseln	100
96	6.1.9.2 Mit eGK entschlüsseln	103
97	6.1.9.3 Authentisierungsrequest mit eGK signieren	106
98	6.1.9.4 Zertifikat von eGK lesen	108
99	6.2 Realisierung der Leistungen der TI-Plattform.....	111
100	6.2.1 Transportschnittstelle für Kartenkommandos.....	112
101	6.2.1.1 Kartenterminals der Sicherheitsklasse 1.....	113
102	6.2.1.2 Kartenterminals der Sicherheitsklasse 2.....	113
103	6.2.1.3 Kartenterminals der Sicherheitsklasse 3.....	114
104	6.2.2 Schnittstelle für PIN-Operationen und Anbindung der Karten der TI.....	114
105	6.2.3 Schnittstelle zur Freischaltung der eGK	115
106	6.2.4 Schnittstelle zu Diensten der zentralen TI-Plattform	116
107	6.3 Schnittstelle zwischen AdV-App und AdV-Server.....	118
108	6.4 Identitäten der KTR-AdV	118
109	7 Informationsmodell	121
110	8 Verteilungssicht.....	122
111	9 Anhang A Verzeichnisse.....	123
112	9.1 Abkürzungen	123
113	9.2 Glossar	125

114	9.3 Abbildungsverzeichnis	125
115	9.4 Tabellenverzeichnis	126
116	9.5 Referenzierte Dokumente	130
117	9.5.1 Dokumente der gematik	130
118	9.5.2 Weitere Dokumente	131
119	9.6 Hinweistexte der Fachanwendungen	132
120	1 Einordnung des Dokumentes	8
121	1.1 Zielsetzung	8
122	1.2 Zielgruppe	8
123	1.3 Geltungsbereich	8
124	1.4 Abgrenzungen	8
125	1.5 Methodik	9
126	2 Systemüberblick	10
127	2.1 Einordnung des Produkttyps in die Telematikinfrastruktur	10
128	2.2 Leistungen der TI-Plattform	11
129	3 Systemkontext	13
130	3.1 Akteure und Rollen	13
131	3.2 Nachbarsysteme	15
132	3.3 Ablaufumgebung	16
133	4 Zerlegung des Produkttyps	18
134	5 Übergreifende Festlegungen	22
135	5.1 Datenschutz und Sicherheit	22
136	5.1.1 Verarbeitung personenbezogener Daten	22
137	5.1.2 Absicherung der Adv-Komponenten	23
138	5.1.3 Verbindungsaufbau und Freischaltung eGK	25
139	5.1.4 Filterung von Kartenkommandos an die eGK	26
140	5.2 Logging	26
141	5.3 Nicht-funktionale Anforderungen	29
142	6 Funktionsmerkmale	30
143	6.1 Implementation der Adv Anwendungsfälle	30
144	6.1.1 Adv-Sitzung des Versicherten	32
145	6.1.1.1 Adv-Sitzung initialisieren	32
146	6.1.1.2 Adv-Sitzung beenden	39
147	6.1.2 Übergreifende Vorbedingungen	39
148	6.1.3 Hinweistext zu Fachanwendung	42
149	6.1.4 Generische Anwendungsfälle	43
150	6.1.4.1 Anwendung auf eGK deaktivieren	43
151	6.1.4.2 Anwendung auf eGK reaktivieren	47
152	6.1.4.3 PIN-Verwaltung	51

153	6.1.4.3.1 PIN ändern	51
154	6.1.4.3.2 PIN auf eGK entsperren	54
155	6.1.4.3.3 PIN für Fachanwendung einschalten	57
156	6.1.4.3.4 PIN für Fachanwendung ausschalten.....	60
157	6.1.5 Verwaltung der eGK	64
158	6.1.5.1 VSD von eGK anzeigen.....	64
159	6.1.5.2 Zugriffsprotokoll anzeigen	67
160	6.1.5.3 Versicherten-PIN ändern	70
161	6.1.5.4 Versicherten-PIN entsperren	71
162	6.1.5.5 Datenübertragung bei Kartentausch	73
163	6.1.6 Verwaltung der NFD	80
164	6.1.6.1 NFD auf eGK verbergen.....	81
165	6.1.6.2 Verborgenen NFD auf eGK sichtbar machen	81
166	6.1.6.3 PIN für NFD einschalten	82
167	6.1.6.4 PIN für NFD ausschalten.....	83
168	6.1.7 Verwaltung des DPE	83
169	6.1.7.1 Persönliche Erklärung (DPE) von eGK anzeigen.....	83
170	6.1.7.2 Persönliche Erklärung (DPE) auf eGK ändern	86
171	6.1.7.3 Persönliche Erklärung (DPE) auf eGK löschen	90
172	6.1.7.4 PIN für DPE einschalten.....	93
173	6.1.7.5 PIN für DPE ausschalten	93
174	6.1.7.6 Persönliche Erklärung (DPE) auf eGK verbergen.....	94
175	6.1.7.7 Verborgene DPE auf eGK sichtbar machen	95
176	6.1.8 Verwaltung eMP/AMTS	96
177	6.1.8.1 AMTS-Vertreter-PIN ändern	96
178	6.1.8.2 AMTS-Vertreter-PIN entsperren	97
179	6.1.8.3 eMP/AMTS Datensatz verbergen	97
180	6.1.8.4 Verborgenen eMP/AMTS Datensatz sichtbar machen.....	98
181	6.1.8.5 PIN für AMTS einschalten	99
182	6.1.8.6 PIN für AMTS ausschalten.....	99
183	6.1.9 Fachanwendungsunabhängige Anwendungsfälle	100
184	6.1.9.1 Mit eGK verschlüsseln	100
185	6.1.9.2 Mit eGK entschlüsseln	103
186	6.1.9.3 Authentisierungsrequest mit eGK signieren	106
187	6.1.9.4 Zertifikat von eGK lesen	108
188	6.2 Realisierung der Leistungen der TI-Plattform.....	111
189	6.2.1 Transportschnittstelle für Kartenkommandos.....	112
190	6.2.1.1 Kartenterminals der Sicherheitsklasse 1.....	113
191	6.2.1.2 Kartenterminals der Sicherheitsklasse 2.....	113
192	6.2.1.3 Kartenterminals der Sicherheitsklasse 3.....	114
193	6.2.2 Schnittstelle für PIN-Operationen und Anbindung der Karten der TI.....	114
194	6.2.3 Schnittstelle zur Freischaltung der eGK	115
195	6.2.4 Schnittstelle zu Diensten der zentralen TI-Plattform	116
196	6.3 Schnittstelle zwischen AdV-App und AdV-Server	118
197	6.4 Identitäten der KTR-AdV	118
198	7 Informationsmodell	121
199	8 Verteilungssicht.....	122

9 Anhang A – Verzeichnisse	123
9.1 Abkürzungen	123
9.2 Glossar	125
9.3 Abbildungsverzeichnis.....	125
9.4 Tabellenverzeichnis	126
9.5 Referenzierte Dokumente.....	130
9.5.1 Dokumente der gematik.....	130
9.5.2 Weitere Dokumente.....	131
9.6 Hinweistexte der Fachanwendungen	132

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.

242 1.5 Methodik

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

247 Sie werden im Dokument wie folgt dargestellt:

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

249 Text / Beschreibung

250 [**<=**]

251

252 Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke angeführten
 253 Inhalte.

ENTWURF

2 Systemüberblick

2.1 Einordnung des Produkttyps in die Telematikinfrastruktur

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 Telematikinfrastruktur.

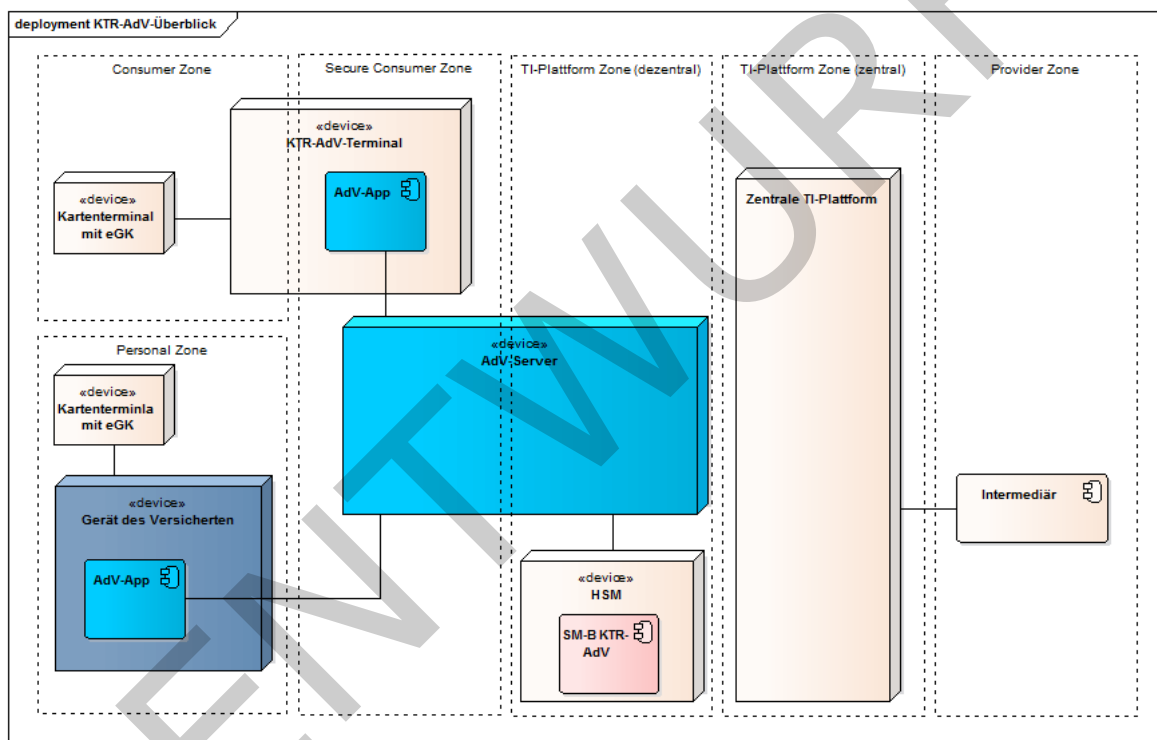


Abbildung 1: ABB_ADV_300 – Überblick AdV in einer Umgebung im Auftrag der Kostenträger

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 C.SMC.AUTR_CVC.E256 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.

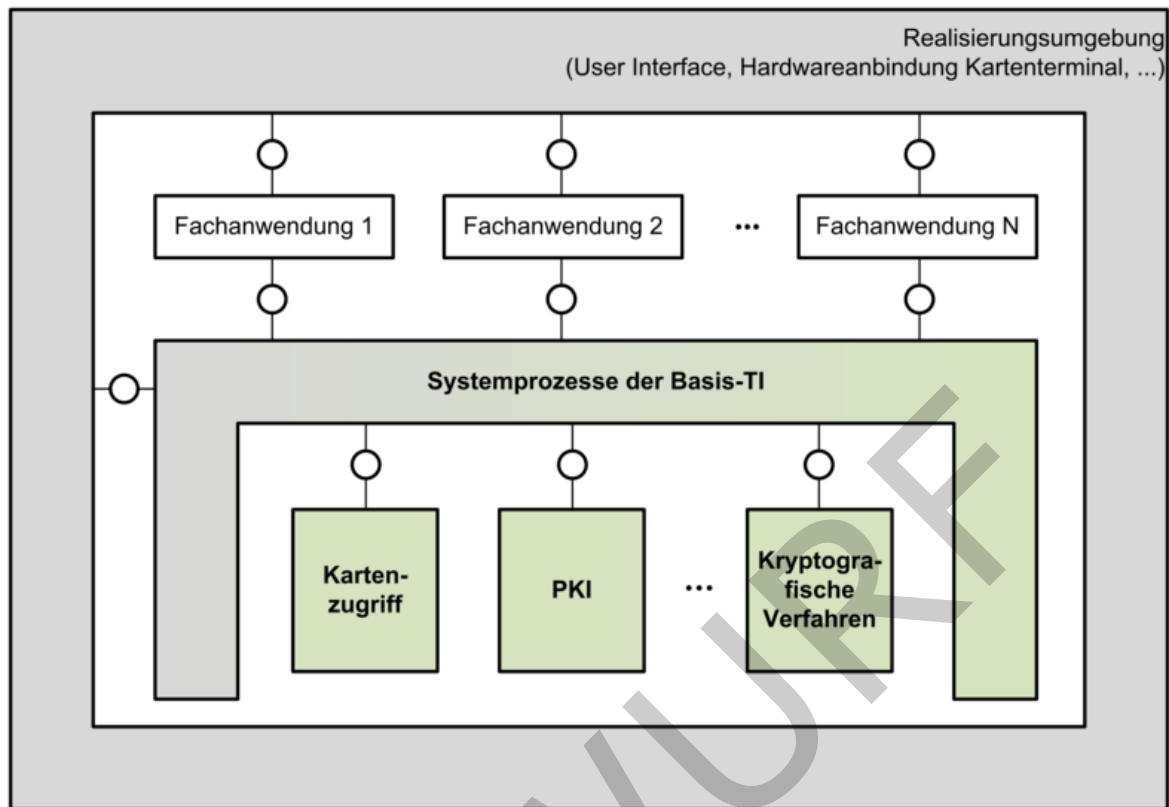


Abbildung 2: ABB_ADV_304 – Zusammenhang Systemprozesse und Fachanwendung

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 [gemSpec_Systemprozesse_dezTI]. 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"> • Installation des Systems und von Updates, • Konfiguration des Systems, • Administration von Nutzern (jedoch nicht von Versicherten), • täglicher Betrieb, • Herstellen und Wahren der Betriebsbereitschaft (z. B. Freischaltung der SM-B(s)). <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. [\leq]

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 Schlüsselmaterial 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

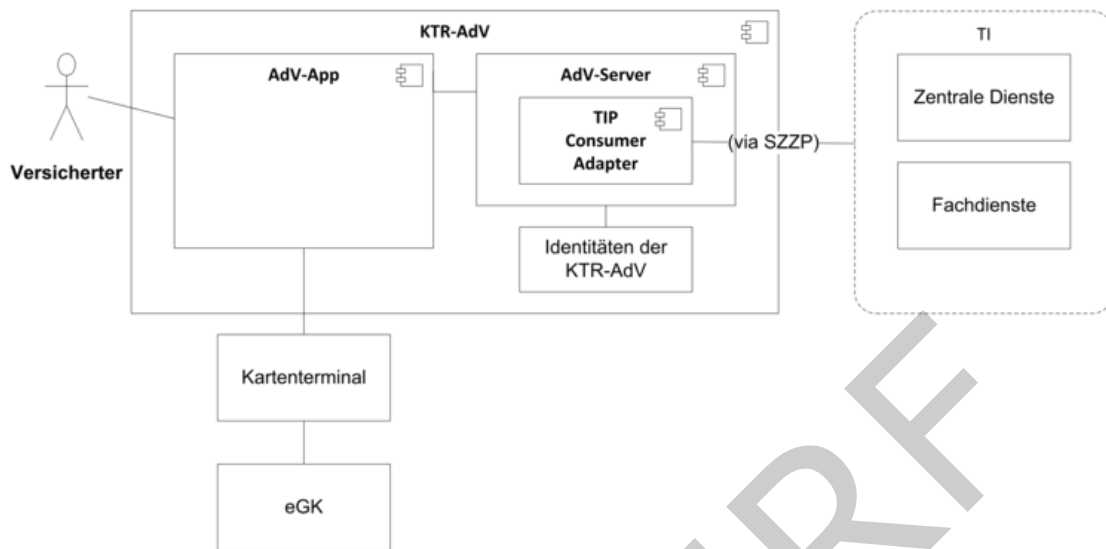
- SM-B-Identitäten der KTR-AdV,
- eGK (G2 und höher),
- SZZP,
- Dienste der zentralen TI-Plattform und
- Fachdienste.

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 Schlüsselmaterials 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.

415



416

417

Abbildung 3: ABB_ADV_301 – Kontextdiagramm

418

3.3 Ablaufumgebung

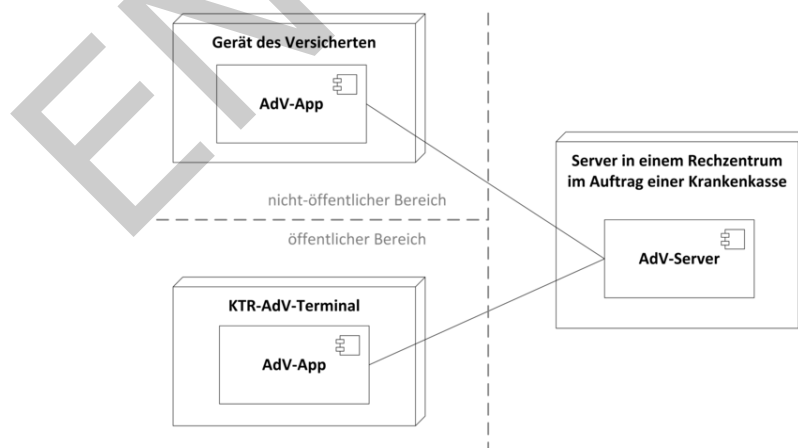
419

Die Komponenten der KTR-AdV werden in verschiedenen Umgebungen betrieben, die in ABB_ADV_303 dargestellt sind.

421

422

423



424

425

Abbildung 4: ABB_ADV_303 – Verteilungsdiagramm

426

427

428

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.

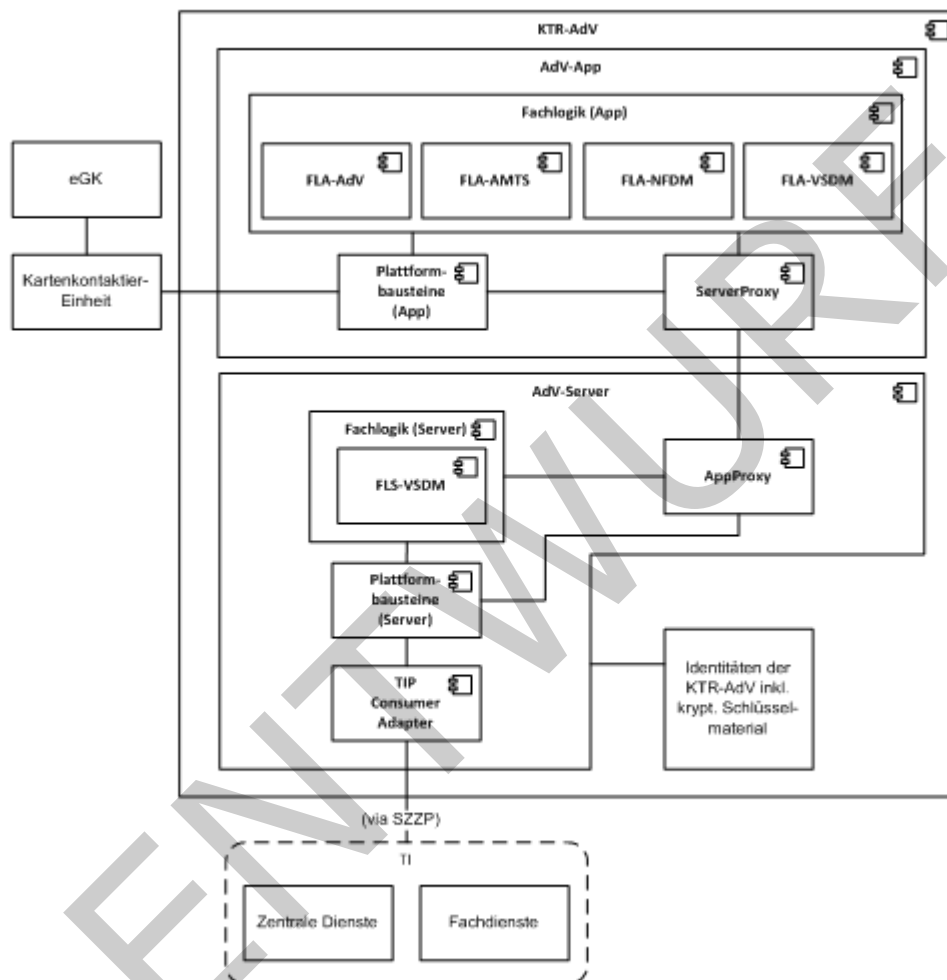


Abbildung 5: ABB_ADV_329 – Komponentendiagramm der KTR-AdV

In Tabelle TAB_ADV_329 werden die Komponenten, ihre Verantwortlichkeit und spezifische Funktionalitäten dargestellt.

