gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Elektronische Gesundheitskarte und Telematikinfrastruktur

Systemspezifisches Konzept Anwendungen des Versicherten (AdV)

Version:	1.3.0
Revision:	72494
Stand:	18.12.2018
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSysL_AdV

Dokumentinformationen

Änderungen zur Vorversion

Einarbeitung aus P17.1.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.1.0	05.10.17		Erstellung	gematik
			Ausbau LE-AdV	
1.2.0	18.12.17		freigegeben	gematik
			Einarbeitung gemäß P17.1	gematik
1.3.0	18.12.18		freigegeben	gematik

Inhaltsverzeichnis

1 Einführung

1.1 Zielsetzung

Das vorliegende Dokument „Systemspezifisches Konzept Anwendungen des Versicherten (AdV)“ beschreibt die Fachanwendung AdV auf Systemebene im Kontext des Online-Rollout (Stufe 2.1) und bildet den Rahmen für die weiterführenden Konzepte und Spezifikationen des Projektes AdV.

Darüber hinaus erfolgt eine Zerlegung der Fachanwendung AdV in die zugehörigen Produkttypen. Die Schnittstellen zwischen den einzelnen Produkttypen werden spezifiziert.

Die Abbildung 1 zeigt schematisch die Dokumentenhierarchie im Projekt AdV, in welcher das systemspezifische Konzept AdV und die Konzepte sowie die Spezifikationen eingeordnet sind. Die Abbildung stellt nicht die vollständige Dokumentenhierarchie des Projekts Online-Rollout (Stufe 2.1) oder den Trace der Anforderungen dar.

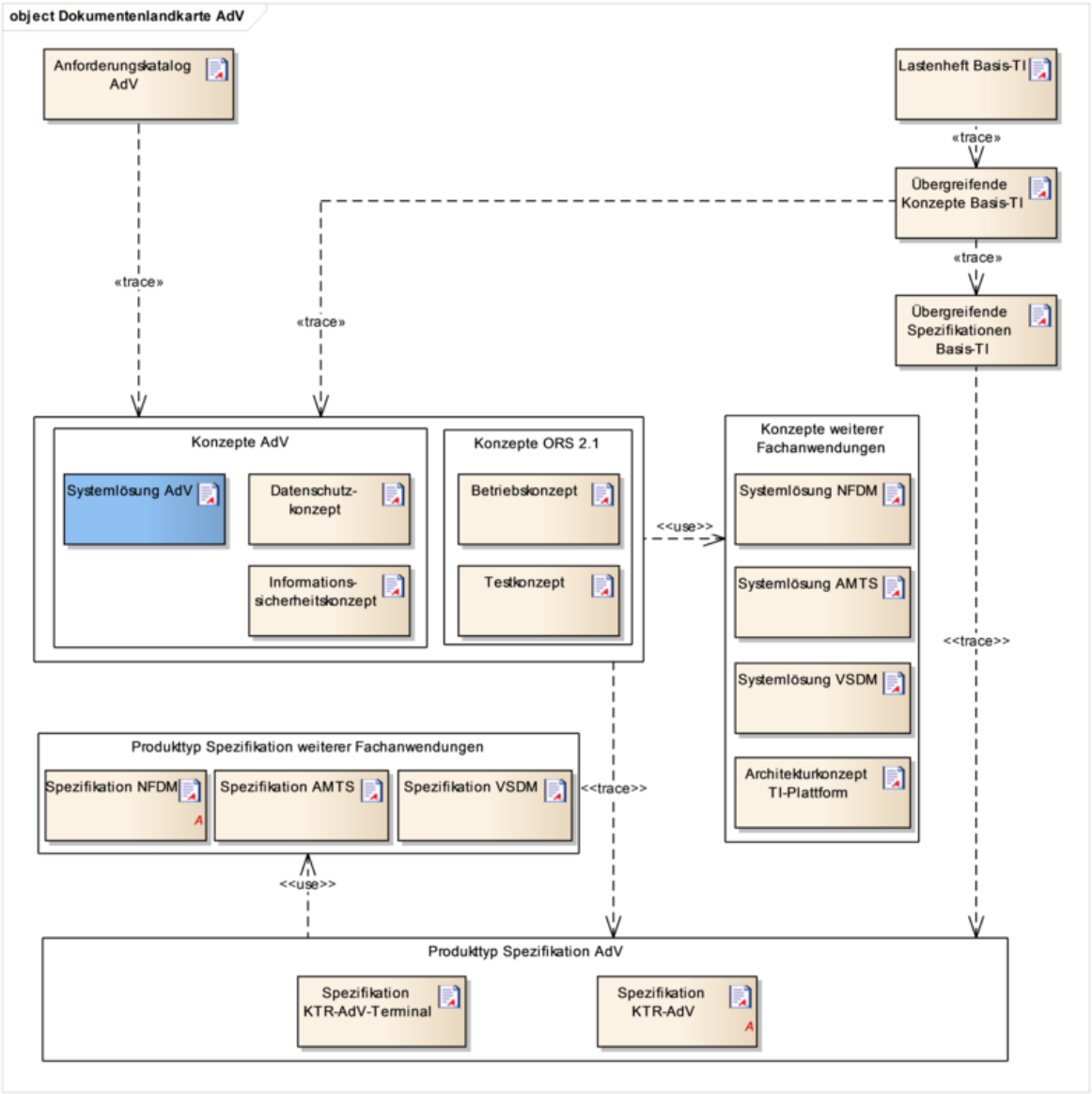

Abbildung 1: Dokumentenlandkarte AdV

Kapitel 2 gibt einen Überblick über die Fachanwendung AdV. Es wird eine Übersicht über die notwendigen Produkttypen und deren Schnittstellen gegeben. Darüber hinaus wird ein Überblick über das Informationsmodell und das Berechtigungsmodell der Anwendungen der Versicherten gegeben.

In Kapitel 3 erfolgt eine detaillierte Beschreibung der Anwendungsfälle, die zur Erfüllung der fachlich-funktionalen Anforderungen identifiziert wurden. Das Konzept AdV definiert ein Set von Bausteinen bzw. Activities (AdV-ACT_*), die in der weiteren Beschreibung zu Basis-Anwendungsfällen (AdV-UC_*) zusammengesetzt werden. Die anschließende Beschreibung der fachlichen Anwendungsfälle setzt auf diese Basis-Anwendungsfälle auf und gibt eine Konfiguration vor, mit welchen Parametern die Basisanwendungsfälle ausgeführt werden sollen.

Die zur Ausführung der fachlichen Anwendungsfälle benötigten Operationen werden in Kapitel 4 dargestellt, sowie deren Eingangs- und Ausgangsparameter definiert.

Kapitel 5 beinhaltet die Systemzerlegung der Fachanwendung AdV in die zugehörigen Produkttypen. Die Fachanwendung AdV gliedert sich dabei in die Produkttypen AdV-Server und AdV-Terminal.

Das Kapitel 6 enthält das technische Informationsmodell der AdV.

Das Kapitel 7 gibt einen Überblick über die Zukunftsthemen der AdV.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von AdV-Produkten.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung im Zulassungsverfahren 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.

Alle Festlegungen im Zusammenhang mit Anwendungen des Versicherten (AdV) stehen unter dem Vorbehalt, dass der Betrieb einer AdV-Umgebung unter noch festzulegenden Bedingungen erfolgt.

1.4 Abgrenzung des Dokuments

Innerhalb dieses Dokuments wird auf die technische Umsetzung zur Nutzung der Anwendungen des Versicherten eingegangen. Prozesse der Kostenträger und Leistungserbringer (z. B. Kartenherausgabe) sind nicht Bestandteil des systemspezifischen Konzeptes.

Für die Aspekte „Datenschutz“ und „Datensicherheit“ werden jeweils eigene systemspezifische Konzepte für die Fachanwendung AdV erstellt. Für die Sichten „Betrieb“ und „Test“ wird ein programmübergreifendes Konzept für den Online-Produktivbetrieb (Stufe 2.1) ausgearbeitet.

Zukunftsthemen werden mit Ausnahme der in Kapitel 7 genannten Ergänzungen zum Leistungsumfang an dieser Stelle nicht aufgenommen.

1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und der Textmarke [<=] angeführten Inhalte.

1.5.1 Diagramme

Innerhalb von Diagrammen werden Objekte blau markiert, wenn sie im Geltungsbereich der Fachanwendung AdV liegen, und rosa, wenn es sich um Objekte aus dem erweiterten Leistungsumfang handelt.

2 Systemüberblick

2.1 Komponentenmodell AdV

Für die eigenständige Nutzung durch den Versicherten in einer Umgebung im Auftrag der Kostenträger und der privaten Umgebung des Versicherten (@home) stehen User-Interface-Komponenten zur Verfügung, welche über einen Zugang zur Telematikinfrastruktur verfügen.