463 **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"> Darstellung der Benutzeroberfläche für den Versicherten 	Kap. 6
Fachlogik (App)	In dieser Komponente wird die gesamte Fachlogik in Form von fachanwendungsspezifischen Modulen gebündelt. Daten werden - soweit möglich - ausschließlich lokal verarbeitet.	Kap. 6.1
FLA-AdV	<p>Dieses Modul setzt die Anwendungsfälle der Fachanwendung AdV um.</p> <p>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.</p> <p>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.</p> <p>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>	<p>Kap. 6.1.6</p> <p>Kap. 6.1.7</p> <p>[gemSpec_FLA_NFDM]</p>
FLA-VSDM	Dieses Modul setzt den Anwendungsfall der Fachanwendung VSDM um. Für den Ablauf wird eine	<p>6.1.5</p> <p>[gemSpec_FM_VSDM]</p>

	fachanwendungsspezifische Operation genutzt, welche in [gemSpec_FM_VSDM] spezifiziert ist.	
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"> • Zugriff auf die eGK 	Kap. 6.1.10
ServerProxy	<p>Diese Komponente stellt die Verbindung zum AdV-Server her.</p> <ul style="list-style-type: none"> • Sichere Verbindung mit dem AdV-Server <p>Diese Verbindung ist eine Innenschnittstelle an die nur Sicherheitsanforderungen im Abschnitt 5.1.2 gestellt werden.</p>	Kap. 5.1.2
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"> • Aufbau der Verbindung zum Intermediär VSDM <p>Festlegungen zum Verbindungsaufbau und die entsprechenden Schnittstelle der Fachdienste sind in [gemSpec_SST_VSDM] und [gemSpec_SST_FD_VSDM] spezifiziert.</p>	<p>Kap. 6.1.5</p> <p>[gemSpec_SST_VSDM]</p> <p>[gemSpec_SST_FD_VSDM]</p>

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"> • Einbeziehung der Identitäten der Kostenträger mit kryptografischen Operation auf deren geheimen Schlüsselmaterial in die AdV-Anwendungsfälle • Prüfung von Zertifikaten • Zugriff auf zentrale Dienste / Fachdienste über den Consumer Adapter 	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"> • Anbindung zu den relevanten zentralen Diensten der TI • Anbindung zu den relevanten Fachdiensten der TI • Prüfung von Zertifikaten der TI • Verwaltung des lokalen Truststores <p>Diese Leistungen können durch Plattformbausteine oder Module mit Fachlogik genutzt werden.</p>	Kap. 6.2.4
AppProxy	<p>Diese Komponente stellt die Verbindung zur AdV-App her.</p> <ul style="list-style-type: none"> • Sichere Verbindung mit der AdV-App <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. E256 [≤]

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 Stateful Packet Inspection/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. [<=]

A_16395 - Kein TLS Session-Resumption und Renegotiation

Die KTR-AdV DARF im Rahmen der TLS-Verbindung zwischen AdV-App und AdV-Server die Renegotiation und Session-Resumption NICHT unterstützen. [<=]

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. [<=]

A_19968 - AdV-App: Darstellen der Voraussetzungen für die sichere Ausführung der App im Handbuch

Der Hersteller der AdV-App MUSS im dazugehörigen Handbuch alle Voraussetzungen leicht ersichtlich darstellen, die von der Ausführungsumgebung (insbesondere KTR-AdV-Terminal) erfüllt werden müssen, damit ein sicherer Betrieb der AdV-App gewährleistet werden kann. [<=]

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.

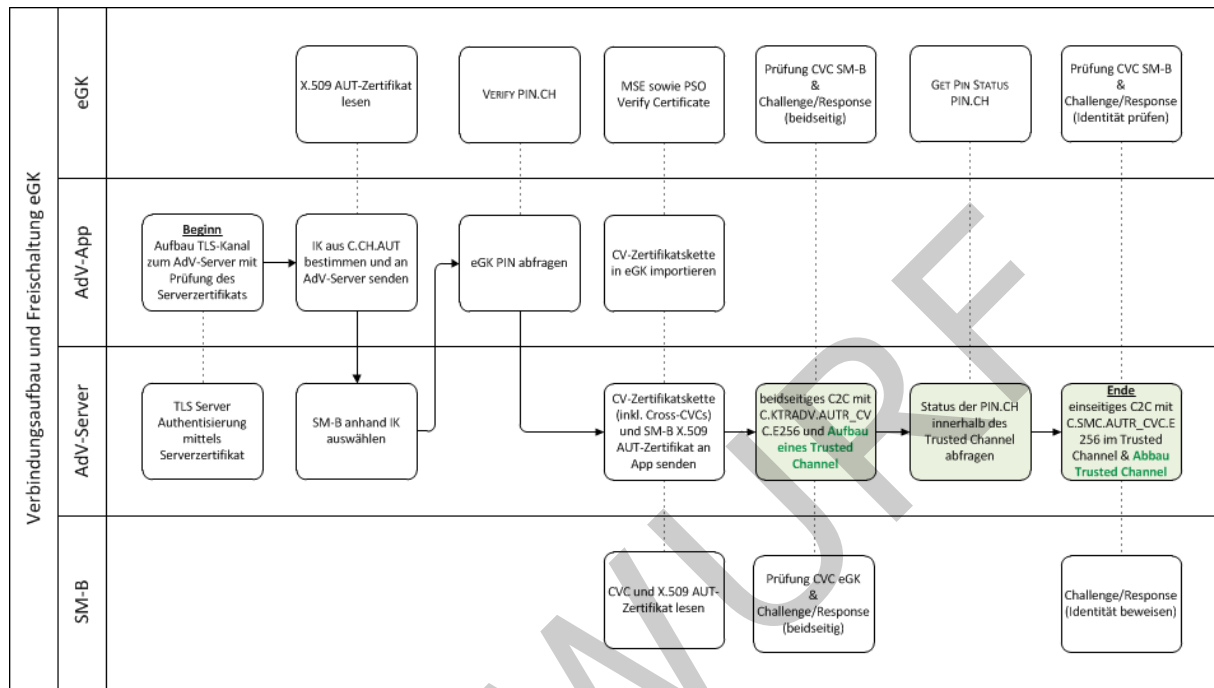


Abbildung 6 : ABB_ADV_333 Verbindungsaufbau und Freischaltung eGK

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: Institutskenzeichen 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 Institutskenzeichen 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 C.KTRADV.AUTR_CVC.E256 erwendet, und einen Trusted Channel etablieren. Der Trusted Channel wird vom Adv-Server zur eGK unter Verwendung der CV Schlüssel (elcSessionkey4TC) ausgehandelt. [<=]

Ein CV-Zertifikat C.KTRADV.AUTR_CVC.E256 hat das Zugriffsprofil CHA.0 und 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. [<=]

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

625 **A_15113 - AdV-App: Flaglist prüfen**

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

628 **A_15114 - AdV-Server: Prüfung Status PIN.CH der eGK**

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

632 Die erwartete Antwort der eGK auf das Kartenkommando Get PIN Status ist NoError (,90
633 00').

634 **A_15115 - AdV-Server, AdV-App: Einseitiges Card-to-Card mit CVC „KTR-AdV“**

635 Der AdV-Server und die AdV-App MÜSSEN nach erfolgreicher Prüfung des Status der
636 PIN.CH der eGK ein einseitiges Card-to-Card durchführen, wobei der AdV-Server ein CV-
637 Zertifikat C.SMC.AUTR_CVC.E256 erwendet.[<=]

638 Ein CV-Zertifikat C.SMC.AUTR_CVC.E256 hat das Zugriffsprofil CHA.1. Das einseitige
639 Card-to-Card schaltet die eGK frei. Der für die Statusabfrage aufgebaute Trusted Channel
640 kann abgebaut werden.

641 **A_15116 - AdV-App: Abbruch bei Fehler im Verbindungsaufbau und
642 Freischaltung eGK**

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

645 Für Erläuterungen zum Card-2-Card und der Prüfung des Status einer PIN siehe auch
646 [gemSpec_CardProxy].

647 **5.1.4 Filterung von Kartenkommandos an die eGK**

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

653 **A_15117 - AdV-App: Ablehnen von Kartenkommandos**

654 Die AdV-App MUSS alle vom AdV-Server gesendeten Kartenkommandos ablehnen,
655 welche nicht gemäß [TR-03158#Anhang C] zulässig sind, und die AdV-Sitzung
656 beenden.[<=]

657 **5.2 Logging**

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

664 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. [<=]

758 AdV-A_2443 - AdV-App: Zugriff auf Protokolldateien

759 Die AdV-App MUSS, wenn sie auf einem KTR-AdV-Terminal betrieben wird, den Zugriff
760 auf Protokolldateien auf berechnigte Nutzer für Administrations- und Betriebsaufgaben
761 beschränken. [≤]

762 5.3 Nicht-funktionale Anforderungen

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

770

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 [gemSpec_Systemprozesse_dezTI] 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.	

796

797 [**<=**]

798 **6.1.1 AdV-Sitzung des Versicherten**

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

802 **6.1.1.1 AdV-Sitzung initialisieren**

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

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

808

809 **AdV-A_2445 - AdV-App: Starten einer Sitzung**

810 Die AdV-App MUSS den Anwendungsfall „Starten einer Sitzung“ gemäß TAB_ADV_303
 811 umsetzen.

812

813 **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"> Die AdV-App hat für die AdV-Sitzung eine TLS-Verbindung zum AdV-Server aufgebaut. Die Benutzerverifikation mit der PIN.CH wurde erfolgreich durchgeführt. Die eGK wurde durch ein Card-2-Card mit einer korrespondierenden SM-B freigeschaltet und auf Gültigkeit geprüft. Die eGK wurde auf Gültigkeit geprüft. Für die eGK werden durch Plattformbaustein PL_TUC_CARD_INFORMATION die dort spezifizierten Informationen bereitgestellt. Die Sitzung des Versicherten wurde gestartet. Der Gültigkeitsstatus der eGK wird angezeigt. Es werden die mit der eGK des Versicherten verfügbaren Fachanwendungen aufgelistet. <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"> Einlesen der Karte Einverständnis des Versicherten einholen (Benutzerverifikation) Versicherten-PIN entsperren (optional) Verbindungsaufbau zum AdV-Server und Freischaltung eGK Protokollieren des eGK-Zugriffs (für eGK G2) Online-Gültigkeitsprüfung der eGK Verfügbare Anwendungen anzeigen

814

815

Tabelle 5: TAB_ADV_304 – Ablaufaktivitäten - Starten einer AdV-Sitzung

Einlesen der Karte	
---------------------------	--

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"> • Kartentyp, MUSS vom Typ eGK sein • Produkttypversion des Objektsystems, MUSS G2 oder höher sein • Echtheit der Karte, die Karte MUSS für echt befunden sein <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>
Einverständnis des Versicherten einholen (Benutzerverifikation)	
Plattformbaustein	PL_TUC_CARD_VERIFY_PIN
Eingangsdaten	
Identifikator	PIN.CH
Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im AdV-App-Benutzerinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT	„Eingabe Versicherten-PIN: “
Rückgabedaten	
Rückgabe - Beschreibung	Aktion durch AdV-App

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.
Versicherten-PIN entsperren (optional)	
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 entsperrt 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).

Verbindungsaufbau zum AdV-Server und Freischaltung eGK	
<i>Beschreibung</i>	Siehe Kap. 5.1.3 Verarbeitung mit Aktivität "Protokollieren des eGK-Zugriffs" fortsetzen.
Protokollieren des eGK-Zugriffs (für eGK G2)	
Plattformbaustein	PL_TUC_EGK_APPEND_PROTOCOL
<i>Eingangsdaten</i>	
DATATYPE	„v“ (Anwendungen des Versicherten in der KTR-AdV Umgebung)
ACCESSTYPE	„Z“ (allgemeiner Zugriff; Lesen und bearbeiten).
<i>Rückgabedaten</i>	
<i>Rückgabe - Beschreibung</i>	Aktion durch AdV-App
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.

Online-Gültigkeitsprüfung der eGK	
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 Karteninhaberzertifikats: Zertifikat mathematisch gültig	Fortfahren und Aufbereitung der Menüstruktur
Mathematische Prüfung des Karteninhaberzertifikats: Zertifikat mathematisch ungültig oder Prüffehler	Fortfahren und Aufbereitung der Menüstruktur und den Versicherten informieren.
Prüfung auf zeitliche Gültigkeit des Karteninhaberzertifikats: Zertifikat zeitlich gültig	Fortfahren und Aufbereitung der Menüstruktur
Prüfung auf zeitliche Gültigkeit des Karteninhaberzertifikats: 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 durchführt und andererseits die Legitimität der Karte mittels Onlineabfrage beim Trust Service Provider geprüft.

Verfügbare Anwendungen anzeigen	
<p><i>Beschreibung</i></p>	<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"> 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. Fachanwendungen im Status <code>ABSENT</code> bzw. <code>TERMINATED</code> sind auf der eGK nicht vorhanden bzw. nicht mehr zu verwenden, deren fachspezifische Anwendungsfälle sollten in der AdV-App nicht auswählbar sein. Fachanwendungen im Status <code>AVAILABLE</code> oder <code>HIDDEN</code> sind auf der eGK verfügbar, deren fachspezifische Anwendungsfälle sind je nach vorangegangener Operation logisch sinnvoll (Daten lesen, Anwendung verbergen nur im Zustand <code>AVAILABLE</code>, Anwendung sichtbar machen nur im Zustand <code>HIDDEN</code>) und sollten entsprechend angeboten bzw. temporär nicht auswählbar sein. Wenn die Fachanwendung über eine PIN verfügt: PINs im Zustand <code>DISABLED</code> können über einen Anwendungsfall eingeschaltet werden, PINs im Zustand <code>OK</code> und <code>VERIFIABLE</code> können abhängig von den Zugriffsrechten im Objektsystem der eGK ausgeschaltet werden, PINs im Zustand <code>BLOCKED</code> müssen vor der Verwendung und den Zugriff auf die Fachanwendung entsperrt werden. <p>Fachanwendungsunabhängige Anwendungsfälle dürfen durch den Status der Fachanwendungen nicht eingeschränkt werden und müssen immer verfügbar sein.</p>
<p><i>Hinweis zur Umsetzung</i></p>	<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</p>

	beschriebenen Anwendungsfälle erst zulässig werden oder nicht mehr zulässig sind.
--	---

816
817
818

[<=]

819 **Adv-A_2446 - Adv-App: Warnung eGK nicht ziehen**

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

823 **6.1.1.2 Adv-Sitzung beenden**

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

829 **Adv-A_2447 - Adv-App: Menüpunkt zum Beenden einer Sitzung**

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

832 **Adv-A_2448 - Adv-App: Ziehen der eGK des Versicherten**

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

835 **Adv-A_2449 - Adv-App: Beenden einer Sitzung in Adv-App**

836 Die Adv-App MUSS das Beenden der Sitzung des angemeldeten Versicherten derart
837 umsetzen, dass ein ggfs. in der Ausführung befindlicher Anwendungsfall – welcher
838 inkonsistente Daten auf der eGK hinterlassen könnte – vor dem Ende der Sitzung
839 abgeschlossen wird. Die Adv-App MUSS zum Beenden der Sitzung

- 840 • mit PL_TUC_CARD_RESET ein Reset der gesteckten Karte anfordern,
- 841 • die TLS Verbindung zum Adv-Server beenden
- 842 • und den Versicherten zum Ziehen der eGK auffordern.

843 [<=]

844 **Adv-A_2450 - Adv-App: Darstellung einer neutralen Anzeige**

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

847 **6.1.2 Übergreifende Vorbedingungen**

848 Die ab Kapitel 6.1.5 beschriebenen fachlichen Anwendungsfälle werden durch den
849 Versicherten eigenständig ausgeführt, die Adv-App ruft die dort benannten Operationen
850 nur bei explizitem Wunsch des Versicherten auf. Folgende Vorbedingungen müssen beim
851 Start jedes Anwendungsfalls 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**

- Der Anwendungsfall „Starten einer Sitzung“ wurde erfolgreich ausgeführt.
- Die eGK des Versicherten wird für die Nutzung in den Anwendungsfällen für den Zeitraum der Sitzung eindeutig identifiziert.

[<=]

AdV-A_2452 - AdV-App: Zulässigkeit der Anwendungsfälle

Die AdV-App MUSS die Zulässigkeit des Anwendungsfalls 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),
UNKNOWN (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 FALSE	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

884
885
886 **[<=]**

887 Definiert eine Fachanwendung in ihrer Fachmodulspezifikation abweichende Kriterien
888 oder von den in TAB_ADV_384 definierten Bedingungen abweichende Vorbedingung zur
889 Zulässigkeit ihrer Anwendungsfälle, so sind jene der Fachanwendung bindend.

890 **6.1.3 Hinweistext zu Fachanwendung**

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

896 **AdV-A_2547 - Empfehlung: Hinweistext zu Fachanwendung**

897 Die AdV-App SOLL im Kontext jeder Fachanwendung einen Hinweistext gemäß
898 TAB_ADV_461 anzeigen, der den Zweck der Fachanwendung beschreibt.
899

900 **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 Gewebespende (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.

901 [**<=**]

902 **6.1.4 Generische Anwendungsfälle**

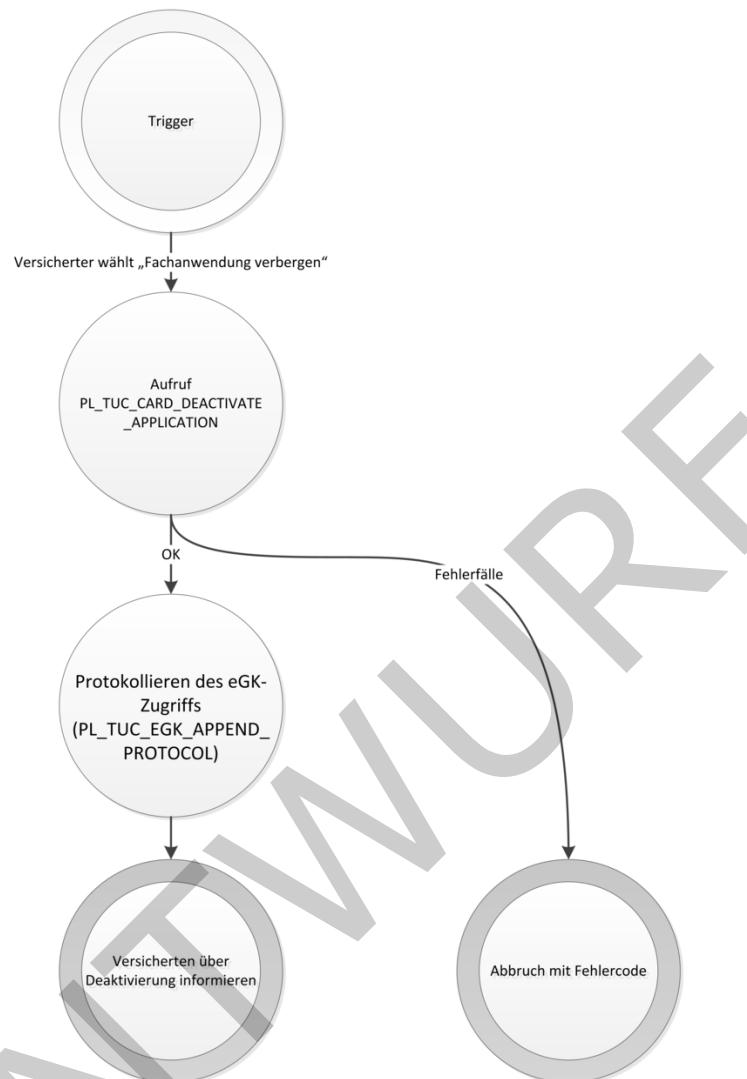
903 Dieses Kapitel beschreibt die generischen Anwendungsfälle, welche durch
 904 Anwendungsfälle verschiedener Fachanwendungen genutzt werden. Unter anderem wird
 905 die Möglichkeit geboten PIN-Objekte, die im Kontext einer Fachanwendung stehen, ein-
 906 oder auszuschalten.

907 **6.1.4.1 Anwendung auf eGK deaktivieren**

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

912 Die folgende Abbildung ABB_ADV_305 zeigt informativ, welche Schritte für
 913 Anwendungsfall AdV-UC_14 „Anwendung auf eGK deaktivieren“ ausgeführt werden
 914 müssen.

915



916

917

Abbildung 7: ABB_ADV_305 – Ablauf „Anwendung auf eGK deaktivieren“

918

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"> 1. PL_TUC_CARD_DEACTIVATE_APPLICATION aufrufen 2. PL_TUC_CARD_DEACTIVATE_APPLICATION Ergebnis verarbeiten 3. Protokollieren des eGK-Zugriffs (für eGK >=G2.1) 4. Ergebnis anzeigen
Diagramm	Abbildung ABB_ADV_305 – Ablauf „Anwendung auf eGK deaktivieren“

923
924

Tabelle 10: TAB_ADV_306 – Ablaufaktivitäten – AdV-UC_14

1. PL_TUC_CARD_DEACTIVATE_APPLICATION aufrufen	
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.	

2. PL_TUC_CARD_DEACTIVATE_APPLICATION Ergebnis verarbeiten	
<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 parametrierten Plattformbaustein PL_TUC_CARD_DEACTIVATE_APPLICATION. Dieser liefert eine Statusmeldung zurück. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben.	
3. Protokollieren des eGK-Zugriffs	
Plattformbaustein	PL_TUC_EGK_APPEND_PROTOCOL
<i>Eingangsdaten</i>	
DATATYPE	Wenn der Identifikator der zu deaktivierenden Applikation <ul style="list-style-type: none"> • „DF.NFD“ ist, dann „b“ • „DF.DPE“ ist, dann „c“ • „DF.AMTS“ ist, dann „e“
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.
Beschreibung	
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.	
4. Ergebnis anzeigen	
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.

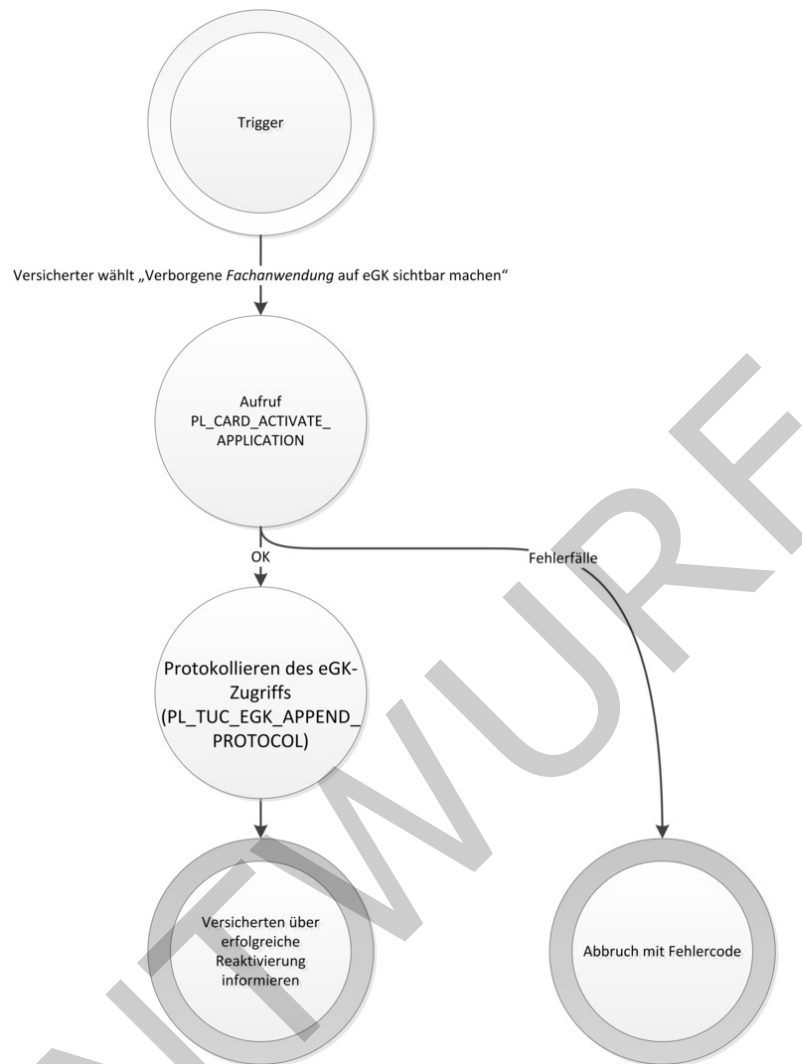
925
926
927 [**<=**]
928

929 **6.1.4.2 Anwendung auf eGK reaktivieren**

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

932 Die folgende Abbildung ABB_ADV_383 zeigt informativ, welche Schritte für
933 Anwendungsfall AdV-UC_15 „Anwendung auf eGK reaktivieren“ ausgeführt werden
934 müssen.

935



936

937

938

Abbildung 8: ABB_ADV_383 – Ablauf „Anwendung auf eGK reaktivieren“

939

940

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.

943

944

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"> 1. PL_TUC_CARD_ACTIVATE_APPLICATION aufrufen 2. PL_TUC_CARD_ACTIVATE_APPLICATION Ergebnis verarbeiten 3. Protokollieren des eGK-Zugriffs (für eGK >=G2.1) 4. Ergebnis anzeigen
Diagramm	Abbildung ABB_ADV_383 – Ablauf „Anwendung auf eGK reaktivieren“

Tabelle 12: TAB_ADV_307 – Ablaufaktivitäten – Adv-UC_15

1. PL_TUC_CARD_ACTIVATE_APPLICATION aufrufen	
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.
2. PL_TUC_CARD_ACTIVATE_APPLICATION Ergebnis verarbeiten	

<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 parametrierten Plattformbaustein PL_TUC_CARD_ACTIVATE_APPLICATION. Dieser liefert eine Statusmeldung zurück. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben.
3. Protokollieren des eGK-Zugriffs	
Plattformbaustein	PL_TUC_EGK_APPEND_PROTOCOL
<i>Eingangsdaten</i>	
DATATYPE	Wenn der Identifikator der zu deaktivierenden Applikation <ul style="list-style-type: none"> • „DF.NFD“ ist, dann „b“ • „DF.DPE“ ist, dann „c“ • „DF.AMTS“ ist, dann „e“
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.

Beschreibung	<p>Die Protokollierung des Datenzugriffs erfolgt für eine eGK der Version größer oder gleich G2.1.</p> <p>Der Aufbau der Eingangsdaten wird in PL_TUC_EGK_APPEND_PROTOCOL beschrieben.</p>
4. Ergebnis anzeigen	
Hinweis an den Versicherten	<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>

[<=]

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.

978 Die folgende Abbildung ABB_ADV_312 zeigt informativ, welche Schritte für
979 Anwendungsfall AdV-UC_01: „PIN ändern“ ausgeführt werden müssen.

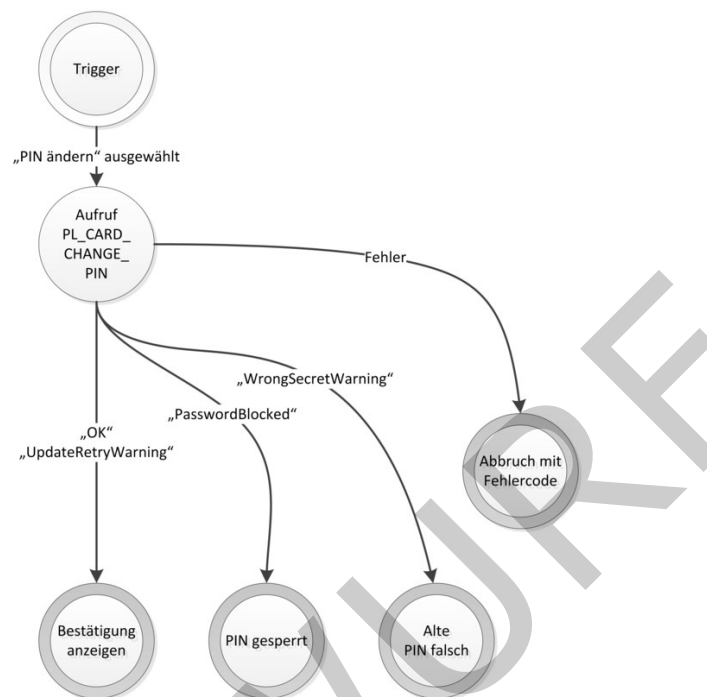


Abbildung 9 : ABB_ADV_312 – Ablauf des AdV-UC_01: „PIN der eGK ändern“

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

Benennung 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 Anwendungsfalles, 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"> 1. PL_TUC_CARD_CHANGE_PIN nutzen 2. PL_TUC_CARD_CHANGE_PIN Ergebnis verarbeiten 3. Ergebnis anzeigen
Diagramm	Abbildung ABB_ADV_312 – Ablauf des Adv-UC_01: „PIN ändern“

989

990

Tabelle 14: TAB_ADV_313 – Ablaufaktivitäten – PIN der eGK ändern

1. PL_TUC_CARD_CHANGE_PIN nutzen	
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.
2. Rückgabewert von PL_TUC_CARD_CHANGE_PIN verarbeiten	
<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 <i>Ergebnis</i> 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>
3. Ergebnis anzeigen	
<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. 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>

991
992
993 [**<=**]
994

995 **6.1.4.3.2 PIN auf eGK entsperren**

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

998 Die folgende Abbildung ABB_ADV_316 zeigt informativ, welche Schritte für
999 Anwendungsfall AdV-UC_02: „PIN auf eGK entsperren“ ausgeführt werden müssen.

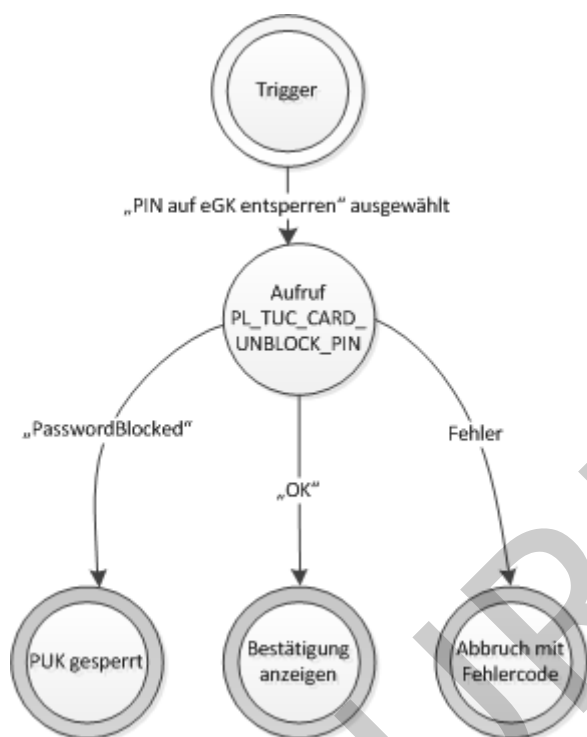


Abbildung 10 : ABB_ADV_316 – Ablauf des AdV-UC_02: „PIN auf eGK entsperren“

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"> 1. PL_TUC_CARD_UNBLOCK_PIN aufrufen 2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten 3. Ergebnis anzeigen
Diagramm	Abbildung ABB_ADV_316 – Ablauf des Adv-UC_02: „PIN auf eGK entsperren“

1010

Tabelle 16: TAB_ADV_317 – Ablaufaktivitäten – PIN der eGK entsperren

1. PL_TUC_CARD_UNBLOCK_PIN aufrufen	
Plattformbaustein	PL_TUC_CARD_UNBLOCK_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>PUK: „Eingabe PUK: “ bzw. Neue PIN: „Eingabe neue Versicherten-PIN: “</p> <p>Für Identifikator = PIN.AMTS_REP</p> <p>PIN.CH: „Eingabe Versicherten-PIN: “ bzw. Neue PIN: „Eingabe neue Vertreter-PIN: “</p>
Beschreibung	Für das Entsperren der PIN wird ein Plattformbaustein genutzt.
2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten	
<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>	<p>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.</p> <p>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.</p>
3. Ergebnis anzeigen	
<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.</p>

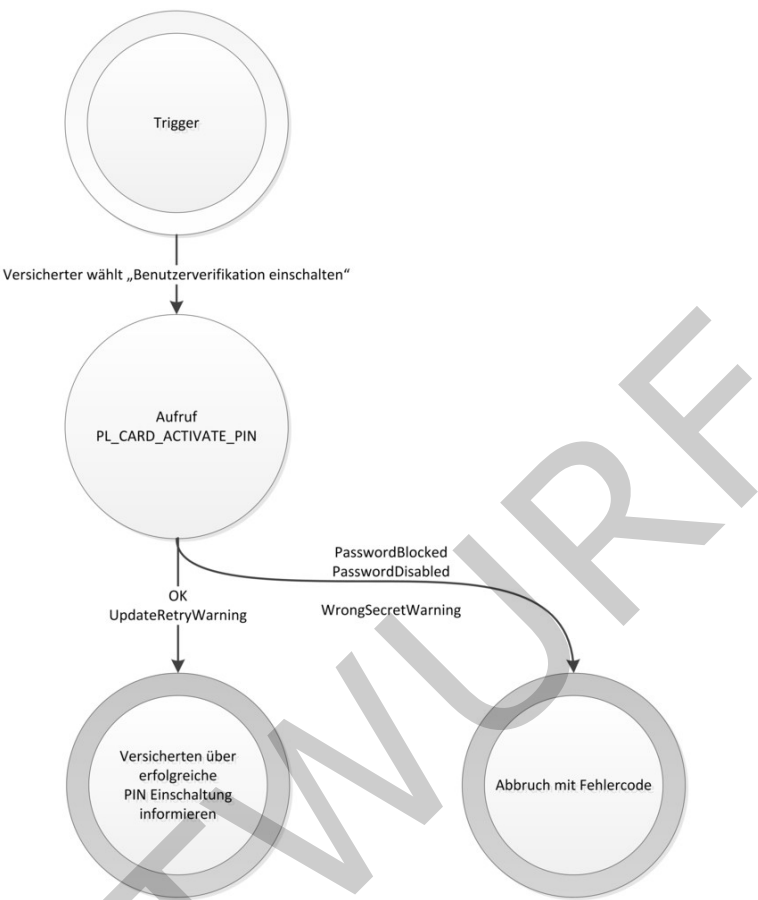
1011
1012
1013 [**<=**]

1014 6.1.4.3.3 PIN für Fachanwendung einschalten

1015 Wenn die Multireferenz-PIN einer Fachanwendung deaktiviert ist, dann kann der
1016 Versicherte diese PIN mit diesem Anwendungsfall aktivieren.

1017 Die folgende Abbildung ABB_ADV_308 zeigt informativ, welche Schritte für
1018 Anwendungsfall Adv-UC_03 „PIN für Fachanwendung einschalten“ ausgeführt werden
1019 müssen.

1020
1021



1022
1023
1024

Abbildung 11: ABB_ADV_308 – Ablauf AdV-UC_03 „PIN für Fachanwendung einschalten“

1026
1027

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. 1. PL_TUC_CARD_ENABLE_PIN aufrufen 2. PL_TUC_CARD_ENABLE_PIN Ergebnis verarbeiten 3. Ergebnis anzeigen
Diagramm	Abbildung ABB_ADV_308 – Ablauf Adv-UC_03 „PIN für Fachanwendung einschalten“

1032

1033

Tabelle 18: TAB_ADV_309 – Ablaufaktivitäten – Adv-UC_03

1. PL_TUC_CARD_ENABLE_PIN aufrufen	
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.

2. PL_TUC_CARD_ENABLE_PIN Ergebnis verarbeiten	
<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>	<p>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.</p> <p>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.</p>
3. Ergebnis anzeigen	
<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>

1034
1035
1036
1037

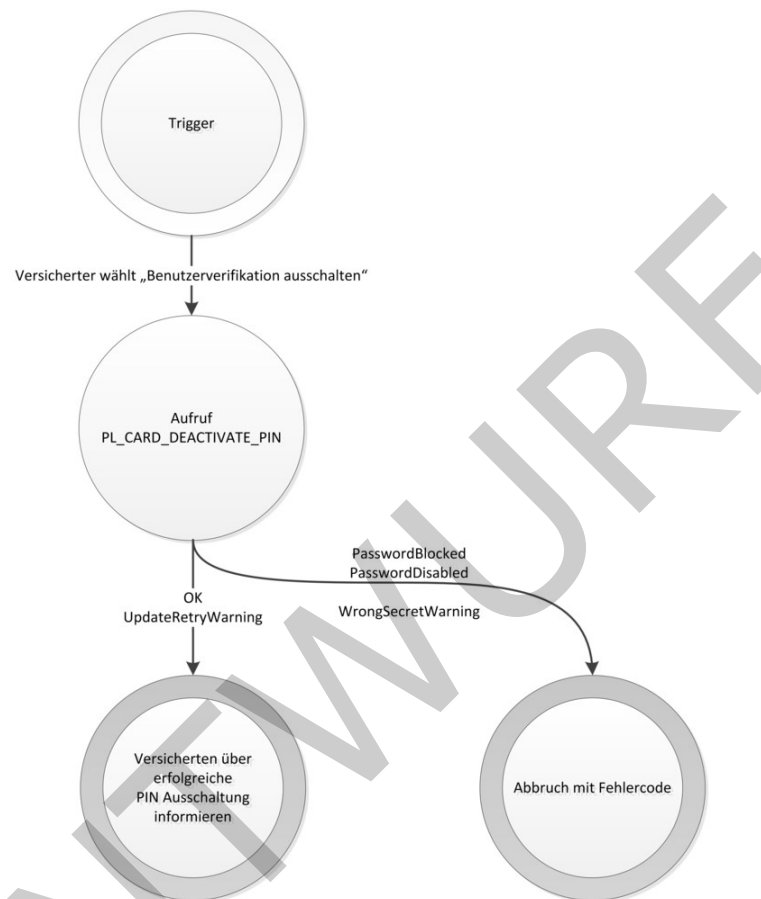
[<=]

1038 6.1.4.3.4 PIN für Fachanwendung ausschalten

1039 Um die Anzahl der beim Leistungserbringer notwendigen PIN-Eingaben pro
1040 Kartensteckzyklus zu minimieren, kann der Versicherte für bestimmte Fachanwendungen
1041 die Multireferenz-PIN für diese Fachanwendung deaktivieren.

1042 Die folgende Abbildung ABB_ADV_310 zeigt informativ, welche Schritte für
1043 Anwendungsfall AdV-UC_04 „PIN für Fachanwendung ausschalten“ ausgeführt werden
1044 müssen.

1045
1046



1047
1048
1049

1050 **Abbildung 12: ABB_ADV_310 – Ablauf AdV-UC_04 „PIN für Fachanwendung ausschalten“**

1051

1052 **AdV-A_2456 - AdV-UC_04 Hinweis bei ausgeschaltetem PIN**

1053 Die AdV-App MUSS, wenn der Versicherte den PIN einer Anwendung ausschalten möchte,
1054 dem Versicherten einen Hinweis anzeigen, dass bei ausgeschalteter PIN ein Arzt oder
1055 Apotheker auf die Daten dieser Anwendung ohne die Eingabe einer PIN zugreifen
1056 kann.[<=]

1057 **AdV-A_2457 - AdV-UC_04 „PIN für Fachanwendung ausschalten“**

1058 Die AdV-App MUSS den Anwendungsfall AdV-UC_04 „PIN für Fachanwendung
1059 ausschalten“ gemäß TAB_ADV_310 umsetzen.

1060

1061 **Tabelle 19: TAB_ADV_310 – AdV-UC_04 „PIN für Fachanwendung ausschalten“**

Benennung 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"> 1. PL_TUC_CARD_DISABLE_PIN aufrufen 2. PL_TUC_CARD_DISABLE_PIN Ergebnis verarbeiten 3. Ergebnis anzeigen
Diagramm	Abbildung ABB_ADV_310 – Ablauf Adv-UC_04 „PIN für Fachanwendung ausschalten“

1062

1063

Tabelle 20: TAB_ADV_311 – Ablaufaktivitäten – Adv-UC_04

1. PL_TUC_CARD_DISABLE_PIN aufrufen	
Plattformbaustein	PL_TUC_CARD_DISABLE_PIN
Eingangsdaten	
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 (<i>MRPIN.NFD</i> , <i>MRPIN.DPE</i> , <i>MRPIN.AMTS</i>) 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.
2. PL_TUC_CARD_DISABLE_PIN Ergebnis verarbeiten	
<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>	<p>Das Deaktivieren der Benutzerverifikation basiert auf dem parametrierten Plattformbaustein PL_TUC_CARD_DISABLE_PIN. Dieser liefert eine Statusmeldung zurück. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben.</p> <p>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.</p>
3. Ergebnis anzeigen	
<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.</p> <p>Bei einer Fehleingabe der Pin des Versicherten wird dem Versicherten die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PIN zurückgemeldet.</p>

1064
1065
1066

[<=]

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.