AdV-A_2001 - Komponenten der Fachanwendung AdV
Die Fachanwendung AdV MUSS die blau markierten Produkttypen gemäß Abbildung 2 „Systemzerlegung AdV“ bereitstellen.

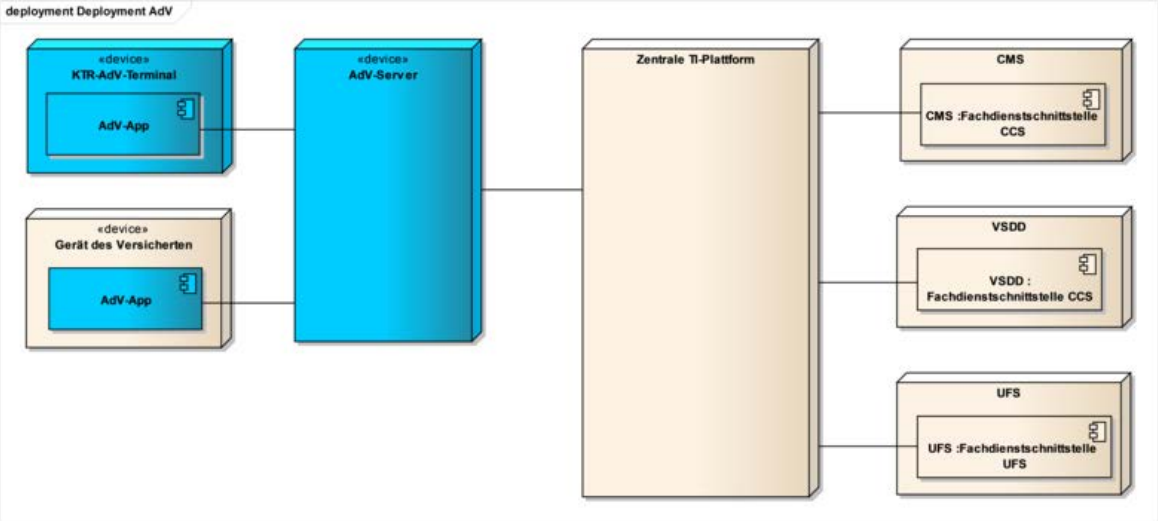

Abbildung 2: Systemzerlegung AdV

[<=]

In der Kostenträgerumgebung, welche die @home-Umgebung einschließt, gliedert sich die Fachanwendung AdV in die Produkttypen KTR-AdV-Terminal und KTR-AdV. Der Produkttyp KTR-AdV wird dabei gebildet aus einem AdV-Server mit zugehöriger AdV-App.

2.2 Schnittstellen

AdV-A_2132 - Schnittstellen der Fachanwendung AdV in der Kostenträger-Umgebung und @home
Die Fachanwendung AdV MUSS die Schnittstellen der Abbildung 3 „AdV-Schnittstellen in der Kostenträger-Umgebung und @home“ zur Anbindung an die TI-Plattform verwenden.**[<=]**

AdV-A_2002 - Gegenseitige Authentisierung zwischen AdV-Server und AdV-App
Der AdV-Server und die AdV-App MÜSSEN sich beim Verbindungsaufbau gegenseitig authentisieren.**[<=]**

AdV-A_2220 - Verschlüsselte Kommunikation zwischen AdV-Server und AdV-App
Der AdV-Server und die AdV-App MÜSSEN über eine gesicherte Schnittstelle, die einen verschlüsselten Kanal herstellt, miteinander kommunizieren.**[<=]**

AdV-A_2003 - Gesicherte HTTPS-Schnittstelle für Clientsysteme
Die AdV-App MUSS in ihrer lokalen Ausführungsumgebung eine gesicherte HTTPS-Verbindung anbieten, über welche der Versicherte mittels Browser in externen Anwendungsfällen die Anwendungsfälle der AdV nutzen kann.
[<=]

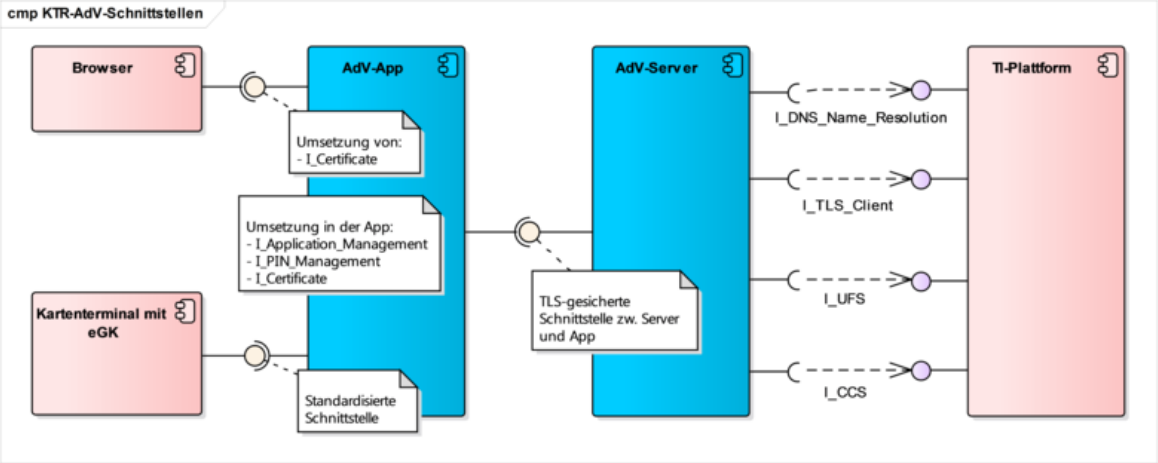

Abbildung 3: AdV-Schnittstellen in der Kostenträger-Umgebung und @home

Die AdV in der Umgebung im Auftrag der Kostenträger und @home nutzt die dargestellten Schnittstellen zur Anbindung an zentrale Dienste der TI-Plattform und Fachdienste. Die Schnittstelle zwischen AdV-Server und zugehöriger App wird nicht näher beschrieben, da AdV-Server und die zugehörige AdV-App im Verbund als Produkttyp KTR-AdV realisiert werden sollen.

Für den Zugriff auf die Karten der TI-Plattform (eGK und SM-B) in der AdV in einer Umgebung im Auftrag der Kostenträger müssen der AdV-Server und die AdV-App Leistungen der TI-Plattform bereitstellen. Die Schnittstellen sollen analog zu den durch die dezentrale TI-Plattform bereitgestellten Schnittstellen realisiert werden. Über diesen Plattformadapter können die Fachmodule der Fachanwendungen AMTS, NFDM und VSDM ihre fachlichen Anwendungsfälle in der KTR-Umgebung abbilden. Die Fachlogik des Fachmodules einer Fachanwendung kann hierbei auf ein clientseitiges und serverseitiges Modul verteilt werden.

Für die Nutzung der AdV in einer Umgebung im Auftrag der Kostenträger soll die AdV-App in ihrer lokalen Ausführungsumgebung (d. h. auf dem Computer des Versicherten oder auf einem KTR-AdV-Terminal) eine Schnittstelle anbieten, über welche der Versicherte die Anwendungsfälle der AdV in der App selbst oder mit einem der gängigen Browser initiiert. Das Auslesen der eGK soll in dieser Umgebung über eine standardisierte API (z. B. eCard-API-Anbindung) und einen Standard-Kartenleser erfolgen.

2.3 Akteure und Berechtigungen

Ein Akteur ist eine gewöhnlich außerhalb des betrachteten bzw. zu realisierenden Systems liegende Einheit, die an der in einem Anwendungsfall beschriebenen Interaktion mit dem System beteiligt ist.

Ein Akteur kann ein Mensch sein, z. B. ein Benutzer, ebenso aber auch ein anderes technisches System. Bei Akteuren werden nicht die konkreten beteiligten Personen unterschieden, sondern ihre Rollen, die sie im Kontext des Anwendungsfalls einnehmen.

Der Versicherte, der von einem Kostenträger eine eGK erhalten hat, ist Akteur in der AdV-Umgebung.

Ärzte, Mitarbeiter medizinischer Institutionen, Apotheker, Mitarbeiter Apotheke sowie Mitarbeiter Institution des Kostenträgers sind in ihrer Rolle keine Akteure in der AdV-Umgebung.

Das Clientsystem bzw. Administratoren können administrative Operationen ausführen. Diese werden nicht als Anwendungsfälle modelliert.

Der Umfang der Anwendungsfälle, welche durch den Versicherten ausgeführt werden können, variiert zwischen den AdV-Umgebungen.

Die Berechtigungsregeln für die Anwendungsfälle werden von der jeweiligen Fachanwendung festgelegt. Auf Grundlage des aktuellen Standes sind dies die Fachanwendungen NFDM, AMTS und VSDM.