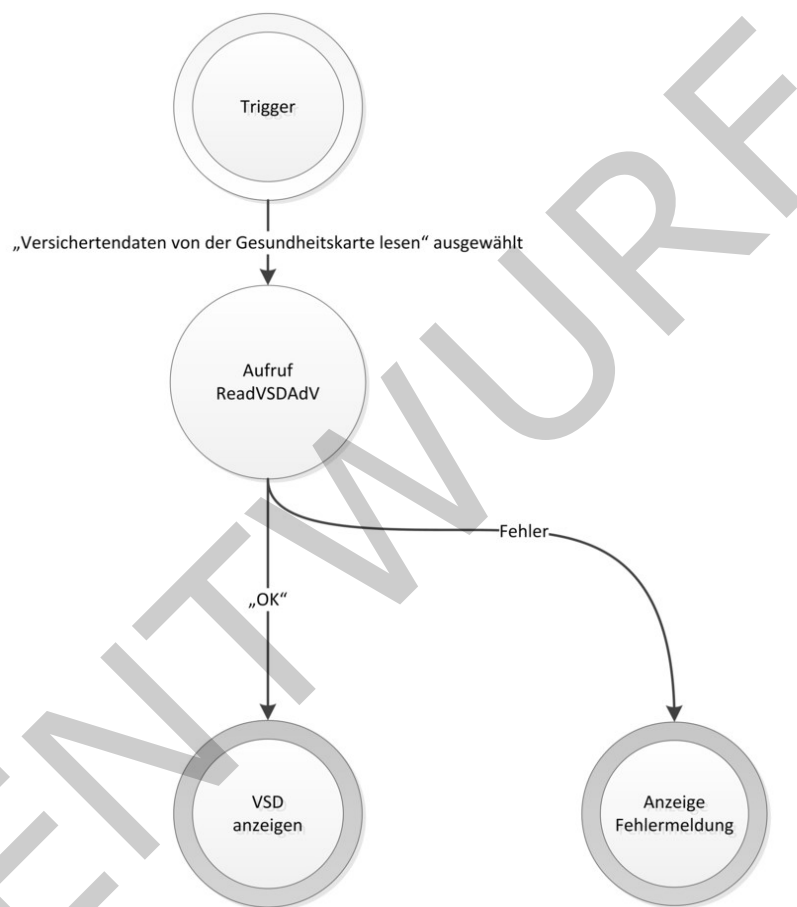


Abbildung 13: ABB_ADV_317 - Ablauf des „VSD von eGK lesen“

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	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	Die Umsetzung ist in „TAB_ADV_315 – Ablaufaktivitäten – VSD von eGK anzeigen“ beschrieben. <ol style="list-style-type: none"> 1. Aufruf Operation ReadVSDAdV 2. Response von Operation ReadVSDAdV verarbeiten 3. VSD anzeigen
Diagramm	Abbildung ABB_ADV_317 - Ablauf des „VSD von eGK lesen“

1084

1085

Tabelle 22: TAB_ADV_315 – Ablaufaktivitäten – VSD von eGK anzeigen

1. AdV-LeseRequest erzeugen	
Operation	ReadVSDAdV
Eingangsdaten	
getGVD	True (GVD sollen gelesen werden)
2. VSD-LeseResponse verarbeiten	
Rückgabedaten	
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 [gemSysL_VSDM#Anhang C].</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"> Fehlercode 114: „Ihre Gesundheitskarte ist gesperrt. Bitte wenden Sie sich an Ihre Krankenkasse“ Fehlercode 106: „Ihre Gesundheitskarte ist ungültig. Bitte prüfen Sie, ob diese Gesundheitskarte Ihre aktuellste ist. Falls ja, wenden Sie sich bitte an Ihre Krankenkasse.“ 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.“ <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>PersoenlicheVersichertendaten - XML-Element UC_PersoenlicheVersichertendatenXML</p> <p>AllgemeineVersicherungsdaten - XML-Element UC_AllgemeineVersicherungsdatenXML</p> <p>GeschuetzteVersichertendaten - XML-Element UC_GeschuetzteVersichertendatenXML)</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 [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].</p>
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_PersoenlicheVersichertendatenXML, 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>

1086

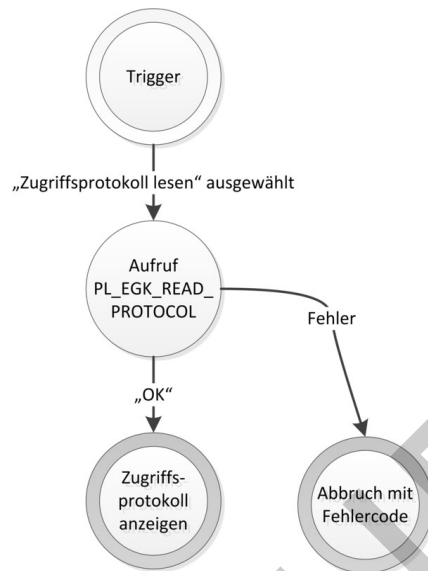
1087 [\leq]

1088 6.1.5.2 Zugriffsprotokoll anzeigen

1089 Mit der Umsetzung dieses Anwendungsfalls sollen dem Versicherten das auf seiner eGK
1090 gespeicherte Zugriffsprotokoll zur Anzeige gebracht werden.

1091 Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall AdV-UC_21:
1092 „Zugriffprotokoll von eGK lesen“ ausgeführt werden müssen.

1093
1094



1095
1096
1097
1098

Abbildung 14: ABB_ADV_314 – Ablauf des AdV-UC_21: „Zugriffsprotokoll anzeigen“

1099
1100
1101
1102
1103

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. [≤]

1104
1105
1106
1107
1108
1109

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. [≤]

1110
1111
1112
1113

AdV-A_2463 - AdV-App: Zugriffsprotokoll anzeigen

Die AdV-App MUSS den Anwendungsfall „Zugriffsprotokoll anzeigen“ gemäß TAB_ADV_350 umsetzen.

1114

Tabelle 23: TAB_ADV_350 – Zugriffsprotokoll anzeigen

Benennung des Anwendungsfalls	„Zugriffsprotokoll anzeigen“
Hinweistext für den Versicherten	TAB_ADV_473#ADV002
Auslöser	Der Versicherte möchte das Zugriffsprotokoll seiner eGK anzeigen lassen. Dazu wählt er

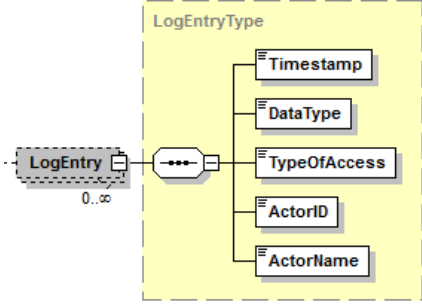
	eine Aktion in der AdV-App aus, die das Auslesen des Protokolls startet.
Akteure	Versicherter
Vorbedingung	Siehe übergreifende Vorbedingungen.
Nachbedingung	Das Zugriffsprotokoll wird dem Versicherten angezeigt.
Standardablauf	<p>Die Umsetzung ist in „TAB_ADV_351 – Ablaufaktivitäten – Zugriffsprotokoll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

1115

1116

Tabelle 24: TAB_ADV_351 – Ablaufaktivitäten – Zugriffsprotokoll anzeigen

1. LeseRequest erzeugen	
Plattformbaustein	PL_TUC_EGK_READ_PROTOCOL
Eingangsdaten	
-	-
Beschreibung	Es wird das gesamte Zugriffsprotokoll auf der elektronischen Gesundheitskarte ausgelesen.
2. LeseResponse verarbeiten	
Rückgabedaten	

OK + Liste	<p>„Daten wurden erfolgreich gelesen“ Beinhaltet das Zugriffsprotokoll. Den Aufbau zeigt die folgende Abbildung und wird in [gemSpec_Karten_Fach_TIP] definiert.</p> 
CorruptDataWarning +Liste	<p>„Daten gelesen, Speicher möglicherweise defekt “ Beinhaltet das Zugriffsprotokoll. Den Aufbau zeigt die Abbildung oben.</p>
Beschreibung	<p>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.</p>
3. Protokoll anzeigen	
Zugriffsprotokoll zur Anzeige bringen	<p>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:</p> <p>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</p>

1117
1118
1119

[<=]

1120 **AdV-A_2464 - AdV-App: Filtern von Protokolleinträgen**

1121 Die AdV-App MUSS es dem Versicherten ermöglichen, die angezeigten Einträge des
1122 Zugriffsprotokolls nach Anwendung, Art des Zugriffs, Zeitraum und zugreifendem Akteur
1123 zu filtern.[<=]

1124 **6.1.5.3 Versicherten-PIN ändern**

1125 Mit diesem Anwendungsfall kann der Versicherte das Geheimnis der Versicherten-PIN
1126 ändern.

1127 Für die Umsetzung wird der in Kap. 6.1.4.3.1 PIN ändern beschriebene generische
1128 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	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

[<=]

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	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.
Nachbedingung	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"> 1. Abfrage Kenntnis PUK 2. Ergebnis Abfrage Kenntnis PUK verarbeiten 3. Gemäß Beschreibung Adv-UC_02: „PIN auf eGK entsperren“

1146

1147

Tabelle 27: TAB_ADV_354 – Ablaufaktivitäten – Versicherten-PIN entsperren

1. Abfrage Kenntnis PUK	
<i>Beschreibung</i>	Die Adv-App MUSS den Versicherten vor einem Versuch der Entsperrung fragen, ob der PUK bekannt ist
2. Ergebnis Abfrage Kenntnis PUK verarbeiten	
Rückgabedaten	
JA (Dem Versicherten ist der PUK bekannt.)	Aufruf des folgenden Schritts im Standardablauf.
NEIN (Dem Versicherten ist der PUK nicht bekannt.)	<p>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.</p> <p>Falls eine Adv-Sitzung aktiv ist, muss anschließend der Anwendungsfall "Adv-Sitzung beenden" aufgerufen werden.</p>
3. Umsetzung entsprechend Adv-UC_02: „PIN der eGK entsperren“	
<i>Beschreibung</i>	<p>Die weitere Umsetzung erfolgt gemäß der Beschreibung des Anwendungsfalls Adv-UC_02: „PIN der eGK entsperren“ mit dem Parameter <code>Identifikator = PIN.CH</code></p>

1148

1149 [**<=**]

1150
1151

1152 **AdV-A_2467 - AdV-App: AdV-UC_02: Abbruch der AdV-Sitzung**

1153 Die AdV-App MUSS, falls die PIN.CH nicht erfolgreich entsperrt wurde und eine AdV-
1154 Sitzung aktiv ist, den Anwendungsfall "AdV-Sitzung beenden" aufrufen.[<=]

1155 **6.1.5.5 Datenübertragung bei Kartentausch**

1156 Dieser Anwendungsfall erlaubt dem Versicherten, Daten von seiner eGK auf eine weitere,
1157 d.h. ihm neu ausgestellte eGK zu kopieren. Mit der Umsetzung dieses Anwendungsfalls
1158 kann der Versicherte seine Daten – welche in der KTR Umgebung zugreifbar sind – auf
1159 eine neue eGK übertragen, wenn der Versicherte von seiner Krankenversicherung eine
1160 neue Karte ausgestellt bekommt.

1161 Der Versicherte kann die Datenbereiche auswählen, deren Daten er auf die Zielkarte
1162 übertragen will. Dafür muss der Datenbereich dieser Anwendung(en) auf der Zielkarte
1163 leer sein. In einer Datenübertragung können ein oder mehrere Datenbereiche übertragen
1164 werden. Der Versicherte kann die Datenübertragung erneut durchführen, solange noch
1165 nicht alle Datenbereiche übertragen wurden.

1166 Zum Zeitpunkt der Erstellung dieser Spezifikation kann in der KTR-AdV nur der
1167 Datenbereich DPE ausgewählt werden.

1168 Die unten beschriebene Lösung sieht vor, dass am KTR-AdV-Terminal für die eGK nur ein
1169 Slot zur Verfügung steht, so dass die beiden eGKs nacheinander gesteckt werden
1170 müssen. In diesem Ausnahmefall dürfen die medizinischen Daten des Versicherten über
1171 den Steckzyklus der Quellkarte hinaus in der AdV-App gespeichert werden. Nach dem
1172 Ende des Vorgangs müssen die Daten gelöscht werden.

1173 Die AdV-App steuert den Ablauf der Datenübertragung vom Lesen der Daten von der
1174 Quellkarte über den Wechsel der Karten bis zum Schreiben auf die neue Karte und
1175 Löschen der zwischengespeicherten Daten. Für die anwendungsspezifischen Lese- und
1176 Schreiboperationen ruft es interne Methoden der entsprechenden Fachmodule auf.

1177 Die Datenübertragung soll auch dann möglich sein, wenn das AUT-Zertifikat der
1178 Quellkarte zeitlich abgelaufen oder online ungültig ist. Daher muss die AdV-App eine eGK
1179 auch in diesem Fall akzeptieren.

1180 Bei den folgenden Beschreibungen wird angenommen, dass zu Beginn die Quellkarte
1181 steckt. Dies kann die AdV-App jedoch erst prüfen, wenn die Zielkarte gesteckt wurde und
1182 ihr AUT-Zertifikat ein neueres Gültigkeitsbeginn-Datum aufweist als das der anderen
1183 eGK.

1184 Falls das Gültigkeitsbeginn-Datum der Zielkarte kleiner als das Gültigkeitsbeginn-Datum
1185 der Quellkarte ist, wird die Kopieroperation abgebrochen. Weiterhin führt zum Abbruch,
1186 wenn die Zielkarte mathematisch oder zeitlich ungültig ist oder gesperrt wurde.

1187 **AdV-A_2548 - Auswahl der zu kopierenden Daten durch den Versicherten**

1188 Die AdV-App MUSS beim Start des Anwendungsfalls Datenübertragung bei Kartentausch
1189 und vor den Kopier-Operationen die Liste der zu kopierenden Anwendungen beim
1190 Versicherten abfragen. Dem Versicherten ist dafür die Liste der in der KTR Umgebung
1191 zugreifbaren und kopierbaren Anwendungen zur Auswahl anzubieten.[<=]

1192 **AdV-A_2549 - Reaktion auf Kartenevents während Anwendungsfall**
1193 **Datenübertragung bei Kartentausch**

1194 Die AdV-App MUSS, falls der Anwendungsfall "Datenübertragung bei Kartentausch
1195 durchführen" umgesetzt wird, während der gesamten Datenübertragung sicherstellen,
1196 dass die KVRN (Unveränderbarer Teil) der Quell- und Ziel-Karte mit der zum Beginn der

1197 Sitzung temporär gespeicherten KVNR (Unveränderbarer Teil) der Quell-Karte
1198 übereinstimmt und bei Ungleichheit die Sitzung nach Hinweis abbrechen.[<=]

1199 **AdV-A_2550 - Aufrechterhaltung der Sitzung des Versicherten bei gezogener**
1200 **Karte während Anwendungsfall Datenübertragung bei Kartentausch**

1201 Die AdV-App MUSS, falls der Anwendungsfall "Datenübertragung bei Kartentausch
1202 durchführen" umgesetzt wird und während des Anwendungsfalls die eGK des
1203 Versicherten aus dem Kartenterminal gezogen wird ohne dass der Versicherte die
1204 Operation explizit abbricht, die Sitzung des Versicherten für zwei Minuten aufrecht
1205 erhalten.[<=]

1206 **AdV-A_2551 - Keine Neuanmeldung des Versicherten bei Stecken der eGK**
1207 **während Anwendungsfall Datenübertragung bei Kartentausch**

1208 Die AdV-App MUSS, falls der Anwendungsfall "Datenübertragung bei Kartentausch
1209 durchführen" umgesetzt wird und während des Anwendungsfalls eine neue eGK mit
1210 derselben KVNR (Unveränderbarer Teil) des angemeldeten Versicherten in das
1211 Kartenterminal gesteckt wird, die aktuelle Sitzung des Versicherten für diese Karte
1212 übernehmen.[<=]

1213 **AdV-A_2552 - Anzeige einer Aufforderung zum Kartenwechsel**

1214 Die AdV-App MUSS, falls der Anwendungsfall "Datenübertragung bei Kartentausch
1215 durchführen" umgesetzt wird, dem Versicherten eine Aufforderung zum Kartenwechsel
1216 anzeigen, wenn während der Ausführung des Anwendungsfalls Datenübertragung ein
1217 Kartentausch von der Quell- zur Ziel-Karte nötig ist.[<=]

1218
1219

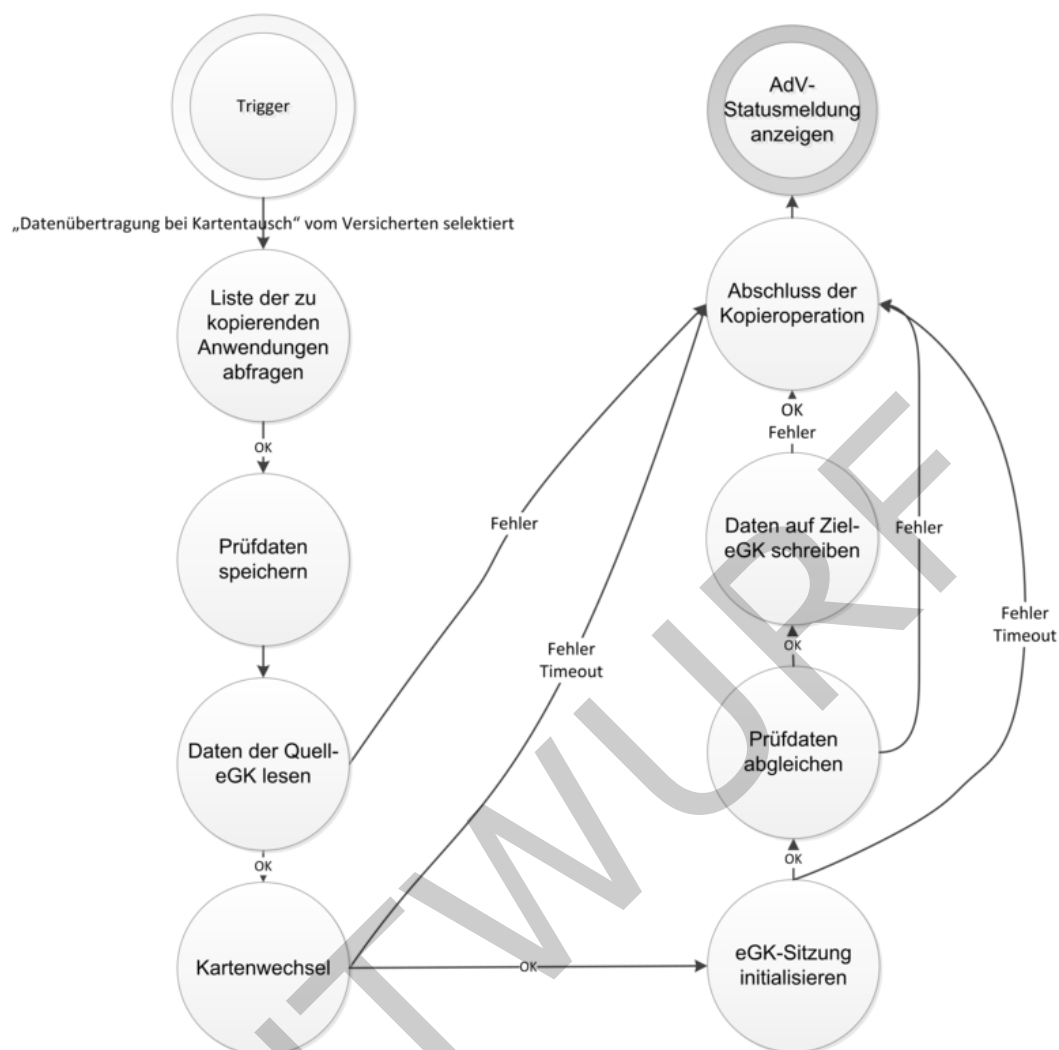


Abbildung 15: ABB_ADV_315 Standardablauf – Datenübertragung bei Kartentausch durchführen

AdV-A_2553 - AdV-App: Datenübertragung bei Kartentausch durchführen

Die AdV-App KANN den Anwendungsfall "Datenübertragung bei Kartentausch durchführen" umsetzen. Falls eine Umsetzung erfolgt, so muss die AdV-App diese gemäß TAB_ADV_324 vornehmen.