AdV-A_2006 - Berechtigungen Anwendungsfälle NFDM
Die Fachanwendung AdV MUSS die Berechtigungen für die Anwendungsfälle NFDM entsprechend den Vorgaben der Fachanwendung NFDM in [gemSysL_NFDM] umsetzen.**[**<=**]**

AdV-A_2007 - Berechtigungen Anwendungsfälle eMP/AMTS
Die Fachanwendung AdV MUSS die Berechtigungen für die Anwendungsfälle eMP/AMTS entsprechend den Vorgaben der Anwendung eMP/AMTS in [gemSysL_AMTS_A] umsetzen.**[**<=**]**

AdV-A_2008 - Berechtigungen Anwendungsfälle VSDM
Die Fachanwendung AdV MUSS die Berechtigungen für die Anwendungsfälle VSDM entsprechend den Vorgaben der Fachanwendung VSDM in [gemSysL_VSDM] umsetzen.**[**<=**]**

AdV-A_2009 - Berechtigungen weitere Anwendungsfälle
Die Fachanwendung AdV MUSS die Berechtigungen für die Anwendungsfälle, welche nicht durch die Fachanwendungen NFDM, eMP/AMTS oder VSDM vorgegeben sind, entsprechend den Vorgaben der Tabelle TAB_ADV_001 umsetzen.

Tabelle 1: TAB_ADV_001 Berechtigungen für die Nutzung der AdV

Funktionen	Akteur Arzt/ Zahnarzt	Akteur Mit-arbeiter medi-zinische Institution	Akteur Apo-theker	Akteur Mit-arbeiter Apotheke	Akteur Psycho-therapeut	Akteur Vertreter des Versicherten	Akteur Versicherter
Anwendungsfälle der AdV ausführen							xA

***Legende**: xA = berechtigt nach Authentisierung durch PIN Eingabe des Versicherten; (leer) = keine Berechtigung*
[<=]

2.4 Überblick Informationsmodell

Die fachanwendungsspezifischen Informationsmodelle werden in den Spezifikationen der Fachanwendungen beschrieben. Die Dokumente, in denen die Informationsmodelle der Fachanwendungen beschrieben werden, sind in TAB_ADV_091 gelistet.

Neben den fachanwendungsspezifischen Informationsobjekten gibt es im Kontext der AdV folgende Informationsobjekte:

- Protokollierung von eGK-Zugriffen
- Verwaltung freiwilliger Anwendungen mit den zugehörigen Verweisen

PIN-Objekte und Zertifikate werden an dieser Stelle als Eigenschaften der eGK behandelt, nicht als Informationsobjekte der eGK, auf die sich Datenschutzrechte der Versicherten beziehen.

Die Konfiguration der Zugriffe auf Daten des AdV-Informationsmodells wird in Kapitel 6.2 behandelt.

3 Anwendungsfälle

Die vom Versicherten in der AdV ausführbaren Anwendungsfälle lassen sich in fachanwendungsspezifische Funktionen und Kernfunktionen einteilen.

Fachanwendungsspezifische Funktionen werden fachlich durch Fachanwendungen (z. B. NFDM) verantwortet. Die AdV stellt eine Ausführungsumgebung bereit.

Kernfunktionen werden unabhängig von den Fachanwendungen bereitgestellt und dienen der allgemeinen Verwaltung von Datenobjekten auf der eGK.

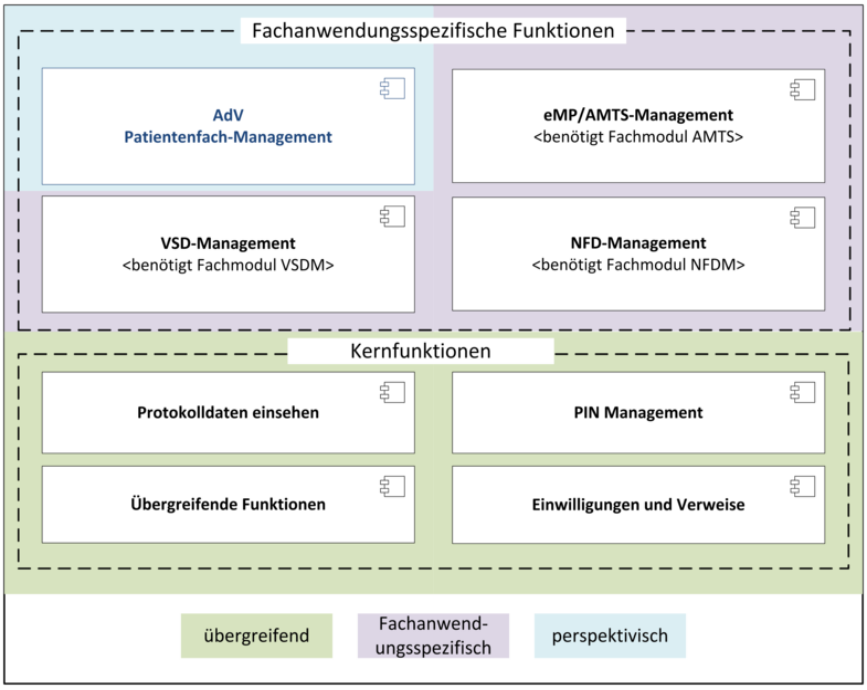

Abbildung 4: Gliederung der Anwendungsfälle für den Versicherten

Ein Teil der Funktionen (z. B. Anwendungsfälle zum Patientenfach) werden erst in einer späteren Ausbaustufe der AdV realisiert. Sie sind in Form eines Ausblicks in Kapitel 7 aufgeführt, ohne dass Anwendungsfälle ausdifferenziert werden.

Für jeden Anwendungsfall erfolgt eine Detaillierung mittels einer tabellarischen Anwendungsfallbeschreibung.

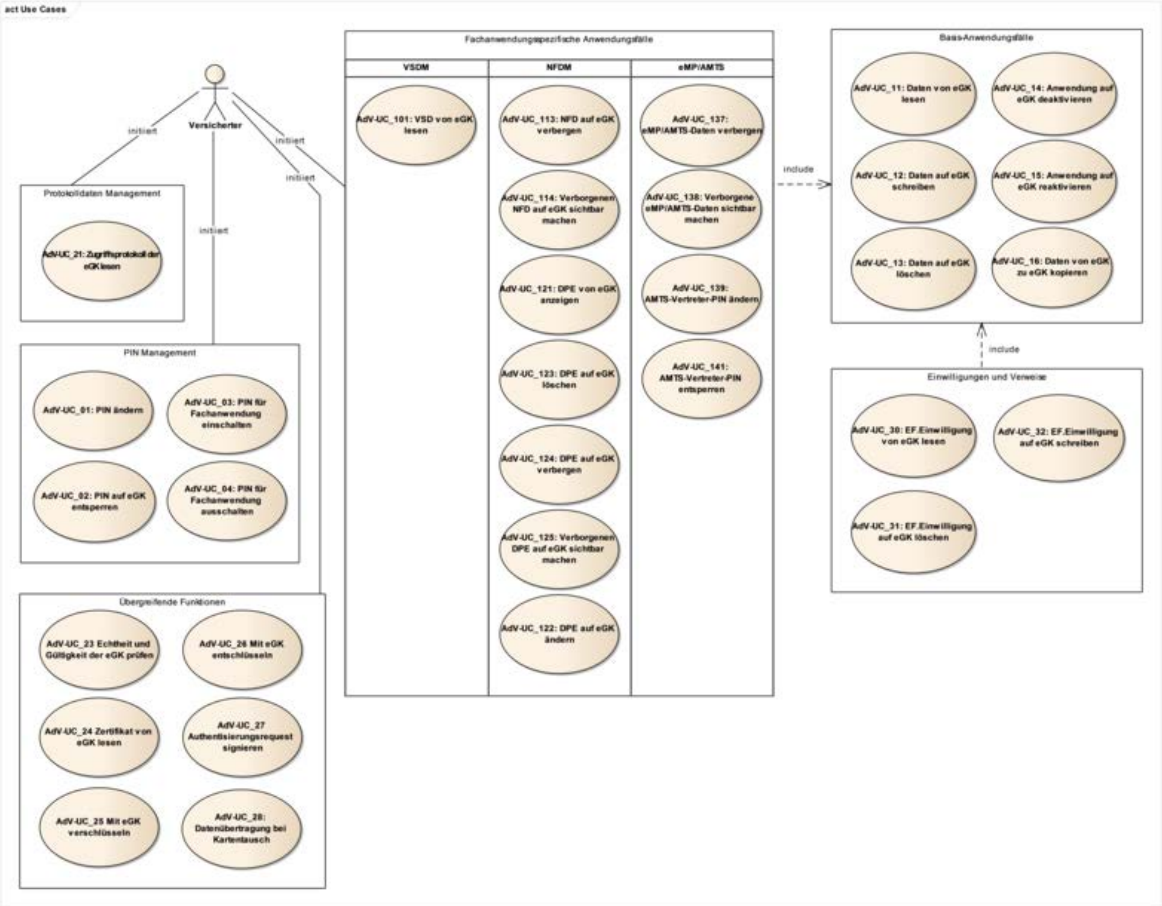

Abbildung 5: Übersicht Use Cases AdV

3.1 Vorbedingungen in den Umgebungen

Damit die Anwendungsfälle ausgeführt werden können, müssen neben den Diensten der TI-Plattform und den Fachdiensten der weiteren Fachanwendungen die folgenden Komponenten in den Umgebungen im Auftrag der Kostenträger betriebsbereit sein:

- ein KTR-AdV-Terminal bzw. ein Gerät des Versicherten als Ausführungsumgebung für die AdV-App
- eine AdV-App mit Zugriff auf den AdV-Server
- ein AdV-Server
- ein Kartenterminal zur Anbindung der eGK
- eine SM-B für KTR-AdV (Profil 1)
- eine eGK

Das SM-B kann, wenn nicht anders beschrieben, in den Ausprägungen SMC-B oder in einem HSM genutzt werden.

Für die folgende Beschreibung der Anwendungsfälle wird angenommen, dass diese Vorbedingungen in den Umgebungen erfüllt sind.

3.2 Übergreifende Erfolgsbedingungen

Folgende Erfolgsbedingungen müssen für alle Operationen erfüllt sein, damit sie erfolgreich zu Ende geführt werden können. Wenn die Erfolgsbedingungen nicht erfüllt sind, so muss die Operation mit einer Fehlermeldung abbrechen.

AdV-A_2010 - Übergreifende Erfolgsbedingung: Aufrufparameter gültig
Die AdV-App MUSS bei allen Operationen mit einer qualifizierten Fehlermeldung abbrechen, wenn notwendige Aufrufparameter unvollständig oder ungültig sind.**[**<=**]**

AdV-A_2011 - Übergreifende Erfolgsbedingung: DF.HCA nicht gesperrt
Die AdV-App MUSS bei allen Operationen mit einer qualifizierten Fehlermeldung abbrechen, wenn die Gesundheitsanwendung der eGK (DF.HCA) gesperrt ist und nicht durch eine Aktualisierung in der Operation entsperrt wird.**[**<=**]**

Die Entsperrung der Gesundheitsanwendung ist durch eine Onlineprüfung und Aktualisierung im Anwendungsfall „Versichertenstammdaten von der eGK lesen“ möglich.

AdV-A_2012 - Übergreifende Erfolgsbedingung: Keine Unterstützung anderer Karten als der eGK
Die Fachanwendung AdV DARF NICHT die Nutzung anderer Karten des Versicherten als die eGK unterstützen.**[**<=**]**

Damit soll sichergestellt werden, dass die Fachanwendung AdV nicht auf KVK, ec-Karten oder sonstigen Karten operiert.

AdV-A_2013 - Übergreifende Erfolgsbedingung: Version eGK
Die AdV-App MUSS bei allen Operationen mit einer qualifizierten Fehlermeldung abbrechen, wenn die eGK Version älter als die Versionsanforderung für die Operation ist.**[**<=**]**

AdV-A_2014 - Übergreifende Erfolgsbedingung: Echtheit der Smartcards
Die AdV-App MUSS bei allen Operationen mit einer qualifizierten Fehlermeldung abbrechen, wenn die beteiligten Smartcards nicht erfolgreich auf Echtheit geprüft werden konnten.**[**<=**]**

Die beteiligten Smartcards sind die eGK und SM-B.

AdV-A_2015 - Übergreifende Erfolgsbedingung: SM-B freigeschaltet
Die AdV-App MUSS bei allen Operationen mit einer qualifizierten Fehlermeldung abbrechen, wenn die beteiligte SM-B nicht freigeschaltet ist.**[**<=**]**

AdV-A_2016 - Übergreifende Erfolgsbedingung: Einverständnis des Versicherten
Die AdV-App MUSS bei Operationen, die eine PIN-Eingabe des Versicherten bedingen, mit einer qualifizierten Fehlermeldung abbrechen, wenn der Versicherte nicht durch PIN-Eingabe sein Einverständnis in die Ausführung dieser Operation gegeben hat.**[**<=**]**

AdV-A_2017 - Übergreifende Erfolgsbedingung: Abbruch im Fehlerfall
Die AdV-App MUSS im Fehlerfall die Operation abbrechen und eine Fehlermeldung zurückgeben.**[**<=**]**

Der Aufbau der Systemmeldungen wird durch das übergeordnete Konzept zum einheitlichen Fehlermanagement bestimmt und die jeweiligen Inhalte in den Spezifikationen der AdV-Produkttypen und weiteren Fachmodulen festgelegt.

3.3 PIN-Handling

Der Zugriff des Versicherten auf die Daten der eGK (außer Persönliche Versichertendaten (PD) und Allgemeine Versicherungsdaten (VD)) ist mittels PIN-Schutz abgesichert. Die PIN.CH ist das PIN-Objekt, dessen Geheimnis durch mehrere Multireferenz-PINs, z. B. MRPIN.NFD und MRPIN.home, genutzt wird. In der Objektsystemspezifikation der eGK [gemSpec_eGK_ObjSys] ist festgelegt, welche Datenobjekte durch welche PINs freigeschaltet werden.

AdV-A_2018 - PIN Abfrage nach Stecken der eGK
Die Fachanwendung AdV MUSS nach dem Stecken der eGK eine Authentifizierung des Versicherten mittels Verifikation der PIN.CH durchführen.**[**<=**]**

Die Verifikation der PIN.CH dient dem Schutz vor Missbrauch der eGK und ermöglicht das Protokollieren für die fachlichen Anwendungsfälle.

Weitere PIN-Abfragen erfolgen im Zusammenhang mit den Anwendungsfällen.

Wenn die Freischaltung eines Bereiches der eGK erfolgt ist, sollen die weitergehenden Aktionen innerhalb dieses Bereiches so optimiert werden, dass keine unnötigen Mehrfacheingaben der PIN erforderlich sind. Dabei kann der einmal für ein Datenobjekt erlangte erhöhte Sicherheitszustand der eGK genutzt werden.

In der Umgebung des Versicherten (@home) wird die MRPIN.home nicht genutzt. Die Freischaltung des Zugriffs auf die Datenobjekte wird über die AdV-App und den AdV-Server umgesetzt. Die im Anforderungskatalog AdV für den Zugriff mittels MRPIN.home vorgesehenen funktionalen Anforderungen werden dabei vollumfänglich von AdV-App und AdV-Server realisiert. Aufgrund der Anbindung der AdV-App an den AdV-Server wird für das Erreichen der Zugriffsberechtigung auf die Daten der eGK ein C2C mit einer SM-B die das Profil für @home abbildet und die Eingabe der PIN.CH bzw. der PIN der Fachanwendung genutzt. Auf diese Weise kann auch in der Umgebung des Versicherten u. a. die durch den Datenschutz geforderte Protokollierung von Datenzugriffen auf der eGK umgesetzt werden.

3.4 Zugriffsprotokollierung auf der eGK

Die Fachanwendung AdV und die weitere Fachanwendungen protokollieren Zugriffe auf die Daten der eGK in EF.Logging.

AdV-A_2137 - Zugriffsprotokolleintrag AdV zuordenbar
Die Fachanwendungen MÜSSEN sicherstellen, dass bei einer Zugriffsprotokollierung auf der eGK aus dem Protokolleintrag hervorgeht, dass der Zugriff in einer AdV-Umgebung stattfand.**[**<=**]**

Dies kann beispielsweise durch die Spezifikation gesonderte Flags für Type of Access erfolgen.

AdV-A_2138 - Protokolleintrag der AdV-Umgebung zuordenbar
Die Fachanwendungen MÜSSEN sicherstellen, dass bei einer Zugriffsprotokollierung auf der eGK aus dem Protokolleintrag hervorgeht, in welcher AdV-Umgebung der Zugriff stattfand.**[**<=**]**

Die AdV-Umgebung wird durch die SM-B identifiziert.

AdV-A_2157 - Protokollierung nach erster Authentifizierung
Die Fachanwendung AdV MUSS einen Eintrag im Zugriffsprotokoll der eGK der Generation kleiner G2.1 nach der ersten Authentifizierung des Versicherten mittels Verifikation der PIN.CH hinzufügen.**[**<=**]**

AdV-A_2158 - Protokollierung in Anwendungsfällen
Die Fachanwendung AdV MUSS für jeden Zugriff auf eine eGK ab einer Generation G2.1 in einem Anwendungsfall zum Lesen, Schreiben oder Löschen von Daten auf der eGK sowie der Verwaltung der medizinischen Fachanwendungen (verbergen, sichtbar machen) einen Eintrag im Zugriffsprotokoll der eGK hinzufügen.**[**<=**]**

Führt der Versicherte in der AdV mit einer eGK G2 mehrere Anwendungsfälle nacheinander aus, dann muss in jedem Anwendungsfall die PIN des Versicherten zur Authentifizierung eingegeben werden. Dies gilt insbesondere, wenn mehrere Anwendungsfälle einer Fachanwendung ausgeführt werden. Für die Optimierung der Benutzerführung soll bei Nutzung der eGK der Generation 2 nur ein Eintrag im Zugriffsprotokoll am Beginn der AdV-Sitzung auf der eGK für alle ausgeführten Anwendungsfälle angelegt werden. Die Zugriffe auf die Daten der eGK in den einzelnen Anwendungsfällen werden nicht auf der eGK geloggt.