Tabelle 28: TAB_ADV_324 – Datenübertragung bei Kartentausch durchführen

Benennung des Anwendungsfalls	„Datenübertragung bei Kartentausch“
Hinweistext für den Versicherten	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"> • Quell- und Zielkarte (eGK) sind für den selben Versicherten personalisiert • Die Zielkarte ist neuer als die Quellkarte. • eGK Zielkarte: X.509 (Karteninhaberzertifikat) ist mathematisch und zeitlich gültig • eGK Zielkarte: X.509 (Karteninhaberzertifikat) ist Online gültig oder Onlinestatus unbekannt • Auf der Zielkarte sind die ausgewählten Datenbereiche leer (falls ein Datenbereich gefüllt ist, liefert putData einen Fehler).
Nachbedingung	<ul style="list-style-type: none"> • Anwendungsdaten auf neue eGK übertragen. • 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. • Auf der Quellkarte sind die bearbeiteten Anwendungen verborgen • 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.
Standardablauf	<p>Die Umsetzung ist in der Tabelle TAB_ADV_325 – Ablaufaktivitäten – Datenübertragung bei Kartentausch durchführen beschrieben.</p> <ol style="list-style-type: none"> 1. Liste der zu kopierenden Anwendungen abfragen 2. Prüfdaten speichern 3. Daten der Quell-eGK lesen 4. Kartenwechsel 5. AdV-Sitzung initialisieren 6. Prüfdaten abgleichen 7. Daten auf Ziel-eGK schreiben 8. Abschluss der Kopieroperation 9. AdV-Statusmeldung anzeigen

Diagramm	ABB_ADV_315 Standardablauf – Datenübertragung bei Kartentausch durchführen
----------	--

1232

1233

1234

Tabelle 29: TAB_ADV_325 – Ablaufaktivitäten – Datenübertragung bei Kartentausch durchführen

1. Liste der zu kopierenden Anwendungen abfragen	
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.
2. Prüfdaten speichern	
Daten der Quell-eGK in der AdV-App speichern	<ul style="list-style-type: none"> • ICCSN der Karte • KVN (Unveränderbarer Teil) des Versicherten • Gültigkeitsdatum des AUT-Zertifikats • Version des Objektsystems der eGK
<i>Beschreibung</i>	Die Daten der Quell-eGK werden für die spätere Prüfung der Ziel-eGK zwischengespeichert.
3. Daten der Quell-eGK lesen	
<i>Eingangsdaten</i>	
n*[Application]	Liste der Bezeichner der zu kopierenden Fachanwendungen Zulässige Bezeichner sind: DF . DPE

<i>Beschreibung</i>	<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>
4. Kartenwechsel	
<i>Beschreibung</i>	<ul style="list-style-type: none"> • Quellkarte auswerfen: Der Versicherte wird zum Ziehen der Quellkarte aufgefordert. • Wenn nach einem Timeout von 2 Minuten die Quellkarte nicht gezogen wurde, dann wird mit Punkt 9 Abschluss der Kopieroperation fortgesetzt. • Neue eGK anfordern: Der Versicherte wird zum Stecken seiner neuen eGK aufgefordert.
5. AdV-Sitzung initialisieren	
<i>Beschreibung</i>	<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>
6. Prüfdaten abgleichen	

<p><i>Beschreibung</i></p>	<p>Prüfdaten der neuen eGK mit denen der alten eGK vergleichen:</p> <ul style="list-style-type: none"> • Wenn $ICCSN_{alt} = ICCSN_{neu}$, 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." • Wenn $KVNR_{alt} \neq KVNR_{neu}$ (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. • Sei <i>validfrom</i> das Gültigkeitsbeginn-Datum des X.509-AUT-Zertifikats. Wenn $validfrom_{neu} < validfrom_{alt}$, dann Abbruch mit der Fehlermeldung "Falsche Reihenfolge. Bitte wiederholen Sie den Vorgang mit Ihrer alten Gesundheitskarte und stecken Sie dann erst Ihre neue Gesundheitskarte." <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"> • eGK Zielkarte: X.509 (Karteninhaberzertifikat) ist mathematisch und zeitlich gültig (PL_TUC_EGK_STATUS # Mathematische Gültigkeit & Gültigkeit zu Referenzzeitpunkt) • eGK Zielkarte: X.509 (Karteninhaberzertifikat) ist Online gültig oder Onlinestatus unbekannt (PL_TUC_EGK_STATUS # OCSP-Prüfung) <p>Bei Abbruch: gespeicherte Daten der Quellkarte verwerfen und eGK Sitzung beenden, falls der Karteninhaber nicht identisch ist.</p>
<p>7. Daten auf Ziel-eGK schreiben</p>	

<i>Beschreibung</i>	<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 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. }</pre>
8. Abschluss der Kopieroperation	
	<ul style="list-style-type: none"> • Alle zwischengespeicherten Anwendungsdaten aus dem Arbeitsspeicher entfernen
9. AdV-Statusmeldung anzeigen	
<i>Hinweis an den Versicherten</i>	<p>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.</p>

1235

1236 [\leq]

1237 6.1.6 Verwaltung der NFD

1238 In diesem Abschnitt sind die Anwendungsfälle für die Verwaltung des Notfalldatensatzes
1239 (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	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>

[≤]

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	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>

1261

1262 [\leq]1263 **6.1.6.3 PIN für NFD einschalten**

1264 Mit diesem Anwendungsfall soll die technische Notwendigkeit der Verifikation der
 1265 MRPIN.NFD eingeschaltet werden.

1266 **AdV-A_2471 - AdV-App: PIN für NFD einschalten**

1267 Die AdV-App MUSS den Anwendungsfall „PIN für NFD einschalten“ gemäß
 1268 TAB_ADV_357umsetzen.

1269

1270 **Tabelle 32: TAB_ADV_357 – PIN für NFD einschalten**

Benennung des Anwendungsfalls	„PIN-Schutz für Notfalldaten einschalten“
Hinweistext für den Versicherten	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 <code>Identifikator = MRPIN.NFD</code>

1271
1272 [\leq]

1273 6.1.6.4 PIN für NFD ausschalten

1274 Mit diesem Anwendungsfall soll die technische Notwendigkeit der Verifikation der
1275 MRPIN.NFD ausgeschaltet werden.

1276 **Adv-A_2472 - Adv-App: PIN für NFD ausschalten**

1277 Die Adv-App MUSS den Anwendungsfall „PIN für NFD ausschalten“ gemäß TAB_ADV_358
1278 umsetzen.
1279

1280 **Tabelle 33: TAB_ADV_358 – PIN für NFD ausschalten**

Benennung des Anwendungsfalls	„PIN-Schutz für Notfalldaten ausschalten“
Hinweistext für den Versicherten	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 <code>Identifikator = MRPIN.NFD</code>

1281
1282 [\leq]

1283 6.1.7 Verwaltung des DPE

1284 In diesem Abschnitt sind die Anwendungsfälle für die Verwaltung der Anwendung
1285 Datensatz ‚Persönliche Erklärungen‘ (DPE) beschrieben.

1286 **Adv-A_2473 - Adv-App: Hinweis bei verborgenem DPE**

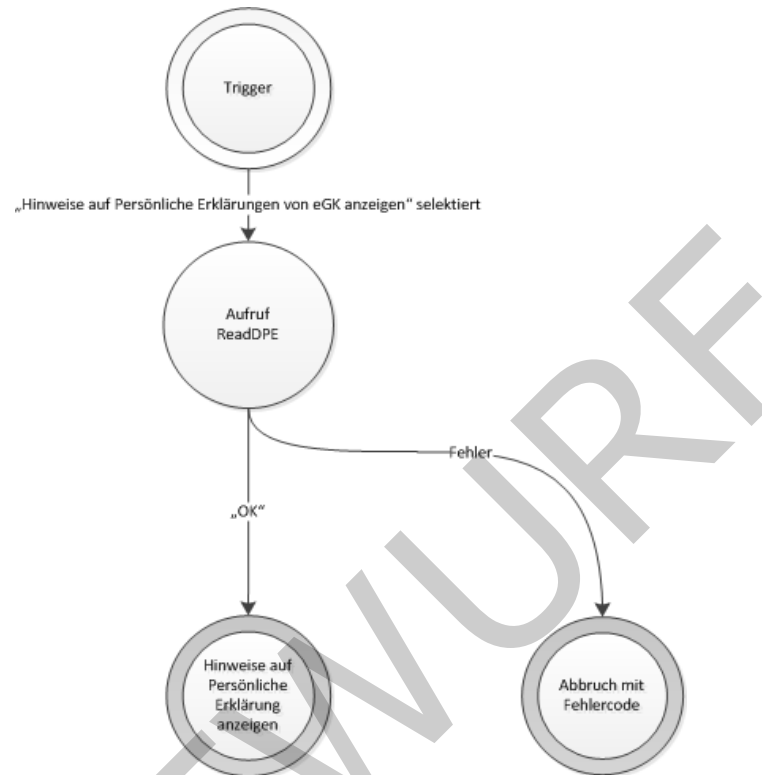
1287 Die Adv-App MUSS beim Aufruf des Bereiches mit den Anwendungsfälle zur Anwendung
1288 DPE, wenn der DPE auf der eGK des Versicherten verborgen ist, einen Hinweis an den
1289 Versicherten ausgeben, dass die Anwendung verborgen ist und die Daten im Notfall nicht
1290 gelesen werden können.[\leq]

1291 6.1.7.1 Persönliche Erklärung (DPE) von eGK anzeigen

1292 Mit der Umsetzung dieses Anwendungsfalls soll dem Versicherten der auf seiner eGK
1293 gespeicherte Datensatz Persönliche Erklärungen (DPE) zur Anzeige gebracht werden.

1294 Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall AdV-
1295 UC_121: „DPE von eGK anzeigen“ ausgeführt werden müssen.

1296
1297



1298
1299
1300

Abbildung 16: ABB_ADV_359 – Ablauf des AdV-UC_121: „DPE von eGK anzeigen“

1302

AdV-A_2474 - AdV-App: DPE von eGK anzeigen

1303 Die AdV-App MUSS den Anwendungsfall „DPE von eGK anzeigen“ gemäß TAB_ADV_359
1304 umsetzen.
1305
1306

Tabelle 34: TAB_ADV_359 – DPE von eGK anzeigen

Benennung des Anwendungsfalls	„Hinweise auf Persönliche Erklärungen von eGK anzeigen“
Hinweistext für den Versicherten	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"> 1. DPE-LeseRequest erzeugen 2. DPE-LeseResponse verarbeiten 3. DPE anzeigen
Diagramm	Abbildung ABB_ADV_359 – Ablauf des Adv-UC_121: „DPE von eGK anzeigen“

1308

1309

Tabelle 35: TAB_ADV_360 – Ablaufaktivitäten – DPE von eGK anzeigen

1. DPE-LeseRequest erzeugen	
Operation	ReadDPE
Eingangsdaten	
(keine)	
2. DPE-LeseResponse verarbeiten	
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.
3. DPE anzeigen	

	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.
--	---

1310
1311
1312

[<=]

1313 **6.1.7.2 Persönliche Erklärung (DPE) auf eGK ändern**

1314 Mit der Umsetzung dieses Anwendungsfalls ändert der Versicherte eine oder mehrere
1315 Hinweise auf persönliche Erklärungen des auf der eGK gespeicherten Datensatzes
1316 Persönliche Erklärungen (DPE). Dem Ändern eines oder mehrerer Erklärungen muss ein
1317 Lesen der DPE vorausgehen, da der DPE nur im Ganzen auf die Karte geschrieben
1318 werden kann.

1319 Wenn noch kein DPE auf der eGK gespeichert ist, dann kann der Versicherte einen DPE
1320 anlegen.

1321 Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall AdV-
1322 UC_122: „DPE auf eGK ändern“ ausgeführt werden müssen.

ENTWURF

1323
1324

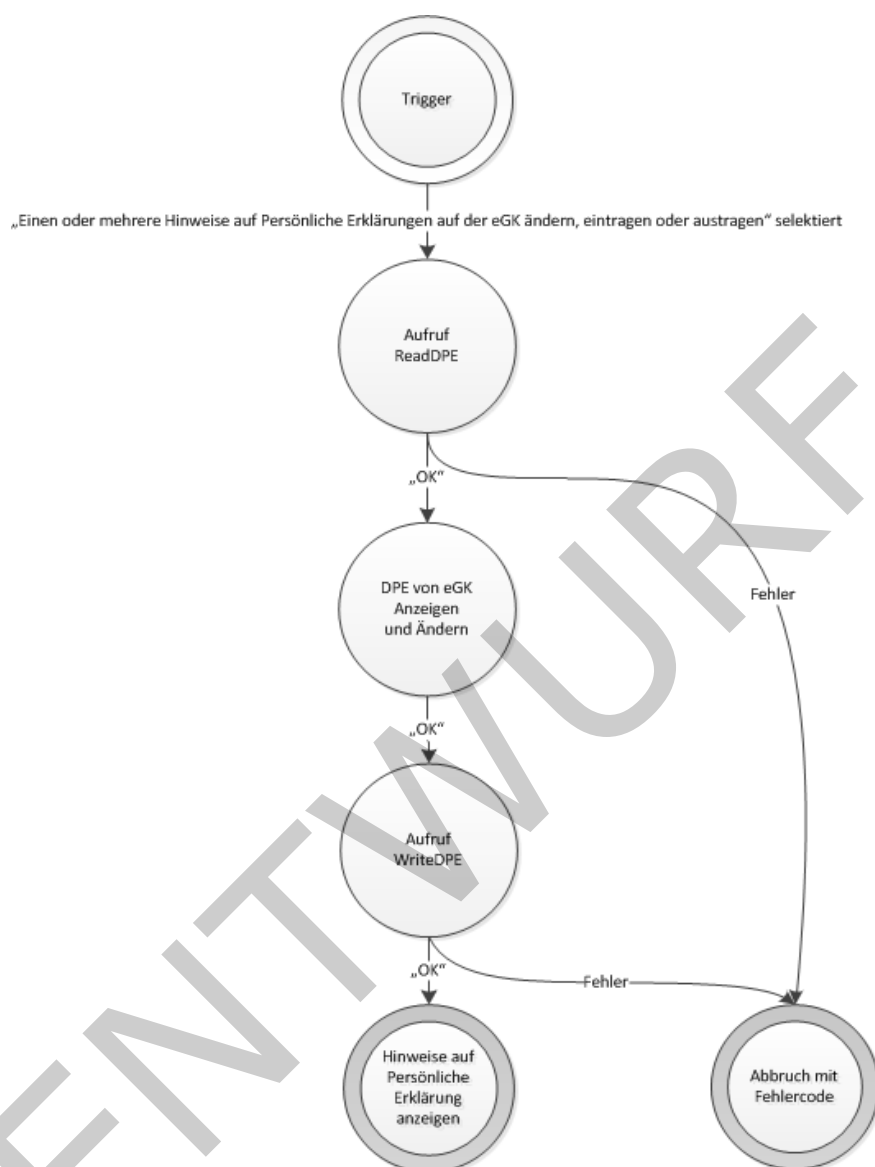


Abbildung 17: ABB_ADV_361 – Ablauf des AdV-UC_122: „DPE auf eGK ändern“

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	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"> 1. DPE von eGK lesen und anzeigen 2. Eintrag im DPE editieren 3. DPE-SchreibRequest erzeugen 4. PE-SchreibResponse verarbeiten 5. Änderungsbestätigung und geänderte DPE anzeigen
Diagramm	Abbildung ABB_ADV_361 – Ablauf des AdV-UC_122: „DPE auf eGK ändern“

1333

1334

Tabelle 37: TAB_ADV_362 – Ablaufaktivitäten – DPE auf eGK ändern

1. DPE von eGK lesen und anzeigen	
Hinweis zur Umsetzung	Das Lesen der DPE soll gemäß Tabelle "TAB_ADV_359 – DPE von eGK anzeigen" erfolgen.
2. Persönliche Erklärung in DPE editieren	

	<p>Die AdV-App soll es dem Versicherten ermöglichen, einzelne Hinweise auf Persönliche Erklärungen des DPE zu ändern. Dabei sollen die übrigen Hinweise von der Änderung nicht beeinflusst werden, d.h. das Ändern eines Elementes führt NICHT zum Ändern eines anderen Elementes. Editierbar sind die folgenden Elemente <code>DPE_Gewebe_Organspendeerklärung</code>, <code>DPE_Vorsorgevollmacht</code> und <code>DPE_Patientenverfügung</code> 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>
3. DPE-SchreibRequest erzeugen	
Operation	WriteDPE
Eingangsdaten	
DPEDocument	Auf die eGK des Versicherten zu schreibender DPE
Beschreibung	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.
4. DPE-SchreibResponse verarbeiten	
Rückgabedaten	
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.
5. DPE-Änderungsbestätigung anzeigen	
<i>Hinweis an den Versicherten</i>	Der <i>Status</i> 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.

1335

1336 [**<=**]

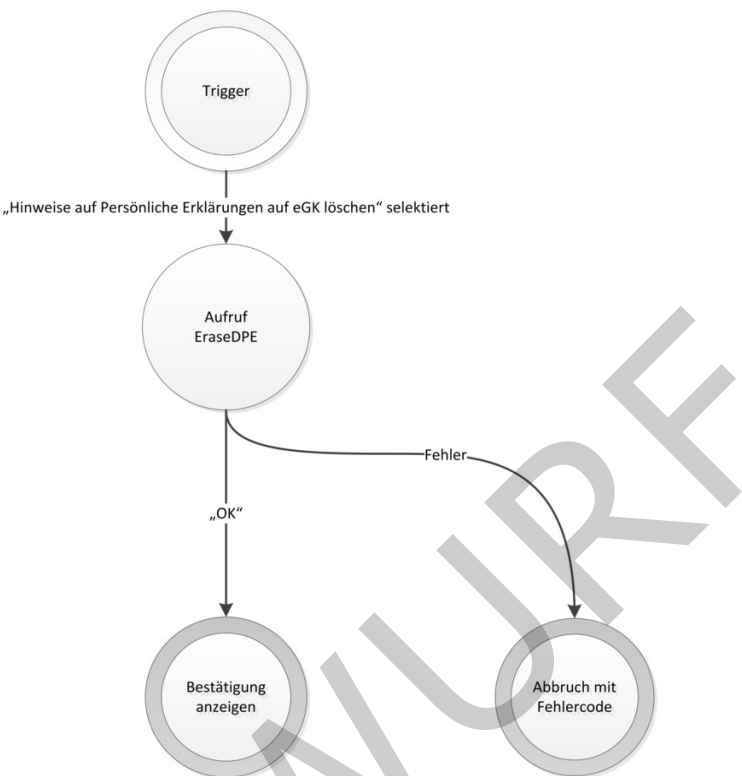
1337

1338 **6.1.7.3 Persönliche Erklärung (DPE) auf eGK löschen**

1339 Mit der Umsetzung dieses Anwendungsfalls löscht der Versicherte den gesamten
1340 Datensatz seiner persönlichen Erklärungen (DPE) auf der eGK.

1341 Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall AdV-
1342 UC_123: „DPE auf eGK löschen“ ausgeführt werden müssen.

1343
1344



1345
1346
1347
1348

Abbildung 18: ABB_ADV_363 – Ablauf des AdV-UC_123: „DPE auf eGK löschen“

1349
1350
1351
1352

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.

1353 **Tabelle 38: TAB_ADV_363 – DPE auf eGK löschen**

Benennung des Anwendungsfalls	„Alle Hinweise auf Persönliche Erklärungen löschen“
Hinweistext für den Versicherten	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	Die Umsetzung ist in der Tabelle TAB_ADV_364 – Ablaufaktivitäten – DPE auf eGK löschen beschrieben. <ol style="list-style-type: none"> 1. Bestätigung des Löschwunsches vom Versicherten einholen 2. DPE-LöschRequest erzeugen 3. DPE-LöschResponse verarbeiten 4. DPE Löschbestätigung anzeigen
Diagramm	Abbildung ABB_ADV_363 – Ablauf des Adv-UC_123: „DPE auf eGK löschen“

1354

1355

Tabelle 39: TAB_ADV_364 – Ablaufaktivitäten – DPE auf eGK löschen

1. Bestätigung des Löschwunsches vom Versicherten einholen	
	Zum Starten der Löschaktion des Datensatzes der persönlichen Erklärungen soll der Versicherte seine Auswahl noch einmal bestätigen.
2. DPE-LöschRequest erzeugen	
Operation	EraseDPE
Eingangsdaten	
keine	Es wird der komplette DPE Datensatz gelöscht.
3. DPE-LöschResponse verarbeiten	
Rückgabedaten	
Keine (bzw. Fehlermeldung)	Im Erfolgsfall werden keine Daten von der Operation zurückgegeben. Im Fehlerfall wird eine Fehlermeldung zurückgegeben.
Beschreibung	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.

4. DPE-Löschbestätigung anzeigen	
<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.

1356

1357 [**<=**]1358 **6.1.7.4 PIN für DPE einschalten**

1359 Mit diesem Anwendungsfall kann der Versicherte die technische Notwendigkeit der
 1360 Verifikation der MRPIN.DPE einschalten.

1361 **Adv-A_2477 - Adv-App: PIN für DPE einschalten**

1362 Die Adv-App MUSS den Anwendungsfall „PIN für DPE einschalten“ gemäß TAB_ADV_365
 1363 umsetzen.

1364

1365 **Tabelle 40: TAB_ADV_365 – PIN für DPE einschalten**

Benennung des Anwendungsfalls	„PIN-Schutz für Persönliche Erklärungen einschalten“
Hinweistext für den Versicherten	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 <code>Identifikator = MRPIN.DPE</code>

1366

1367 [**<=**]1368 **6.1.7.5 PIN für DPE ausschalten**

1369 Mit diesem Anwendungsfall kann der Versicherte die technische Notwendigkeit der
 1370 Verifikation der MRPIN.DPE ausschalten.

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	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 <code>Identifikator = MRPIN.DPE</code>

[<=]

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	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 <code>Identifikator = DF.DPE</code>

1387

1388 [\leq]1389 **6.1.7.7 Verborgene DPE auf eGK sichtbar machen**

1390 Mit diesem Anwendungsfall kann der Versicherte den verborgenen Datensatz Persönliche
 1391 Erklärungen auf seiner eGK wieder sichtbar machen.

1392 **Adv-A_2480 - Adv-App: Verborgenen DPE auf eGK sichtbar machen**

1393 Die Adv-App MUSS den Anwendungsfall "Verborgenen DPE auf eGK sichtbar machen"
 1394 gemäß TAB_ADV_368 umsetzen.

1395

1396 **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	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 <code>Identifikator = DF.DPE</code>

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>
------------------------------	--

1397

1398 [\leq]1399 **6.1.8 Verwaltung eMP/AMTS**

1400 In diesem Abschnitt sind die Anwendungsfälle für die Verwaltung der Daten des
 1401 elektronischen Medikationsplans und zur Prüfung der Arzneimitteltherapiesicherheit
 1402 beschrieben. Ein Zugriff auf medizinische Daten ist nicht möglich.

1403 **6.1.8.1 AMTS-Vertreter-PIN ändern**

1404 Mit der Umsetzung dieses Anwendungsfalls kann die AMTS-Vertreter-PIN auf der eGK
 1405 gesetzt oder geändert werden.

1406 Für die Umsetzung wird der in Kap. 6.1.4.3.1 PIN ändern beschriebene generische
 1407 Anwendungsfall genutzt.

1408 **Adv-A_2481 - Adv-App: AMTS-Vertreter-PIN ändern**

1409 Die Adv-App MUSS den Anwendungsfall „AMTS-Vertreter-PIN ändern“ gemäß
 1410 TAB_ADV_369 umsetzen.

1411

1412 **Tabelle 44: TAB_ADV_369 – AMTS-Vertreter-PIN ändern**

Benennung des Anwendungsfalls	„Vertreter-PIN ändern“
Hinweistext für den Versicherten	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 <code>Identifikator = PIN.AMTS_REP</code>

1413
1414 [\leq]

1415 **6.1.8.2 AMTS-Vertreter-PIN entsperren**

1416 Mit diesem Anwendungsfall kann der Versicherte die gesperrten AMTS-Vertreter-PIN
1417 entsperren.

1418 Für die Umsetzung wird der 6.1.4.3.2 PIN auf eGK entsperren beschriebene generische
1419 Anwendungsfall genutzt.

1420 **Adv-A_2482 - Adv-App: AMTS-Vertreter-PIN entsperren**

1421 Die Adv-App MUSS den Anwendungsfall „AMTS-Vertreter-PIN entsperren“ gemäß
1422 TAB_ADV_370 umsetzen.

1423

1424 **Tabelle 45: TAB_ADV_370 – AMTS-Vertreter-PIN entsperren**

Benennung des Anwendungsfalls	„Vertreter-PIN entsperren“
Hinweistext für den Versicherten	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 entsperret.
Umsetzung	Gemäß Beschreibung des Anwendungsfalls Adv-UC_02: „PIN auf eGK entsperren“ mit dem Parameter <code>Identifikator = PIN.AMTS_REP</code>

1425
1426 [\leq]

1427 **6.1.8.3 eMP/AMTS Datensatz verbergen**

1428 Mit der Umsetzung dieses Anwendungsfalls soll der eMP/AMTS-Datensatz des
1429 Versicherten auf seiner eGK verborgen werden.

1430 **Adv-A_2483 - Adv-App: eMP/AMTS-Datensatz verbergen**

1431 Die Adv-App MUSS den Anwendungsfall „eMP/AMTS-Datensatz auf eGK verbergen“
1432 gemäß TAB_ADV_371 umsetzen.

1433

1434 **Tabelle 46: TAB_ADV_371 – eMP/AMTS-Datensatz auf eGK verbergen**

Benennung des Anwendungsfalls	„Medikationsplan verbergen“
-------------------------------	-----------------------------

Hinweistext für den Versicherten	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 <code>Identifikator = DF.AMTS</code>

1435

1436 [\leq]

1437 6.1.8.4 Verborgenen eMP/AMTS Datensatz sichtbar machen

1438 Mit der Umsetzung dieses Anwendungsfalls soll der verborgene eMP/AMTS-Datensatz des
1439 Versicherten auf seiner eGK sichtbar gemacht werden.

1440 Adv-A_2484 - Adv-App: Verborgenen eMP/AMTS-Datensatz sichtbar machen

1441 Die Adv-App MUSS den Anwendungsfall „Verborgene eMP/AMTS-Datensatz auf eGK
1442 sichtbar machen“, gemäß TAB_ADV_372 umsetzen.

1443

1444 Tabelle 47: TAB_ADV_372 – Verborgene eMP/AMTS-Datensatz auf eGK sichtbar machen

Benennung des Anwendungsfalls	„Verborgenen Medikationsplan wieder anzeigen“
Hinweistext für den Versicherten	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 <code>Identifikator = DF.AMTS</code>
-----------	--

[<=]

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	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 <code>Identifikator = MRPIN.AMTS</code>

[<=]

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.

1466 **Tabelle 49: TAB_ADV_374 – PIN für AMTS ausschalten**

Benennung des Anwendungsfalls	„PIN-Schutz für Medikationsplan ausschalten“
Hinweistext für den Versicherten	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 <code>Identifikator = MRPIN.AMTS</code>

1467
1468 [\leq]

1469 6.1.9 Fachanwendungsunabhängige Anwendungsfälle

1470 Dieses Kapitel beschreibt Anwendungsfälle, die keiner spezifischen Fachanwendung
1471 zugeordnet sind.

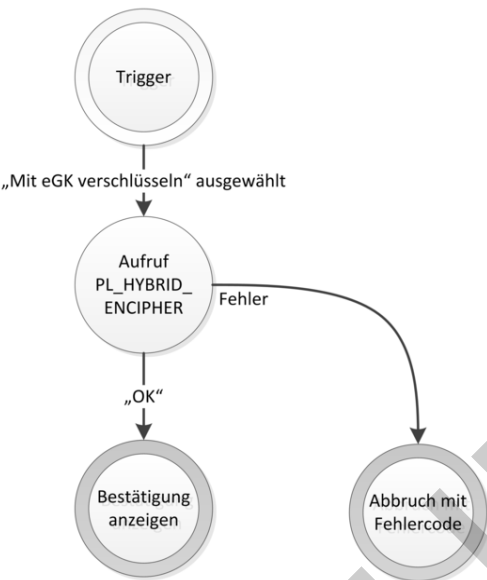
1472 6.1.9.1 Mit eGK verschlüsseln

1473 Der Anwendungsfall ermöglicht es dem Versicherten, mit der Adv-App ein Dokument mit
1474 der eGK zu verschlüsseln.

1475 Dieser Anwendungsfall zielt auf die @home-Umgebung, da der Versicherte dort auf einen
1476 Datenträger (z.B. USB-Stick oder lokale Festplatte) mit privaten Dokumenten zugreifen
1477 kann. In der @home-Umgebung kann in dem Anwendungsfall eine Datei auf einem
1478 lokalen Datenträger des Versicherten selektiert und der Ablageort für das Ergebnis
1479 definiert werden.

1480 Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall Adv-UC_25:
1481 „Mit eGK verschlüsseln“ ausgeführt werden müssen.

1482
1483



1484
1485
1486

Abbildung 19: ABB_ADV_322 – Ablauf des AdV-UC_25: "Mit eGK verschlüsseln"

1487
1488
1489
1490
1491

AdV-A_2487 - AdV-App: AdV-UC_25: „Mit eGK verschlüsseln“
Die AdV-App KANN den Anwendungsfall AdV-UC_25: „Mit eGK verschlüsseln“ umsetzen. Falls eine Umsetzung erfolgt, so muss die AdV-App diese gemäß TAB_ADV_375 vornehmen.

1492 **Tabelle 50: TAB_ADV_375 – AdV-UC_25: „Mit eGK verschlüsseln“**

Benennung des Anwendungsfalls	„Mit eGK verschlüsseln“
Hinweistext für den Versicherten	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	<p>Die Umsetzung ist in der Tabelle TAB_ADV_376 – Ablaufaktivitäten – Mit eGK verschlüsseln beschrieben.</p> <ol style="list-style-type: none"> 1. Eingangsdaten ermitteln 2. PL_TUC_HYBRID_ENCIPHER aufrufen 3. PL_TUC_HYBRID_ENCIPHER Ergebnis verarbeiten 4. Ausgangsdaten zurückgeben und Ergebnis anzeigen
Diagramm	Abbildung ABB_ADV_322 – Ablauf des Adv-UC_25: "Mit eGK verschlüsseln"

1493

1494

Tabelle 51: TAB_ADV_376 – Ablaufaktivitäten – Mit eGK verschlüsseln

1. Eingangsdaten ermitteln	
	Der Versicherte wählt das zu verschlüsselnde Dokument aus.
2. PL_TUC_HYBRID_ENCIPHER aufrufen	
Plattformbaustein	PL_TUC_HYBRID_ENCIPHER
<i>Eingangsdaten</i>	
Dokument	Vom Versicherten ausgewähltes Dokument.
Zertifikat	Zertifikat „C.CH.ENC“ gemäß PL_TUC_CARD_INFORMATION
3. PL_TUC_HYBRID_ENCIPHER Ergebnis verarbeiten	
<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.

Beschreibung	<p>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.</p> <p>Im Fehlerfall wird im Folgeschritt der Versicherte informiert.</p>
4. Ausgangsdaten zurückgeben und Ergebnis anzeigen	
Hinweis an den Versicherten	<p>Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige gebracht und das verschlüsselte Dokument zurückgegeben.</p> <p>Im Fehlerfall werden dem Versicherten entsprechende Fehlerinformationen ausgegeben.</p>

1495
1496
1497

[<=]

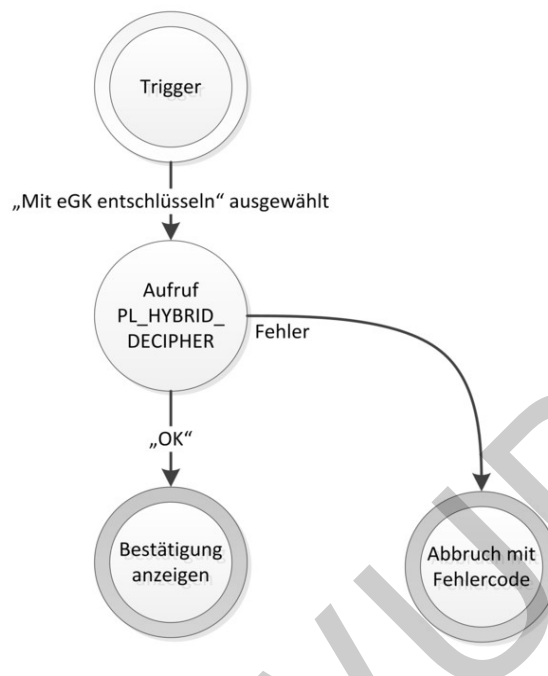
1498 **6.1.9.2 Mit eGK entschlüsseln**

1499 Der Anwendungsfall ermöglicht es dem Versicherten, mit der Adv-App ein Dokument mit
1500 der eGK zu entschlüsseln.

1501 Analog zum Anwendungsfall „Mit eGK verschlüsseln“ zielt dieser Anwendungsfall auf die
1502 @home-Umgebung, da der Versicherte dort auf seine privaten Dokumente zugreifen
1503 kann.

1504 Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall Adv-UC_26:
1505 „Mit eGK entschlüsseln“ ausgeführt werden müssen.

1506
1507



1508
1509
1510

Abbildung 20: ABB_ADV_324 – Ablauf des AdV-UC_26: „Mit eGK entschlüsseln“

1511
1512
1513
1514
1515

AdV-A_2488 - AdV-App: AdV-UC_26: „Mit eGK entschlüsseln“

Die AdV-App KANN den Anwendungsfall AdV-UC_26: „Mit eGK entschlüsseln“ umsetzen. Falls eine Umsetzung erfolgt, so muss die AdV-App diese gemäß TAB_ADV_377 vornehmen.

1516

Tabelle 52: TAB_ADV_377 – AdV-UC_26: „Mit eGK entschlüsseln“

Benennung des Anwendungsfalls	"Mit eGK entschlüsseln"
Hinweistext für den Versicherten	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"> 1. Eingangsdaten ermitteln 2. PL_TUC_HYBRID_DECIPHER aufrufen 3. PL_TUC_HYBRID_DECIPHER Ergebnis verarbeiten 4. Ausgangsdaten zurückgeben und Ergebnis anzeigen
Diagramm	Abbildung ABB_ADV_324 – Ablauf des Adv-UC_26: „Mit eGK entschlüsseln“

1517

1518

Tabelle 53: TAB_ADV_378 – Ablaufaktivitäten – Mit eGK entschlüsseln

1. Eingangsdaten ermitteln	
	Der Versicherte wählt das – mit seiner eGK - zu entschlüsselnde Dokument aus.
2. PL_TUC_HYBRID_DECIPHER aufrufen	
Plattformbaustein	PL_TUC_HYBRID_DECIPHER
<i>Eingangsdaten</i>	
Dokument	Vom Versicherten ausgewähltes Dokument.
3. PL_TUC_HYBRID_DECIPHER Ergebnis verarbeiten	
<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.

4. Ausgangsdaten zurückgeben und Ergebnis anzeigen	
<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.

1519
1520
1521

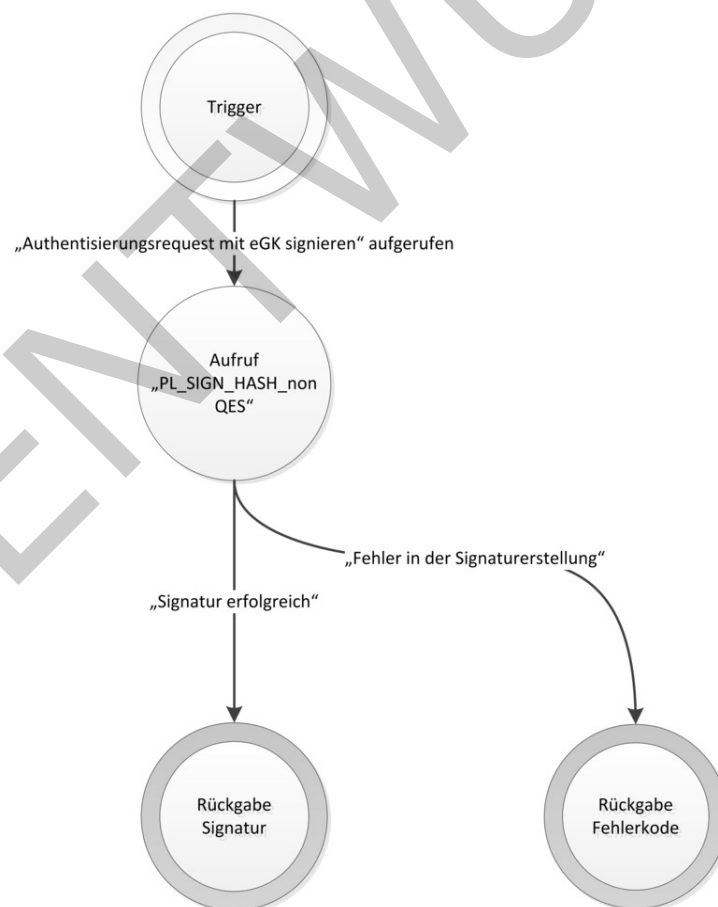
[<=]

1522 6.1.9.3 Authentisierungsrequest mit eGK signieren

1523 Die Operation versteht unter Verwendung des AUT-Zertifikates der eGK eine Message
1524 (Binärstring/Hashwert) mit einer nicht-qualifizierten elektronischen Signatur. Die
1525 Operation verhält sich konform zu [TR-03112-4#3.5.5] (Crypto Services/Sign).

1526 Die folgende Abbildung zeigt informativ, welche Schritte für Operation
1527 „Authentisierungsrequest mit eGK signieren“ ausgeführt werden müssen.

1528
1529



1530
1531
1532

Abbildung 21: ABB_ADV_379 – Ablauf des AdV-UC_27 „Authentisierungsrequest mit eGK signieren“

1533

1534 **AdV-A_2489 - AdV-App: AdV-UC_27: „Authentisierungsrequest mit eGK**
 1535 **signieren“**

1536 Die AdV-App KANN den Anwendungsfall AdV-UC_27: „Authentisierungsrequest mit eGK
 1537 signieren“ umsetzen. Falls eine Umsetzung erfolgt, so muss die AdV-App diese gemäß
 1538 TAB_ADV_379 vornehmen.
 1539

1540 **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	Die Umsetzung ist in der Tabelle TAB_ADV_380 – Ablaufaktivitäten – Authentisierungsrequest mit eGK signieren beschrieben. 1. PL_TUC_SIGN_HASH_nonQES aufrufen 2. PL_TUC_SIGN_HASH_nonQES Ergebnis verarbeiten 3. Ausgangsdaten zurückgeben
Diagramm	Abbildung ABB_ADV_379 – Ablauf des AdV-UC_27 „Authentisierungsrequest mit eGK signieren“

1541

1542 **Tabelle 55: TAB_ADV_380 – Ablaufaktivitäten – Authentisierungsrequest mit eGK**
 1543 **signieren**

1. PL_TUC_SIGN_HASH_nonQES aufrufen	
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).
2. PL_TUC_SIGN_HASH_nonQES Ergebnis verarbeiten	
<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.
3. Ausgangsdaten zurückgeben	
<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.

1544

1545 [**<=**]1546 **6.1.9.4 Zertifikat von eGK lesen**

1547 Anwendungsfall AdV-UC_24: Zertifikat von eGK lesen wird ausgelöst, wenn ein externes
 1548 Programm oder Clientsystem von der eGK des Versicherten ein Zertifikat lesen will.

1549 Die folgende Abbildung zeigt informativ, welche Schritte für Anwendungsfall AdV-UC_24:
 1550 Zertifikat von eGK lesen ausgeführt werden müssen.

1551
1552



1553
1554
1555

Abbildung 22: ABB_ADV_381 – Ablauf AdV-UC_24: Zertifikat von eGK lesen

1557
1558

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“ umsetzen. Falls eine Umsetzung erfolgt, so muss die AdV-App diese gemäß TAB_ADV_381 vornehmen.

1563

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. 1. Zertifikat in PL_TUC_CARD_INFORMATION auswählen (C.CH.ENC oder C.CH.ENCV) 2. Zertifikat zurückgeben
Diagramm	Abbildung ABB_ADV_381 – Ablauf Adv-UC_24: Zertifikat von eGK lesen

1565

1566

Tabelle 57: TAB_ADV_382 – Ablaufaktivitäten – Adv-UC_24: Zertifikat von eGK lesen

1. PL_TUC_CARD_INFORMATION auslesen	
Plattformbaustein	PL_TUC_CARD_INFORMATION
<i>Eingangsdaten</i>	
Zertifikat	C.CH.ENC oder C.CH.ENCV als Identifikator des Zertifikats
2. PL_TUC_CARD_INFORMATION Ergebnis verarbeiten	
<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.
3. Ausgangsdaten zurückgeben	

Beschreibung	Das gewünschte Zertifikat wird an den aufrufenden Anwendungsfall zurückgegeben.
--------------	---

[<=]

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 [gemSpec_Systemprozesse_dezTI].

Die KTR-Adv verwendet die in der Tabelle TAB_FM_ePA_KTR_019 dargestellten Plattformleistungen.

Tabelle 58: TAB_AdV_302 - Verwendete Plattformleistungen

Kürzel	Bezeichnung
PL_TUC_CARD_ACTIVATE_APPLICATION	Anwendung aktivieren
PL_TUC_CARD_CHANGE_PIN	PIN ändern
PL_TUC_CARD_DEACTIVATE_APPLICATION	Anwendung deaktivieren
PL_TUC_CARD_DISABLE_PIN	PIN-Schutz abschalten
PL_TUC_CARD_ENABLE_PIN	PIN-Schutz einschalten
PL_TUC_CARD_INFORMATION	Gesammelte Statusinformationen zu einer Karte
PL_TUC_CARD_RESET	Rücksetzen einer Karte
PL_TUC_CARD_UNBLOCK_PIN	PIN mit PUK entsperren
PL_TUC_CARD_VERIFY_PIN	Benutzer verifizieren
PL_TUC_EGK_APPEND_PROTOCOL	Zugriff auf eGK protokollieren
PL_TUC_EGK_READ_PROTOCOL	Auslesen des Zugriffsprotokolls der eGK
PL_TUC_EGK_STATUS	Gültigkeit der eGK prüfen

PL_TUC_HYBRID_DECIPHER	Hybrid entschlüsseln
PL_TUC_HYBRID_ENCIPHER	Hybrid verschlüsseln
PL_TUC_SIGN_HASH_nonQES	mit TI-Identität nonQES signieren

1582

1583 Zusätzlich muss in der Realisierung der Leistung der Plattform – wie in 2.2 beschrieben –
 1584 festgelegt werden, wie umgebungsspezifische Operationen an der Schnittstelle zu den
 1585 Leistungen der TI-Plattform umgesetzt werden sollen. Diese Festlegungen werden in den
 1586 folgenden Abschnitten festgelegt.