3.5 Basis-Anwendungsfälle für die Anwendungsverwaltung

In der Systemlösung werden für den Zugriff auf die Daten von Anwendungen auf der eGK Basis-Anwendungsfälle modelliert. Mit den Basis-Anwendungsfällen können Daten von der eGK gelesen, auf die eGK geschrieben, auf der eGK gelöscht, sowie freiwillige Anwendungen deaktiviert und wieder aktiviert werden.

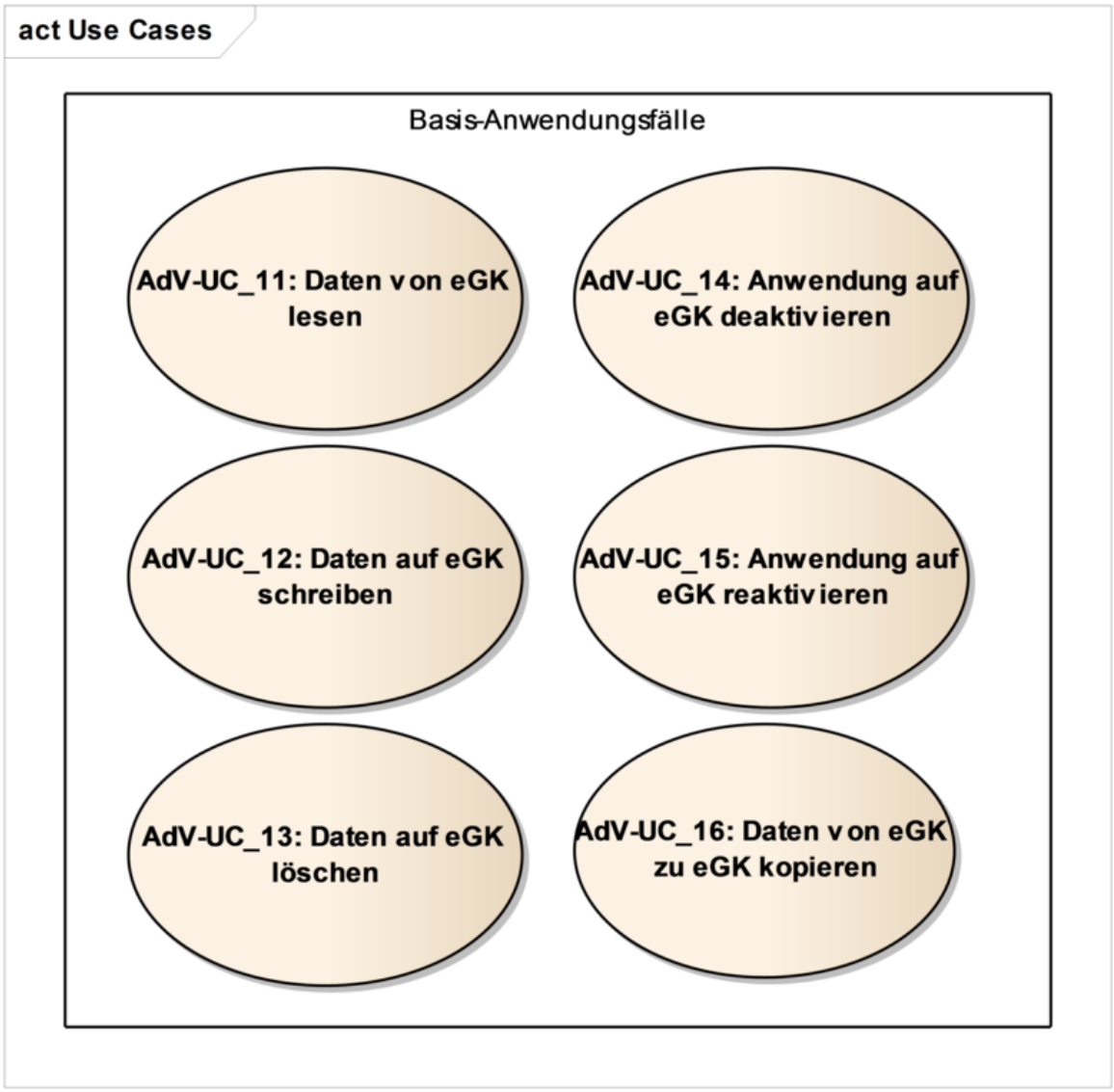

Abbildung 6: Übersicht Basis-Anwendungsfälle AdV

Basis-Anwendungsfälle sind verallgemeinerte Anwendungsfälle für den Datenzugriff auf der eGK. Folgende Aktivitäten können in ihnen aufgerufen werden und sind somit mögliche Bausteine aus denen sich ein Anwendungsfall zusammensetzt:

- AdV-ACT_51: Gültigkeit der eGK prüfen
- AdV-ACT_52: Version der eGK prüfen
- AdV-ACT_53: Echtheit der beteiligten Karten durch C2C prüfen
- AdV-ACT_54: Authentifizierung des Versicherten mittels PIN-Verifikation einholen
- AdV-ACT_55: Daten lesen
- AdV-ACT_56: Daten schreiben
- AdV-ACT_57: Daten löschen
- AdV-ACT_58: Applikation deaktivieren
- AdV-ACT_59: Applikation aktivieren
- AdV-ACT_60: Aufruf einer fachanwendungsspezifischen Operation
- AdV-ACT_61: Datenzugriff protokollieren

Die in Abbildung 5 „Übersicht Use Cases AdV“ dargestellten fachanwendungsspezifischen Anwendungsfälle werden mittels der Basis-Anwendungsfälle umgesetzt. Dafür wird für jeden fachanwendungsspezifischen Anwendungsfall eine Konfiguration angegeben. In der Konfiguration wird festgelegt, welche Bausteine in welcher Reihenfolge mit welchen Parametern ausgeführt werden.

Bausteine können ein- oder mehrmals in einem Anwendungsfall aufgerufen werden.

Wenn die Ergebnisse von Bausteinen deterministisch und reproduzierbar sind, d. h. keine fachliche, zeitliche oder andere Abhängigkeit zwischen den Ergebnissen der Bausteine besteht, dann sollen diese mit dem Ziel einer besseren Performance parallelisiert abgearbeitet werden.

Der Baustein AdV-ACT_60 bietet die Möglichkeit über eine interne Schnittstelle die Operation eines weiteren Fachmoduls aufzurufen. Falls ein fachanwendungsspezifisches Fachmodul (NFDM, AMTS, VSDM) eine Operation für den durchzuführenden Anwendungsfall bereitstellt, wird diese genutzt. In dem Fall kapselt der Basis-Anwendungsfall die Aufrufe von Operationen der fachanwendungsspezifischen Interfaces (I_NFD_Management, I_VSDService, etc.). Die Kommunikation von AdV mit einem weiteren Fachmodul ist von der beteiligten Fachanwendung vorzusehen.

Beim Aufruf einer Operation zur Initiierung eines Basis-Anwendungsfalls an der Außenschnittstelle der AdV-App muss eine spezifische Konfiguration referenziert werden, mit welcher der Basis-Anwendungsfall ausgeführt wird. Dafür wird der Identifier der Anwendung als Parameter angegeben.

Die Konfiguration für einen fachanwendungsspezifischen Anwendungsfall wird durch die beteiligten Fachanwendungen spezifiziert. D. h. die Fachanwendungen legen fest, welche Bausteine der Basis-Anwendungsfälle sie für ihren jeweiligen Anwendungsfall benötigen bzw. nutzen.

Im Kapitel 3.5.1 werden die Bausteine und in den folgenden Kapiteln ab 3.5.2 die Basis-Anwendungsfälle beschrieben. In den Kapiteln 3.6 und 3.7 werden die Konfigurationen der Basis-Anwendungsfälle für die Umsetzung der fachlichen Anwendungsfälle beschrieben.

3.5.1 Bausteine der Basis-Anwendungsfälle

3.5.1.1 Aktivität AdV-ACT_51: Gültigkeit der eGK prüfen

Die Aktivität prüft die Gültigkeit der eGK. Die eGK ist gültig, wenn der HCA-Ordner der eGK aktiv (nicht gesperrt) ist und das AUT-Zertifikat der eGK offline (Ablaufdatum des Authentifizierungszertifikates, rechnerische Prüfung des Authentifizierungszertifikates) und online (Ergebnis des Zertifikatsvalidierungsdienstes) gültig ist.