1587 6.2.1 Transportschnittstelle für Kartenkommandos

1588 Der hier beschriebene Produkttyp KTR-AdV ist als reines Softwareprodukt konzipiert. Als
 1589 solches muss die KTR-AdV eine Schnittstelle zu Karten der TI über ein Kartenterminal
 1590 herstellen. Diese Schnittstelle muss die von den Plattformprozessen erzeugten,
 1591 kartenverständlichen APDUs an die Karte übertragen und wird im Folgenden als
 1592 ENV_TUC_CARD_APDU_TRANSPORT bezeichnet. Neben proprietären
 1593 Schnittstellentreibern von Kartenterminalherstellern existieren eine Reihe standardisierter
 1594 Schnittstellen, die auch von verschiedenen Betriebssystemen zur Anbindung
 1595 handelsüblicher Kartenterminals unterstützt werden.

1596 **AdV-A_2492 - Transportschnittstelle für Kartenkommandos**

1597 Die KTR-AdV MUSS eine Transportschnittstelle für die Übertragung von SmartCard-
 1598 APDUs gegen die Standards CT-API und PCSC implementieren. [<=]

1599 **AdV-A_2493 - Ergänzende Standards für Transportschnittstelle**

1600 Die KTR-AdV KANN eine Transportschnittstelle für die Übertragung von SmartCard-APDUs
 1601 auf Basis des SICCT-Protokolls, gegen den Standard CCID und gegen proprietäre
 1602 Hardwaretreiber eines Kartenterminalherstellers implementieren. [<=]

1603 **AdV-A_2494 - Handbuch: Liste unterstützter Kartenterminals**

1604 Der Hersteller der KTR-AdV MUSS im Handbuch ausweisen, welche Standards und
 1605 Schnittstellen zu Kartenterminals die KTR-AdV unterstützt und MUSS eine Liste mit
 1606 handelsüblichen Kartenterminals angeben, die nachweislich mit dieser Ausprägung der
 1607 KTR-AdV funktionieren. [<=]

1608 Auf Seiten des Versicherten können Kartenterminalvarianten der Sicherheitsklassen 1
 1609 (reine Kontaktiereinheit), 2 (Kartenterminal mit eigenem PIN-Pad) oder 3 (PIN-Pad plus
 1610 Display) zum Einsatz kommen. Zusätzlich ist die Ausstattung des eingesetzten
 1611 Kartenterminals (Klasse 1, 2 oder 3) mit einer NFC-Schnittstelle möglich. Der Hersteller
 1612 der KTR-AdV muss die von den Varianten gebotenen Features geeignet nutzen.

1613 **AdV-A_2499 - PIN-Eingabe nicht speichern**

1614 Die KTR-AdV DARF ein eingegebenes PIN-Geheimnis NICHT temporär und NICHT
 1615 persistent speichern. [<=]

1616 **AdV-A_2562 - PIN-Geheimnis ausschließlich an Karte übermitteln**

1617 Die KTR-AdV MUSS sicherstellen, dass das eingegebene PIN-Geheimnis ausschließlich an
 1618 die Karte und nicht an andere Adressaten übermittelt wird. [<=]

1619 Das temporäre Speichern bezieht sich bei der Verwendung eines Kartenterminals der
 1620 Sicherheitsklasse 1 auf das Verwenden der PIN über den Anwendungsfall hinaus, für den
 1621 die PIN-Eingabe erfolgt ist, z.B. Caching während einer Sitzung. Gelangt die KTR-AdV bei
 1622 der Verwendung eines Kartenterminals der Sicherheitsklassen 2 und 3 ggfs. durch

1623 Fehlkonfiguration in Kenntnis der PIN, darf es diese ebenfalls nicht temporär und nicht
1624 persistent speichern.

1625 Auf Seite der Komponente AdV-Server in einem Rechenzentrum sind zusätzliche
1626 Varianten der Einbeziehung der Identitäten der Kostenträger in die Kartenoperationen
1627 möglich, wie z.B. Nutzung einer Webservice-Schnittstelle zu einem HSM oder das SICCT-
1628 Protokoll zur Anbindung eines HSM-B.

1629 **6.2.1.1 Kartenterminals der Sicherheitsklasse 1**

1630 Kartenterminals der Sicherheitsklasse 1 verfügen über keine Sicherheitsmerkmale, sie
1631 sind eine reine Kontaktiereinheit einer SmartCard. Sämtliche Geheimnis-Eingaben und
1632 Hinweistext-Ausgaben müssen über die KTR-AdV mittels Bildschirm und Tastatur/Maus
1633 erfolgen.

1634 **AdV-A_2495 - Klasse 1: PIN-Eingabe**

1635 Die KTR-AdV MUSS die PIN-/PUK-Eingabe über ein angeschlossenes Eingabegerät
1636 entgegennehmen und in ein an die Karte adressiertes Kommando einbetten, wenn ein
1637 Kartenterminal der Sicherheitsklasse 1 verwendet wird. [<=]

1638 **AdV-A_2496 - Klasse 1: PIN-Eingabe Geheimnis**

1639 Die KTR-AdV DARF die eingegebene PIN/PUK Ziffernfolge NICHT auf dem Bildschirm
1640 darstellen, wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet wird. [<=]

1641 **AdV-A_2497 - Klasse 1: PIN-Eingabe Eingabefeedback**

1642 Die KTR-AdV MUSS ein eingegebenes Zeichen einer Geheimniseingabe mit dem Zeichen „
1643 * “ (Wildcard) quittieren, wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet
1644 wird. [<=]

1645 **AdV-A_2498 - Klasse 1: PIN-Eingabe Eingabevalidierung**

1646 Die KTR-AdV MUSS ein eingegebenes, neues PIN-Geheimnis durch eine erneute Abfrage
1647 des neuen PIN-Geheimnisses verifizieren, wenn das Geheimnis durch einen
1648 Anwendungsfall geändert werden soll und wenn ein Kartenterminal der Sicherheitsklasse
1649 1 verwendet wird. [<=]

1650 **6.2.1.2 Kartenterminals der Sicherheitsklasse 2**

1651 Kartenterminals der Sicherheitsklasse 2 verfügen über eine Eingabeschnittstelle zur
1652 Eingabe eines Benutzergeheimnisses. Typischerweise werden Kartenterminals der
1653 Sicherheitsklasse 2 in Anwendungsfällen mit Eingabe einer PIN bzw. PUK so angesteuert,
1654 dass das vorbereitete Kartenkommando mit einem Platzhalter des PIN-Geheimnisses an
1655 das Kartenterminal geschickt wird. Das Kartenterminal nimmt die PIN über die
1656 Eingabeschnittstelle entgegen, ersetzt den Platzhalter durch das eingegebene Geheimnis
1657 und leitet das Kartenkommando anschließend weiter an die Karte.

1658 **AdV-A_2500 - Klasse 2: PIN-Eingabe**

1659 Die KTR-AdV MUSS ein angeschlossenes Kartenterminal der Sicherheitsklasse 2 so
1660 ansteuern, dass ein Kartenkommando, das eine PIN-/PUK-Eingabe erfordert, an einem
1661 Kartenterminal um die Benutzereingabe ergänzt und anschließend direkt an die
1662 adressierte Karte weitergeleitet wird. [<=]

1663 **AdV-A_2501 - Klasse 2: PIN-Eingabe Fehlkonfiguration**

1664 Die KTR-AdV MUSS alle Operationen mit einer eindeutigen Fehlermeldung abbrechen, in
1665 denen sie die Kenntnis eines PIN/PUK-Geheimnisses erlangt, das an einem PIN-Pad eines
1666 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 Realisierungsumgebung 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

1714 Benutzer. Diese kann je nach Konfiguration an einem Gerät als Kartenterminal der
1715 Sicherheitsklasse 3 oder auch eine Kombination aus Bildschirmausgabe, Kartenterminal-
1716 PIN-Pad und/oder Tastatureingabe erfolgen.

1717 **AdV-A_2506 - Übergabeschnittstelle PIN/PUK-Geheimnis**

1718 Die KTR-AdV MUSS eine Operation ENV_TUC_SECRET_INPUT zur Eingabe eines PIN/PUK-
1719 Geheimnisses und Weiterleitung an eine SmartCard mit den Parametern

- 1720 • Eingabeparameter:
 - 1721 • Identifikator
 - 1722 • Aktion
 - 1723 • minLength
 - 1724 • maxLength
 - 1725 • commandApduPart
- 1726 • Rückgabewerte
 - 1727 • responseApdu

1728 implementieren. [\leq]

1729 **AdV-A_2507 - Umsetzung ENV_TUC_SECRET_INPUT**

1730 Die KTR-AdV MUSS die Abbildung der Eingabeparameter auf die Rückgabewerte der
1731 Operation ENV_TUC_SECRET_INPUT derart umsetzen, dass

- 1732 • die Eingabeparameter `Identifikator` und `Aktion` für einen Hinweistext an den
1733 Benutzer verwendet werden, welche Aktion auf welchem konkreten Kartenobjekt
1734 (z.B. Name einer PIN) durchgeführt wird
- 1735 • wenn der Eingabeparameter `Aktion` die Eingabe eines Benutzerhinweises
1736 erfordert, der `commandApduPart` an der Eingabeschnittstelle um das
1737 Benutzergeheimnis ergänzt wird
- 1738 • der `commandApduPart` über die Transportschnittstelle für Kartenkommandos an die
1739 Karte gesendet wird

1740 und die Antwortnachricht der Karte als `responseApdu` an den Aufrufer zur Auswertung
1741 zurückgegeben wird. [\leq]

1742 **AdV-A_2555 - Minimalprinzip Karteninteraktion**

1743 Die KTR-AdV DARF ein Kartenkommando NICHT an eine angebundene Karte weiterleiten,
1744 dass nicht explizit im Kontext eines Anwendungsfalls (intendierte Kartenoperationen und
1745 Erhöhen des Sicherheitszustands der Karte falls erforderlich) erforderlich ist. [\leq]

1746 **6.2.3 Schnittstelle zur Freischaltung der eGK**

1747 Um dem Versicherten zur Verwaltung seiner eGK die notwendigen Zugriffsrechte
1748 einzuräumen, muss die eGK über ein Card-2-Card-Verfahren freigeschaltet werden. Die
1749 Systemprozesse der TI-Plattform benötigen dafür eine vertrauliche, integrale und
1750 authentische Schnittstelle zum Austausch von eGK-Challenge und einer Signatur dieser
1751 Challenge durch die SM-B-Identität der Kostenträger, die die Echtheit des Zertifikats und
1752 den Besitz des privaten Schlüssels zu diesem Zertifikat bestätigt.

1753 In der Realisierungsumgebung der KTR-AdV muss dazu ein gesicherter Kanal zwischen
1754 der AdV-App beim Versicherten und dem AdV-Server in einem Rechenzentrum hergestellt
1755 werden. Anforderungen an diese gesicherte Verbindung werden im Kapitel "5.1.2-
1756 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 PL_TUC_CARD_INFORMATION gespeicherten CV-Zertifikats gemäß [gemSpec_CardProxy#Konfigurationstabelle CardProxy SMC-B] und dem gewählten kryptografischen Verfahren R2048 bzw. E256.
SIGNATURVERFAHREN	elcRoleAuthentication, oder rsaRoleAuthentication gemäß dem gewählten kryptografischen Verfahren des in PL_TUC_CARD_INFORMATION gespeicherten CV-Zertifikats.
HASHWERT	Weiterleiten des <i>tokens</i> , das an der Schnittstelle ENV_TUC_CARD_TO_CARD 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 Consumer Adapter der Komponente AdV-Server kapseln.[<=]

AdV-A_2510 - Proxy-Funktion des Consumer Adapters 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.

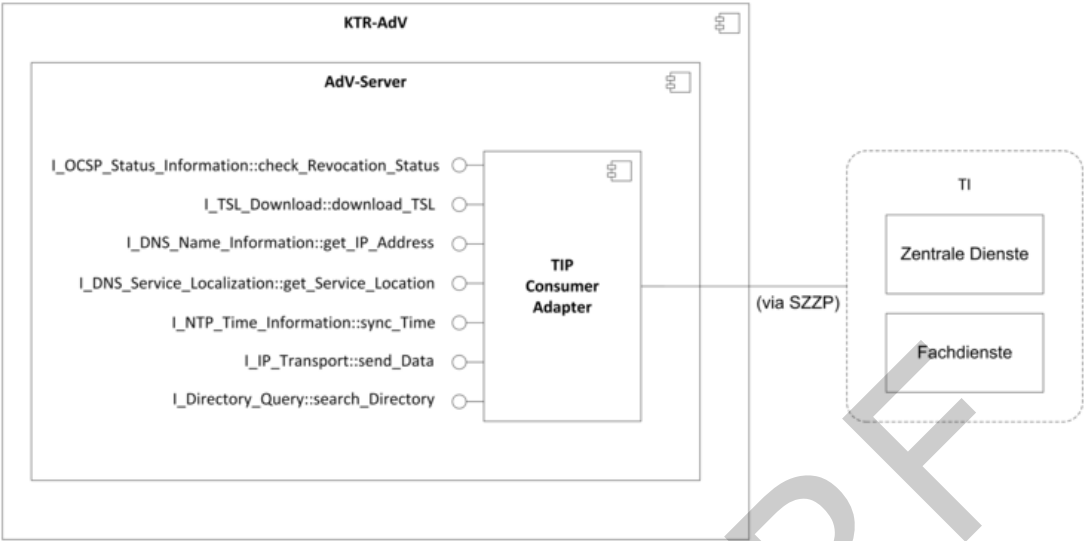


Abbildung 23: ABB_ADV_302 - Schnittstellen des TIP Consumer Adapters

Tabelle 59: TAB_AdV_301 - Schnittstellen des Consumer Adapters

Bereitgestellte Schnittstellen	
Schnittstelle	Anbieter [Spezifikation]
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 [gemSpec_Systemprozesse_dezTI]) selbst um. Lediglich der Sperrstatus wird mittels I_OCSP_Status_Information an der zentralen TI-Plattform abgefragt.
Benötigte Schnittstellen	
Schnittstelle	Anbieter [Spezifikation]
(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.

1791 6.3 Schnittstelle zwischen AdV-App und AdV-Server

1792 Die Schnittstelle zwischen der AdV-App und dem AdV-Server liegt innerhalb des
 1793 Produkttyps KTR-AdV. Es handelt sich daher um eine Innenschnittstelle. An diese werden
 1794 keine inhaltlichen Anforderungen gestellt. Es werden jedoch Sicherheitsanforderungen im
 1795 Kapitel 5.1.2 hierzu erhoben.

1796 6.4 Identitäten der KTR-AdV

1797 *In der Beschreibung der Leistungen der dezentralen TI-Plattform in*
 1798 *[gemSpec_Systemprozesse_dezTI] sowie in der Plattformkomponente CardProxy erfolgt die*
 1799 *Schnittstellendefinition für den Zugriff auf die SM-B-Identitäten und deren kryptografisches*
 1800 *Schlüsselmateriale auf Basis einer SMC-B mit entsprechendem Objektsystem.*

1801 *Mit der Verwendung eines HSM und einer herstellerepezifischen Schnittstelle für den HSM-Zugriff*
 1802 *können sich sowohl die Schnittstellenoperationen als auch die Bezeichner der entsprechenden SM-*
 1803 *B-Identitäten von denen in der Spezifikation der KTR-AdV unterscheiden. Diese Abweichung ist*
 1804 *ausdrücklich zulässig, soweit die Realisierung protokollarische Vorgaben und das geforderte*
 1805 *Sicherheitsniveau einhält.*

1806 Die KTR-AdV benötigt zwei Rollen mit entsprechenden Identitäten zur Abbildung der oben
 1807 genannten Anwendungsfälle. Als Kostenträgerorganisation soll sie dem Versicherten

1808 Zugriffsrechte auf seiner eGK zur Durchführung der AdV-Anwendungsfälle freischalten.
1809 Die Angaben zu dieser Kostenträgerorganisation werden auch zur Vervollständigung des
1810 obligatorischen eGK-Protokolleintrags verwendet.

1811 Des Weiteren muss sich die KTR-AdV mit fachanwendungsspezifischen Fachdiensten
1812 verbinden können. Hierzu muss sie als Rechenzentrums-Consumer in einer passenden
1813 Rolle authentisiert werden.

1814 Diese zwei Aspekte müssen in der KTR-AdV über Zertifikate abgebildet werden, deren
1815 zugehöriges kryptografisches, privates Schlüsselmaterial in der Realisierung der KTR-AdV
1816 integritätsgeschützt und vertraulich gespeichert werden muss.

1817 **AdV-A_2513 - Privates Schlüsselmaterial in HSM speichern**

1818 Die KTR-AdV MUSS privates Schlüsselmaterial zu Zertifikaten der Rollenauthentisierung
1819 gegenüber einer eGK und des Verbindungsaufbaus zu Diensten der TI in einem HSM
1820 integritätsgeschützt und vertraulich speichern, dessen Eignung durch eine erfolgreiche
1821 Evaluierung nachgewiesen wurde. Als Evaluierungsschema kommen dabei Common
1822 Criteria oder Federal Information Processing Standard (FIPS) in Frage. Die Prüftiefe
1823 MUSS mindestens (a) FIPS 140-2 Level 3, oder (b) Common Criteria EAL 4
1824 entsprechen. [≤]

1825 Die Anbindung an den AdV-Server in einem Rechenzentrum kann über eine
1826 herstellerspezifische Schnittstelle mit einem handelsüblichen HSM erfolgen, die die oben
1827 genannten Sicherheitsziele erfüllt. Eine Anbindung eines HSM-Bs via SICCT ist nicht
1828 zwingend erforderlich.

1829 Zum Zeitpunkt der Fertigstellung dieser Spezifikation erfüllt eine zugelassene SMC-B die
1830 oben genannte Anforderung und kann als HSM eingesetzt werden.

1831 Falls keine SMC-B als HSM zum Einsatz kommt, müssen die Zertifikate auf sichere Weise
1832 in das HSM eingebracht werden. An dieser Stelle werden keine konkreten Technologien
1833 oder Prozessschritte vorgegeben, damit der Betreiber der KTR-AdV mit einem TSP ein
1834 geeignetes Verfahren etablieren kann.

1835 **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.

1836

1837 **AdV-A_2575 - Personalisierung des HSMs**

1838 Falls der Betreiber der KTR-AdV keine SMC-B als HSM einsetzt, MUSS er einen sicheren
1839 Prozess zur Personalisierung des HSMs definieren und etablieren, der die in
1840 TAB_ADV_385 genannten Aspekte beinhaltet. [≤]

1841 Falls für diesen Prozess nur eine geringe Anzahl an Instanzen erwartet wird, kann es
 1842 sinnvoll sein, Teile dieses Prozesses rein organisatorisch umzusetzen. Anstelle einer
 1843 technischen Schnittstelle kann dann ein papierbasiertes Verfahren eingesetzt werden.

1844 **A_15118 - CV-Zertifikat für PIN Status Prüfung**

1845 Die KTR-AdV MUSS über ein CV-Zertifikat C.KTRADV.AUTR_CVC.E256 verfügen, mit dem
 1846 in einem Authentisierungsverfahren ein Trusted Channel aufgebaut wird, jedoch keine
 1847 Zugriffsrechte für KTR-AdV- Anwendungsfälle auf einer eGK freigeschaltet werden. [<=]

1848 **AdV-A_2514 - CV-Zertifikat für eGK-Freischaltung**

1849 Die KTR-AdV MUSS über ein CV-Zertifikat C.SMC.AUTR_CVC.E256 verfügen, mit dem auf
 1850 einer eGK Zugriffsrechte für KTR-AdV-Anwendungsfälle in einem
 1851 Authentisierungsverfahren freigeschaltet werden. [<=]

1852 Abhängig von der Realisierung eines sicheren Zertifikatsspeichers in der KTR-AdV kann
 1853 das Authentisierungsverfahren zur Freischaltung der eGK über ein Card-2-Card- oder
 1854 auch Card-2-Server-Verfahren erfolgen.

1855 **AdV-A_2515 - X.509-Zertifikat für TLS-gesicherte Verbindung**

1856 Die KTR-AdV MUSS über ein X.509-Zertifikat zum Zweck des TLS-Verbindungsaufbaus
 1857 mit der Rolle `professionOID = OID <oid_adv_ktr>` gemäß [gemSpec_OID] verfügen,
 1858 um sich gegenüber einem Fachdienst zu authentisieren, welches als C.HCI.AUT
 1859 identifiziert wird. [<=]

1860 **AdV-A_2516 - X.509-Zertifikat für eGK-Protokolleintrag**

1861 Die KTR-AdV MUSS über ein X.509-Zertifikat mit einem CommonName entsprechend den
 1862 Vorgaben des verantwortlichen Zertifikat-Herausgebers verfügen, um einen für den
 1863 Versicherten lesbaren, nachvollziehbaren Protokolleintrag auf der eGK über die Nutzung
 1864 der KTR-AdV erzeugen zu können. [<=]

1865 **AdV-A_2556 - nachvollziehbarer eGK-Protokolleintrag mit Bezug zum Anbieter**

1866 Der Anbieter der KTR-AdV MUSS sicherstellen, dass auf der eGK des Versicherten ein
 1867 lesbarer, nachvollziehbarer Protokolleintrag mit Bezug zum Anbieter der KTR-AdV erzeugt
 1868 werden kann. [<=]

1869 Der Anbieter ist in diesem Zusammenhang eine Krankenkasse, in deren Auftrag ein
 1870 Betreiber die KTR-AdV eines spezifischen Herstellers den Versicherten zur Verfügung
 1871 stellt. Da aus diesem Zertifikat lediglich der CommonName verwendet und kein privates
 1872 Schlüsselmateriale zur Authentisierung verwendet wird, kann auf die Nutzung dieses
 1873 Zertifikats verzichtet werden. Es muss jedoch sichergestellt werden, dass auf der eGK
 1874 des Versicherten ein lesbarer, nachvollziehbarer Protokolleintrag mit Bezug zum Anbieter
 1875 der KTR-AdV erzeugt wird.

1876

7 Informationsmodell

1877

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

1878

ENTWURF

1879

8 Verteilungssicht

1880

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

1881

ENTWURF

1882

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
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	nicht anwendbar, unzutreffend
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	10
Abbildung 2: ABB_ADV_304 – Zusammenhang Systemprozesse und Fachanwendung ..	12
Abbildung 3: ABB_ADV_301 – Kontextdiagramm	16
Abbildung 4: ABB_ADV_303 – Verteilungsdiagramm	16
Abbildung 5: ABB_ADV_329 – Komponentendiagramm der KTR-Adv	18
Abbildung 6 : ABB_ADV_333 Verbindungs Aufbau und Freischaltung eGK	25
Abbildung 7: ABB_ADV_305 – Ablauf „Anwendung auf eGK deaktivieren“	44
Abbildung 8: ABB_ADV_383 – Ablauf „Anwendung auf eGK reaktivieren“	48
Abbildung 9 : ABB_ADV_312 – Ablauf des Adv UC_01: „PIN der eGK ändern“	52
Abbildung 10 : ABB_ADV_316 – Ablauf des Adv UC_02: „PIN auf eGK entsperren“	55
Abbildung 11: ABB_ADV_308 – Ablauf Adv UC_03 „PIN für Fachanwendung einschalten“	58
Abbildung 12: ABB_ADV_310 – Ablauf Adv UC_04 „PIN für Fachanwendung ausschalten“	61
Abbildung 13: ABB_ADV_317 – Ablauf des „VSD von eGK lesen“	64
Abbildung 14: ABB_ADV_314 – Ablauf des Adv UC_21: „Zugriffsprotokoll anzeigen“ ...	68
Abbildung 15: ABB_ADV_315 Standardablauf – Datenübertragung bei Kartentausch durchführen	75
Abbildung 16: ABB_ADV_359 – Ablauf des Adv UC_121: „DPE von eGK anzeigen“	84
Abbildung 17: ABB_ADV_361 – Ablauf des Adv UC_122: „DPE auf eGK ändern“	87
Abbildung 18: ABB_ADV_363 – Ablauf des Adv UC_123: „DPE auf eGK löschen“	91
Abbildung 19: ABB_ADV_322 – Ablauf des Adv UC_25: „Mit eGK verschlüsseln“	101

1913	Abbildung 20: ABB_ADV_324 – Ablauf des Adv-UC_26: „Mit eGK entschlüsseln“	104
1914	Abbildung 21: ABB_ADV_379 – Ablauf des Adv-UC_27 „Authentisierungsrequest mit eGK	
1915	signieren“	106
1916	Abbildung 22: ABB_ADV_381 – Ablauf Adv-UC_24: Zertifikat von eGK lesen	109
1917	Abbildung 23: ABB_ADV_302 – Schnittstellen des TIP Consumer Adapters.....	117
1918	Abbildung 1: ABB_ADV_300 – Überblick Adv in einer Umgebung im Auftrag der	
1919	Kostenträger	10
1920	Abbildung 2: ABB_ADV_304 – Zusammenhang Systemprozesse und Fachanwendung ..	12
1921	Abbildung 3: ABB_ADV_301 – Kontextdiagramm	16
1922	Abbildung 4: ABB_ADV_303 – Verteilungsdiagramm	16
1923	Abbildung 5: ABB_ADV_329 – Komponentendiagramm der KTR-Adv	18
1924	Abbildung 6 : ABB_ADV_333 Verbindungsaufbau und Freischaltung eGK.....	25
1925	Abbildung 7: ABB_ADV_305 – Ablauf „Anwendung auf eGK deaktivieren“	44
1926	Abbildung 8: ABB_ADV_383 – Ablauf „Anwendung auf eGK reaktivieren“	48
1927	Abbildung 9 : ABB_ADV_312 – Ablauf des Adv-UC_01: „PIN der eGK ändern“.....	52
1928	Abbildung 10 : ABB_ADV_316 – Ablauf des Adv-UC_02: „PIN auf eGK entsperren“	55
1929	Abbildung 11: ABB_ADV_308 – Ablauf Adv-UC_03 „PIN für Fachanwendung einschalten“	
1930	58
1931	Abbildung 12: ABB_ADV_310 – Ablauf Adv-UC_04 „PIN für Fachanwendung ausschalten“	
1932	61
1933	Abbildung 13: ABB_ADV_317 - Ablauf des „VSD von eGK lesen“	64
1934	Abbildung 14: ABB_ADV_314 – Ablauf des Adv-UC_21: „Zugriffsprotokoll anzeigen“ ...	68
1935	Abbildung 15: ABB_ADV_315 Standardablauf – Datenübertragung bei Kartentausch	
1936	durchführen	75
1937	Abbildung 16: ABB_ADV_359 – Ablauf des Adv-UC_121: „DPE von eGK anzeigen“	84
1938	Abbildung 17: ABB_ADV_361 – Ablauf des Adv-UC_122: „DPE auf eGK ändern“.....	87
1939	Abbildung 18: ABB_ADV_363 – Ablauf des Adv-UC_123: „DPE auf eGK löschen“	91
1940	Abbildung 19: ABB_ADV_322 – Ablauf des Adv-UC_25: "Mit eGK verschlüsseln"	101
1941	Abbildung 20: ABB_ADV_324 – Ablauf des Adv-UC_26: „Mit eGK entschlüsseln“	104
1942	Abbildung 21: ABB_ADV_379 – Ablauf des Adv-UC_27 „Authentisierungsrequest mit eGK	
1943	signieren“	106
1944	Abbildung 22: ABB_ADV_381 – Ablauf Adv-UC_24: Zertifikat von eGK lesen	109
1945	Abbildung 23: ABB_ADV_302 - Schnittstellen des TIP Consumer Adapters.....	117
1946		
1947		

1948 9.4 Tabellenverzeichnis

1949	Tabelle 1: TAB_ADV_300 – Akteure und ihre Rollen	13
------	--	----

1950	Tabelle 2: TAB_ADV_329 – Komponenten, Verantwortung und Funktionalitäten	19
1951	Tabelle 3: TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine	30
1952	Tabelle 4: TAB_ADV_303 – Starten einer Adv-Sitzung	32
1953	Tabelle 5: TAB_ADV_304 – Ablaufaktivitäten – Starten einer Adv-Sitzung	33
1954	Tabelle 6: TAB_ADV_320 – Übergreifende Vorbedingungen	40
1955	Tabelle 7: TAB_ADV_384 – Zulässige Anwendungsfälle nach Status von Karte,	
1956	Anwendung und PIN	40
1957	Tabelle 8: TAB_ADV_461 – Benennung der Anwendungen und Hinweise am Terminal ..	42
1958	Tabelle 9: TAB_ADV_305 – Adv_UC_14 „Anwendung auf eGK deaktivieren“	44
1959	Tabelle 10: TAB_ADV_306 – Ablaufaktivitäten – Adv_UC_14	45
1960	Tabelle 11: TAB_ADV_383 – Adv_UC_15 „Anwendung auf eGK reaktivieren“	48
1961	Tabelle 12: TAB_ADV_307 – Ablaufaktivitäten – Adv_UC_15	49
1962	Tabelle 13: TAB_ADV_312 – PIN der eGK ändern	52
1963	Tabelle 14: TAB_ADV_313 – Ablaufaktivitäten – PIN der eGK ändern	53
1964	Tabelle 15: TAB_ADV_316 – PIN der eGK entsperren	55
1965	Tabelle 16: TAB_ADV_317 – Ablaufaktivitäten – PIN der eGK entsperren	56
1966	Tabelle 17: TAB_ADV_308 – Adv_UC_03 „PIN für Fachanwendung einschalten“	58
1967	Tabelle 18: TAB_ADV_309 – Ablaufaktivitäten – Adv_UC_03	59
1968	Tabelle 19: TAB_ADV_310 – Adv_UC_04 „PIN für Fachanwendung ausschalten“	61
1969	Tabelle 20: TAB_ADV_311 – Ablaufaktivitäten – Adv_UC_04	62
1970	Tabelle 21: TAB_ADV_314 – VSD von eGK anzeigen	64
1971	Tabelle 22: TAB_ADV_315 – Ablaufaktivitäten – VSD von eGK anzeigen	65
1972	Tabelle 23: TAB_ADV_350 – Zugriffsprotokoll anzeigen	68
1973	Tabelle 24: TAB_ADV_351 – Ablaufaktivitäten – Zugriffsprotokoll anzeigen	69
1974	Tabelle 25: TAB_ADV_352 – Versicherten PIN der eGK ändern	71
1975	Tabelle 26: TAB_ADV_353 – Versicherten PIN entsperren	71
1976	Tabelle 27: TAB_ADV_354 – Ablaufaktivitäten – Versicherten PIN entsperren	72
1977	Tabelle 28: TAB_ADV_324 – Datenübertragung bei Kartentausch durchführen	75
1978	Tabelle 29: TAB_ADV_325 – Ablaufaktivitäten – Datenübertragung bei Kartentausch	
1979	durchführen	77
1980	Tabelle 30: TAB_ADV_355 – NFD auf eGK verbergen	81
1981	Tabelle 31: TAB_ADV_356 – Verborgene NFD auf eGK sichtbar machen	81
1982	Tabelle 32: TAB_ADV_357 – PIN für NFD einschalten	82
1983	Tabelle 33: TAB_ADV_358 – PIN für NFD ausschalten	83
1984	Tabelle 34: TAB_ADV_359 – DPE von eGK anzeigen	84
1985	Tabelle 35: TAB_ADV_360 – Ablaufaktivitäten – DPE von eGK anzeigen	85
1986	Tabelle 36: TAB_ADV_361 – DPE auf eGK ändern	87

1987	Tabelle 37: TAB_ADV_362 – Ablaufaktivitäten – DPE auf eGK ändern	88
1988	Tabelle 38: TAB_ADV_363 – DPE auf eGK löschen	91
1989	Tabelle 39: TAB_ADV_364 – Ablaufaktivitäten – DPE auf eGK löschen.....	92
1990	Tabelle 40: TAB_ADV_365 – PIN für DPE einschalten.....	93
1991	Tabelle 41: TAB_ADV_366 – PIN für DPE ausschalten.....	94
1992	Tabelle 42: TAB_ADV_367 – DPE auf eGK verbergen.....	94
1993	Tabelle 43: TAB_ADV_368 – Verborgenen DPE auf eGK sichtbar machen.....	95
1994	Tabelle 44: TAB_ADV_369 – AMTS-Vertreter PIN ändern.....	96
1995	Tabelle 45: TAB_ADV_370 – AMTS-Vertreter PIN entsperren.....	97
1996	Tabelle 46: TAB_ADV_371 – eMP/AMTS-Datensatz auf eGK verbergen.....	97
1997	Tabelle 47: TAB_ADV_372 – Verborgene eMP/AMTS-Datensatz auf eGK sichtbar machen	
1998	98
1999	Tabelle 48: TAB_ADV_373 – PIN für AMTS einschalten	99
2000	Tabelle 49: TAB_ADV_374 – PIN für AMTS ausschalten.....	100
2001	Tabelle 50: TAB_ADV_375 – Adv UC_25: „Mit eGK verschlüsseln“.....	101
2002	Tabelle 51: TAB_ADV_376 – Ablaufaktivitäten – Mit eGK verschlüsseln	102
2003	Tabelle 52: TAB_ADV_377 – Adv UC_26: „Mit eGK entschlüsseln“	104
2004	Tabelle 53: TAB_ADV_378 – Ablaufaktivitäten – Mit eGK entschlüsseln	105
2005	Tabelle 54: TAB_ADV_379 – Authentisierungsrequest mit eGK signieren	107
2006	Tabelle 55: TAB_ADV_380 – Ablaufaktivitäten – Authentisierungsrequest mit eGK	
2007	signieren.....	107
2008	Tabelle 56: TAB_ADV_381 – Adv UC_24: Zertifikat von eGK lesen	109
2009	Tabelle 57: TAB_ADV_382 – Ablaufaktivitäten – Adv UC_24: Zertifikat von eGK lesen	110
2010	Tabelle 58: TAB_Adv_302 – Verwendete Plattformleistungen	111
2011	Tabelle 59: TAB_Adv_301 – Schnittstellen des Consumer Adapters.....	117
2012	Tabelle 60: TAB_ADV_473 – Hinweistexte für den Versicherten	132
2013	Tabelle 1: TAB_ADV_300 – Akteure und ihre Rollen	13
2014	Tabelle 2: TAB_ADV_329 – Komponenten, Verantwortung und Funktionalitäten	19
2015	Tabelle 3: TAB_ADV_318 – Behandlung von Fehlercodes der Plattformbausteine	30
2016	Tabelle 4: TAB_ADV_303 – Starten einer Adv-Sitzung	32
2017	Tabelle 5: TAB_ADV_304 – Ablaufaktivitäten - Starten einer Adv-Sitzung	33
2018	Tabelle 6: TAB_ADV_320 – Übergreifende Vorbedingungen	40
2019	Tabelle 7: TAB_ADV_384 – Zulässige Anwendungsfälle nach Status von Karte,	
2020	Anwendung und PIN	40
2021	Tabelle 8: TAB_ADV_461 – Benennung der Anwendungen und Hinweise am Terminal ..	42
2022	Tabelle 9: TAB_ADV_305 – Adv-UC_14 „Anwendung auf eGK deaktivieren“	44
2023	Tabelle 10: TAB_ADV_306 – Ablaufaktivitäten – Adv-UC_14	45

2024	Tabelle 11: TAB_ADV_383 – Adv-UC_15 „Anwendung auf eGK reaktivieren“	48
2025	Tabelle 12: TAB_ADV_307 – Ablaufaktivitäten – Adv-UC_15	49
2026	Tabelle 13: TAB_ADV_312 – PIN der eGK ändern.....	52
2027	Tabelle 14: TAB_ADV_313 – Ablaufaktivitäten – PIN der eGK ändern.....	53
2028	Tabelle 15: TAB_ADV_316 – PIN der eGK entsperren	55
2029	Tabelle 16: TAB_ADV_317 – Ablaufaktivitäten – PIN der eGK entsperren	56
2030	Tabelle 17: TAB_ADV_308 – Adv-UC_03 „PIN für Fachanwendung einschalten“	58
2031	Tabelle 18: TAB_ADV_309 – Ablaufaktivitäten – Adv-UC_03	59
2032	Tabelle 19: TAB_ADV_310 – Adv-UC_04 „PIN für Fachanwendung ausschalten“	61
2033	Tabelle 20: TAB_ADV_311 – Ablaufaktivitäten – Adv-UC_04	62
2034	Tabelle 21: TAB_ADV_314 – VSD von eGK anzeigen	64
2035	Tabelle 22: TAB_ADV_315 – Ablaufaktivitäten – VSD von eGK anzeigen.....	65
2036	Tabelle 23: TAB_ADV_350 – Zugriffsprotokoll anzeigen	68
2037	Tabelle 24: TAB_ADV_351 – Ablaufaktivitäten – Zugriffsprotokoll anzeigen	69
2038	Tabelle 25: TAB_ADV_352 – Versicherten-PIN der eGK ändern	71
2039	Tabelle 26: TAB_ADV_353 – Versicherten-PIN entsperren	71
2040	Tabelle 27: TAB_ADV_354 – Ablaufaktivitäten – Versicherten-PIN entsperren	72
2041	Tabelle 28: TAB_ADV_324 – Datenübertragung bei Kartentausch durchführen	75
2042	Tabelle 29: TAB_ADV_325 – Ablaufaktivitäten – Datenübertragung bei Kartentausch	
2043	durchführen	77
2044	Tabelle 30: TAB_ADV_355 – NFD auf eGK verbergen.....	81
2045	Tabelle 31: TAB_ADV_356 – Verborgene NFD auf eGK sichtbar machen	81
2046	Tabelle 32: TAB_ADV_357 – PIN für NFD einschalten	82
2047	Tabelle 33: TAB_ADV_358 – PIN für NFD ausschalten.....	83
2048	Tabelle 34: TAB_ADV_359 – DPE von eGK anzeigen	84
2049	Tabelle 35: TAB_ADV_360 – Ablaufaktivitäten – DPE von eGK anzeigen	85
2050	Tabelle 36: TAB_ADV_361 – DPE auf eGK ändern	87
2051	Tabelle 37: TAB_ADV_362 – Ablaufaktivitäten – DPE auf eGK ändern	88
2052	Tabelle 38: TAB_ADV_363 – DPE auf eGK löschen	91
2053	Tabelle 39: TAB_ADV_364 – Ablaufaktivitäten – DPE auf eGK löschen.....	92
2054	Tabelle 40: TAB_ADV_365 – PIN für DPE einschalten.....	93
2055	Tabelle 41: TAB_ADV_366 – PIN für DPE ausschalten	94
2056	Tabelle 42: TAB_ADV_367 – DPE auf eGK verbergen	94
2057	Tabelle 43: TAB_ADV_368 – Verborgenen DPE auf eGK sichtbar machen.....	95
2058	Tabelle 44: TAB_ADV_369 – AMTS-Vertreter-PIN ändern	96
2059	Tabelle 45: TAB_ADV_370 – AMTS-Vertreter-PIN entsperren.....	97
2060	Tabelle 46: TAB_ADV_371 – eMP/AMTS-Datensatz auf eGK verbergen.....	97

Tabelle 47: TAB_ADV_372 – Verborgene eMP/AMTS-Datensatz auf eGK sichtbar machen	98
Tabelle 48: TAB_ADV_373 – PIN für AMTS einschalten	99
Tabelle 49: TAB_ADV_374 – PIN für AMTS ausschalten.....	100
Tabelle 50: TAB_ADV_375 – Adv-UC_25: „Mit eGK verschlüsseln“.....	101
Tabelle 51: TAB_ADV_376 – Ablaufaktivitäten – Mit eGK verschlüsseln	102
Tabelle 52: TAB_ADV_377 – Adv-UC_26: „Mit eGK entschlüsseln“	104
Tabelle 53: TAB_ADV_378 – Ablaufaktivitäten – Mit eGK entschlüsseln	105
Tabelle 54: TAB_ADV_379 – Authentisierungsrequest mit eGK signieren.....	107
Tabelle 55: TAB_ADV_380 – Ablaufaktivitäten – Authentisierungsrequest mit eGK signieren.....	107
Tabelle 56: TAB_ADV_381 – Adv-UC_24: Zertifikat von eGK lesen	109
Tabelle 57: TAB_ADV_382 – Ablaufaktivitäten – Adv-UC_24: Zertifikat von eGK lesen	110
Tabelle 58: TAB_AdV_302 - Verwendete Plattformleistungen.....	111
Tabelle 59: TAB_AdV_301 - Schnittstellen des Consumer Adapters.....	117
Tabelle 60: TAB_ADV_473 – Hinweistexte für den Versicherten	132

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: Glossar der Telematikinfrastruktur
[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
[gemSpec_Systemprozesse_dezTI]	gematik: Spezifikation Systemprozesse der dezentralen TI
[gemSysL_VSDM]	gematik: Systemspezifisches Konzept Versichertenstammdatenmanagement (VSDM)

2089

9.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[TR-03158]	Technische Richtlinie BSI TR-03158 Anwendungen des Versicherten - AdV-App

2090 **9.6 Hinweistexte der Fachanwendungen**2091 **Tabelle 60: TAB_ADV_473 – Hinweistexte für den Versicherten**

ID	Bezeichnung Anwendungsfall	Hinweistext für Versicherten
Verwaltung der eGK durch den Versicherten		
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.
Verwaltung der NFD		

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.
Verwaltung des DPE		
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.
Verwaltung eMP / AMTS		
AdV022	Vertreter-PIN ändern	Sie können eine Vertreter-PIN für den Medikationsplan / die arzneimitteltherapiesicherheitsrelevanten 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.
Fachanwendungsunabhängige Anwendungsfälle		
Adv030	Mit eGK verschlüsseln	Sie können mit Ihrer Gesundheitskarte Daten verschlüsseln.
Adv031	Mit eGK entschlüsseln	Sie können mit Ihrer Gesundheitskarte verschlüsselte Daten wieder entschlüsseln.

2092
2093