AdV-A_2019 - Aktivität AdV-ACT_51: Gültigkeit der eGK prüfen
Die AdV MUSS die Aktivität AdV-ACT_51: „Gültigkeit der eGK prüfen“ durchführen.

Abbildung 7: SD AdV-ACT_51 Gültigkeit der eGK prüfen

[<=]

Funktionale Ergänzungen

Wird die Aktivität im Rahmen eines Basis-Anwendungsfalls aufgerufen, muss über die Konfiguration festgelegt werden, ob der Anwendungsfall fortgesetzt oder abgebrochen wird, falls die Online-Prüfung des Gültigkeitsstatus nicht durchgeführt werden konnte.

Über die Konfiguration der Aktivität kann die Prüfung darauf beschränkt werden, ob der HCA-Ordner der eGK aktiv ist. Als Default wird die vollständige Prüfung durchgeführt.

3.5.1.2 Aktivität AdV-ACT_52: Version der eGK prüfen

Die Aktivität liest die Version der eGK von der Karte und prüft diese gegen in der Konfiguration vorgegebenen Werte.

AdV-A_2020 - Aktivität AdV-ACT_52: Version der eGK prüfen
Die AdV MUSS die Aktivität AdV-ACT_52: „Version der eGK prüfen“ durchführen.

Abbildung 8: SD AdV-ACT_52 Version der eGK prüfen

[<=]

Die in der Konfiguration vorgegebenen Werte geben einen Bereich von Versionen der eGK an, für den das Prüfergebnis positiv ist.

3.5.1.3 Aktivität AdV-ACT_53: Echtheit der beteiligten Karten durch C2C prüfen

Die Aktivität führt eine Card-to-Card-Authentisierung zwischen zwei Smartcards durch. Die eGK (Target) wird mittels einer SM-B (Source) mit dem „gegenseitig“-Mode freigeschaltet. Bei der SM-B kann es sich um eine SMC-B oder einem HSM-B handeln.

AdV-A_2021 - Aktivität AdV-ACT_53: Echtheit der beteiligten Karten durch C2C prüfen

Die AdV MUSS die Aktivität AdV-ACT_53: „Echtheit der beteiligten Karten durch C2C prüfen“ durchführen.

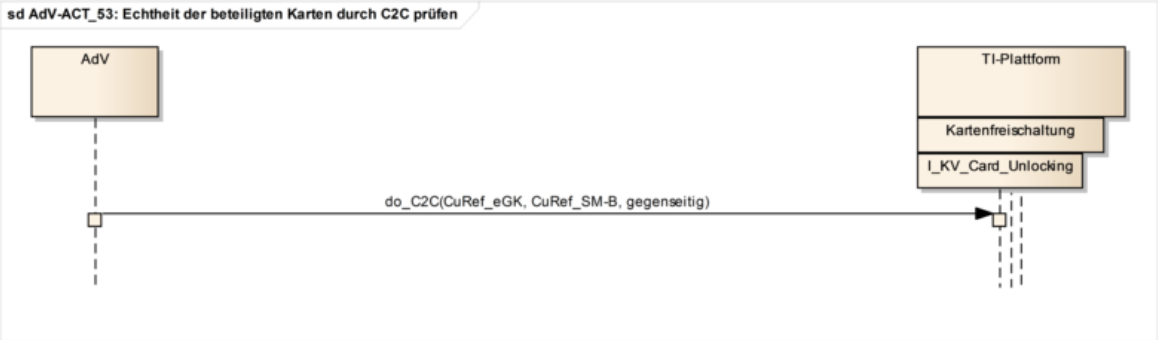

Abbildung 9: SD AdV-ACT_53 Echtheit der beteiligten Karten durch C2C prüfen

[<=]

3.5.1.4 Aktivität AdV-ACT_54: Authentifizierung des Versicherten mittels PIN-Verifikation einholen

Die Aktivität veranlasst eine Aufforderung am Kartenterminal zur Eingabe einer PIN. Das Kartenterminal übermittelt die PIN zum Verifizieren an die eGK. Das Prüfergebnis gibt Aufschluss über Erfolg oder Misserfolg der PIN-Verifikation und ggf. die Anzahl der verbleibenden Versuche zur PIN-Eingabe.

AdV-A_2022 - Aktivität AdV-ACT_54: Authentifizierung des Versicherten mittels PIN-Verifikation einholen

Die AdV MUSS die Aktivität AdV-ACT_54: „Authentifizierung des Versicherten mittels PIN-Verifikation einholen“ durchführen.

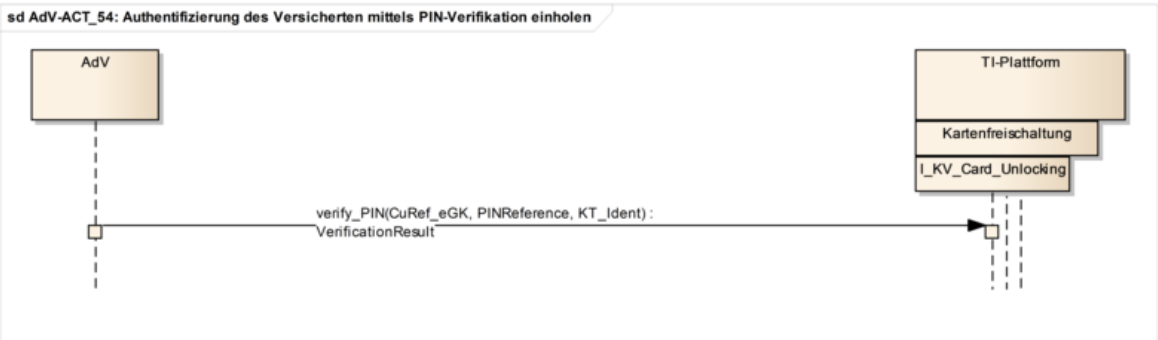

Abbildung 10: SD AdV-ACT_54 Authentifizierung des Versicherten mittels PIN-Verifikation einholen

[<=]

In der Konfiguration der Aktivität wird festgelegt, welche PIN abgefragt wird.

3.5.1.5 Aktivität AdV-ACT_55: Daten lesen

Die Aktivität liest Daten von der eGK.

AdV-A_2023 - Aktivität AdV-ACT_55: Daten lesen
Die AdV MUSS die Aktivität AdV-ACT_55: „Daten lesen“ durchführen.

Abbildung 11: SD AdV-ACT_55 Daten lesen

[<=]

In der Konfiguration der Aktivität wird die Datei (Elementary File (EF)) festgelegt, aus dem die Daten gelesen werden.

3.5.1.6 Aktivität AdV-ACT_56: Daten schreiben

Die Aktivität schreibt Fachdaten auf die eGK.

AdV-A_2024 - Aktivität AdV-ACT_56: Daten schreiben
Die AdV MUSS die Aktivität AdV-ACT_56: „Daten schreiben“ durchführen.

Abbildung 12: SD AdV-ACT_56 Daten schreiben

[<=]

In der Konfiguration der Aktivität wird die Datei (EF) festgelegt, in dem die Daten geschrieben werden.

3.5.1.7 Aktivität AdV-ACT_57: Daten löschen

Die Aktivität löscht Fachdaten von der eGK.

AdV-A_2025 - Aktivität AdV-ACT_57: Daten löschen
Die AdV MUSS die Aktivität AdV-ACT_57: „Daten löschen“ durchführen.

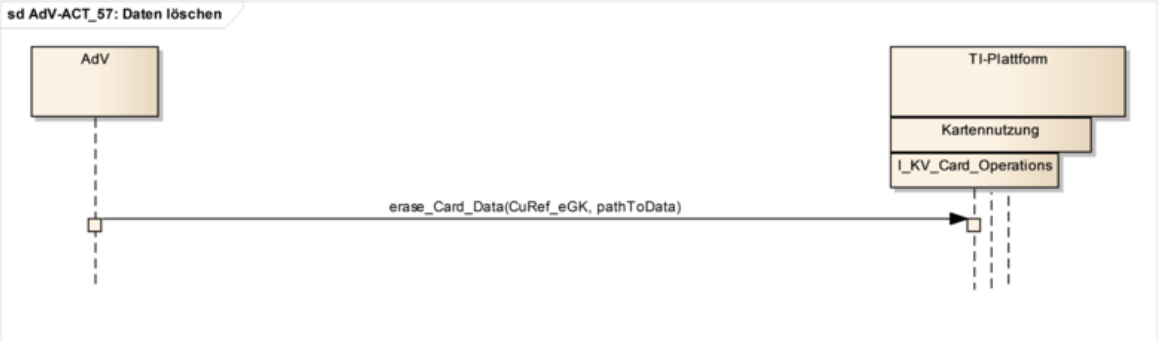

Abbildung 13: SD AdV-ACT_57 Daten löschen

[<=]

In der Konfiguration der Aktivität wird die Datei (EF) festgelegt, aus dem die Daten gelöscht werden.

3.5.1.8 Aktivität AdV-ACT_58: Applikation deaktivieren

Die Aktivität setzt den Status eines Ordners auf der eGK auf inaktiv.

AdV-A_2026 - Aktivität AdV-ACT_58: Applikation deaktivieren
Die AdV MUSS die Aktivität AdV-ACT_58: „Applikation deaktivieren“ durchführen.**[<=]**

Die Funktionalität des Deaktivierens des Ordners einer freiwilligen Fachanwendung wird mit der Operation I_KV_Card_Operations::deactivate_Application als Plattformleistung der Basis-TI zur Verfügung gestellt.

In der Konfiguration der Aktivität wird der Ordner (DF) festgelegt, dessen Status geändert wird.

3.5.1.9 Aktivität AdV-ACT_59: Applikation aktivieren

Die Aktivität setzt den Status eines Ordners auf der eGK auf aktiv.

AdV-A_2027 - Aktivität AdV-ACT_59: Applikation aktivieren
Die AdV MUSS die Aktivität AdV-ACT_59: „Applikation aktivieren“ durchführen.**[<=]**

Die Funktionalität des Aktivierens des Ordners einer freiwilligen Fachanwendung wird mit der Operation I_KV_Card_Operations::activate_Application als Plattformleistung der Basis-TI zur Verfügung gestellt.

In der Konfiguration der Aktivität wird der Ordner (DF) festgelegt, dessen Status geändert wird.

3.5.1.10 Aktivität AdV-ACT_60: Aufruf einer fachanwendungsspezifischen Operation

Die Aktivität ruft die Operation eines weiteren Fachmodules über eine interne Schnittstelle auf.

AdV-A_2028 - Aktivität AdV-ACT_60: Aufruf einer fachanwendungsspezifischen Operation
Die AdV MUSS die Aktivität AdV-ACT_60: „Aufruf einer fachanwendungsspezifischen Operation“ durchführen.

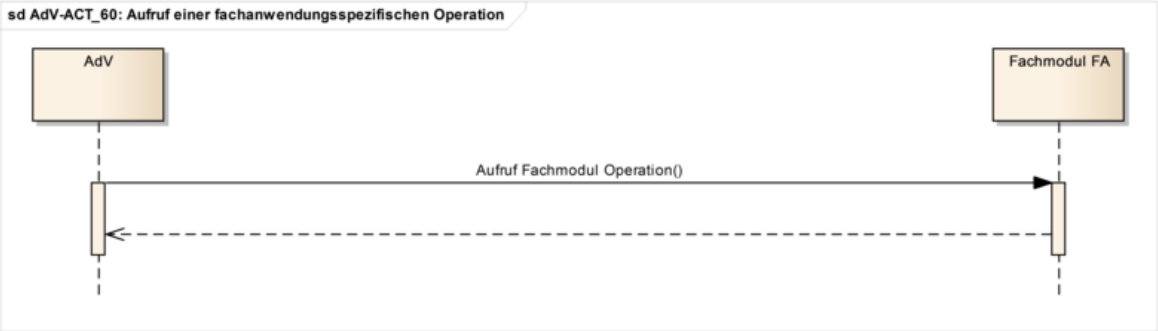

Abbildung 14: SD AdV-ACT_60 Aufruf einer fachanwendungsspezifischen Operation

[<=]

Funktionale Ergänzungen

Das Ergebnis der aufgerufenen Operation wird durch das Fachmodul AdV unverändert an das AdV-Terminal weitergeleitet.

3.5.1.11 Aktivität AdV-ACT_61: Datenzugriff protokollieren

Die Aktivität schreibt einen Protokolleintrag auf die eGK. Voraussetzung ist, dass durch eine vorangegangene Card-to-Card-Authentisierung und eine Verifikation der PIN.CH bereits der benötige Sicherheitszustand hergestellt wurde.

AdV-A_2029 - Aktivität AdV-ACT_61: Datenzugriff protokollieren
Die AdV MUSS die Aktivität AdV-ACT_61: „Datenzugriff protokollieren“ durchführen.

Abbildung 15: SD AdV-ACT_61 Datenzugriff protokollieren

[<=]

Funktionale Ergänzungen

Aus dem Protokolleintrag muss ersichtlich sein, dass der Datenzugriff in einer AdV-Umgebung stattfand.

3.5.2 Daten von eGK lesen

Der Anwendungsfall stellt eine generische Funktionalität zum Lesen von Daten einer Anwendung von der eGK zu Verfügung. Für die Verwendung muss eine Konfiguration festgelegt werden, in der angegeben wird, auf welche Datenobjekte zugegriffen und welche Bausteine im Ablauf des Anwendungsfalls mit welchen Parametern ausgeführt werden.

AdV-A_2030 - Anwendungsfall AdV-UC_11: Daten von eGK lesen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_11: „Daten von eGK lesen“ abbilden.**[<=]**

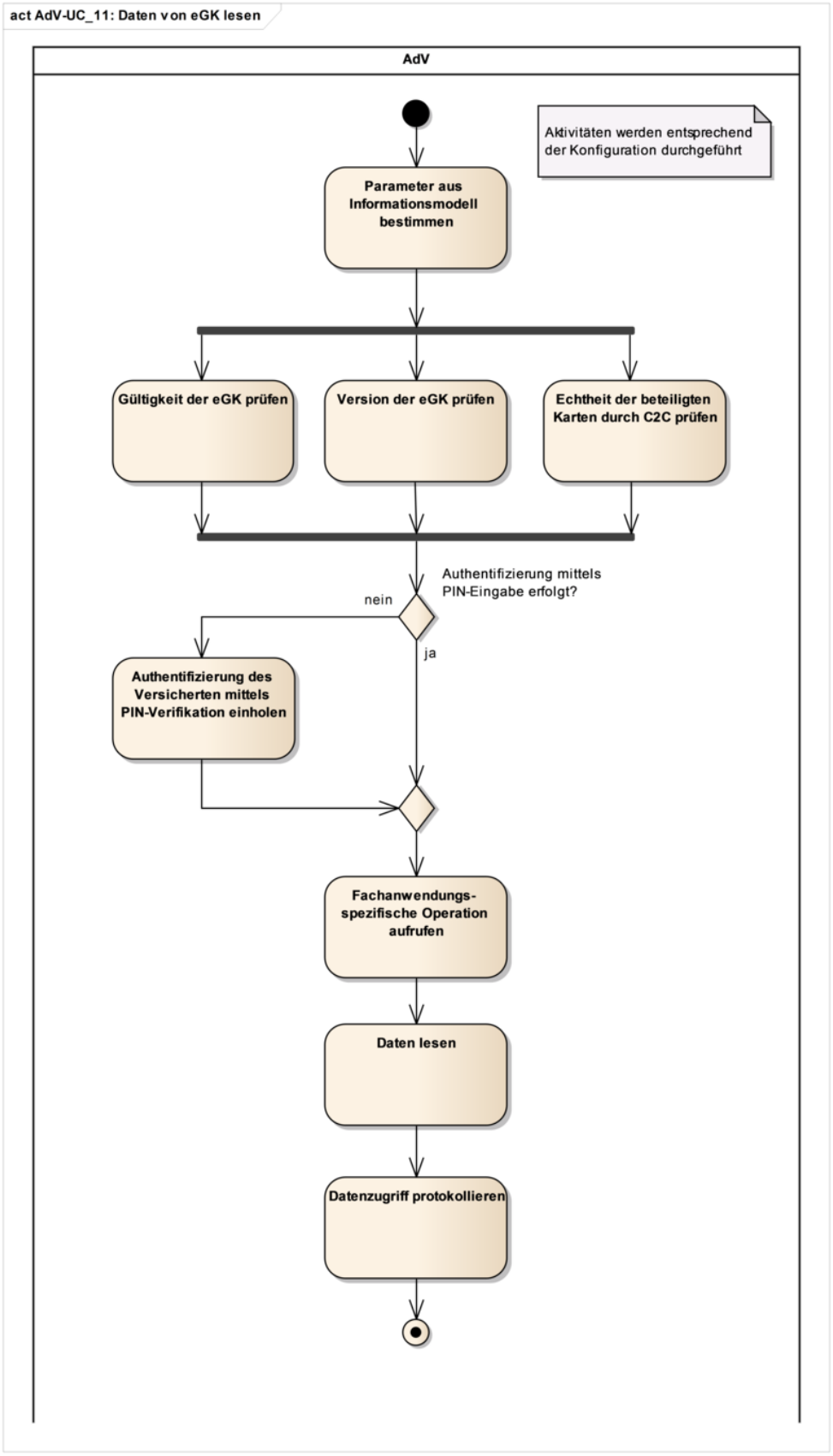

Abbildung 16: Darstellung AdV-UC_11: „Daten von eGK lesen“

Tabelle 2: TAB_ADV_002 Anwendungsfall AdV-UC_11

ID	AdV-UC_11	
Name	Daten von eGK lesen	
Kurzbeschreibung	Der Anwendungsfall liest die Daten einer Anwendung von der eGK des Versicherten.	
Initiierender Akteur	Versicherter über AdV-Umgebung	
Vorbedingungen	Der Ordner auf der eGK ist nicht verborgen. Verifikation der PIN.CH erfolgreich durchgeführt.	
Eingangsdaten	Identifikator eGK Identifier der Anwendung	
Auslöser	Die Auswahl wird über die Benutzeroberfläche getroffen.	
Nachbedingungen	Die Daten stehen in der AdV zur Anzeige zur Verfügung. Falls gefordert, ist der Zugriffsprotokolleintrag auf die eGK des Versicherten geschrieben.	
Ausgangsdaten	Daten der Anwendung Statusinformationen	
Bausteine		
ID	Aktivität	Details
	Bestimmen der anwendungsspezifischen Parameter für die Ausführung des Anwendungsfalls aus dem Informationsmodell	u. a. • Identifikator SM-B • Datei (mehrere möglich) • Optionale Teilschritte der Operation • Parameter der Operationen
AdV-ACT_51	Gültigkeit der eGK prüfen	Status des DF.HCA und Gültigkeit des AUT Zertifikates prüfen
AdV-ACT_52	Version der eGK prüfen	Version von eGK lesen und

		prüfen
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	Freischaltung SM-B prüfen
Card-to-Card-Authentisierung		
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	
AdV-ACT_60	Aufruf einer fachanwendungsspezifischen Operation	Operation eines weiteren Fachmodules
AdV-ACT_55	Daten lesen	Mehrfacher Aufruf, falls mehrere Dateien konfiguriert.
AdV-ACT_61	Datenzugriff protokollieren	

Funktionale Ergänzungen

Die Berechtigung zum Lesen von Anwendungsdaten wird von den Fachanwendungen und dem Objektsystem der eGK gesteuert.

3.5.3 Daten auf eGK schreiben

Der Anwendungsfall stellt eine generische Funktionalität zum Schreiben von Daten einer Anwendung auf die eGK zu Verfügung.

AdV-A_2031 - Anwendungsfall AdV-UC_12: Daten auf eGK schreiben
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_12: „Daten auf eGK schreiben“ abbilden.
[<=]

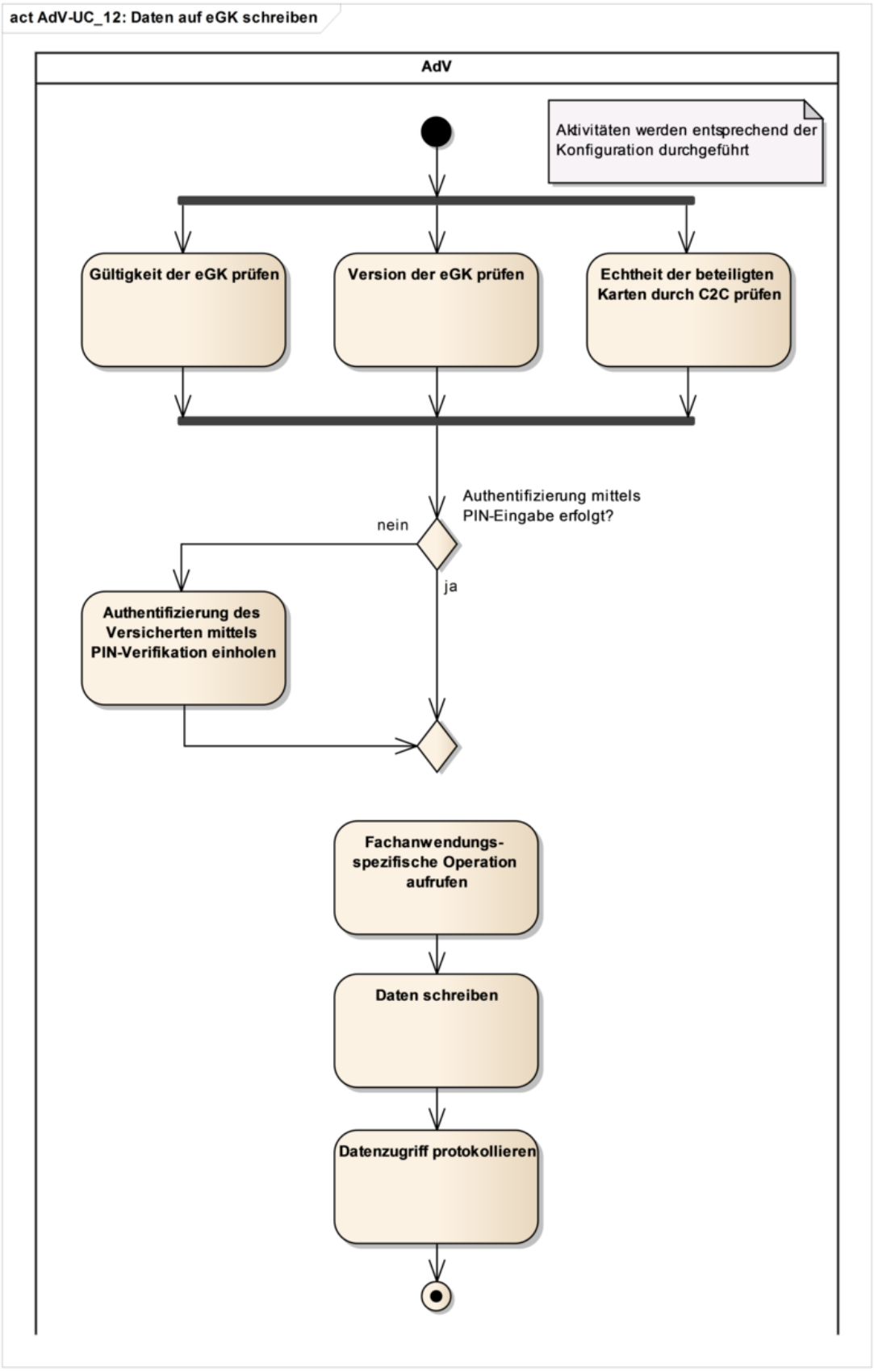

Abbildung 17: Darstellung AdV-UC_12: „Daten auf eGK schreiben“

Tabelle 3: TAB_ADV_003 Anwendungsfall AdV-UC_12

ID	AdV-UC_12	
Name	Daten auf eGK schreiben	
Kurzbeschreibung	Der Anwendungsfall schreibt die Daten einer Anwendung auf die eGK des Versicherten.	
Initiierender Akteur	Versicherter über AdV-Umgebung	
Vorbedingungen	Der Ordner auf der eGK ist nicht verborgen. Verifikation der PIN.CH erfolgreich durchgeführt.	
Eingangsdaten	Identifikator eGK Identifier der Anwendung CardDataDetails (optional) Daten CardDataDetails (optional) Daten (optional)	
Auslöser	Die Auswahl wird über die Benutzeroberfläche getroffen.	
Nachbedingungen	Die Daten der Anwendung sind auf die eGK geschrieben. Falls gefordert, ist der Zugriffsprotokolleintrag auf die eGK des Versicherten geschrieben.	
Ausgangsdaten	Daten der Anwendung Statusinformation	
Bausteine		
ID	Aktivität	Details
	Bestimmen der anwendungsspezifischen Parameter für die Ausführung des Anwendungsfalls aus dem Informationsmodell	u. a. • Identifikator SM-B • Datei (mehrere möglich) • Optionale Teilschritte der Operation • Parameter der Operationen

AdV-ACT_51	Gültigkeit der eGK prüfen	
AdV-ACT_52	Version der eGK prüfen	Version von eGK lesen und prüfen
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	Freischaltung SM-B prüfen
Card-to-Card-Authentisierung		
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	
AdV-ACT_60	Aufruf einer fachanwendungsspezifischen Operation	Operation eines weiteren Fachmodules
AdV-ACT_56	Daten schreiben	Mehrfacher Aufruf, falls mehrere Dateien konfiguriert.
AdV-ACT_61	Datenzugriff protokollieren	

3.5.4 Daten auf eGK löschen

Der Anwendungsfall stellt eine generische Funktionalität zum Löschen von Daten einer Anwendung von der eGK zu Verfügung.

AdV-A_2032 - Anwendungsfall AdV-UC_13: Daten auf eGK löschen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_13: „Daten auf eGK löschen“ abbilden.
[<=]

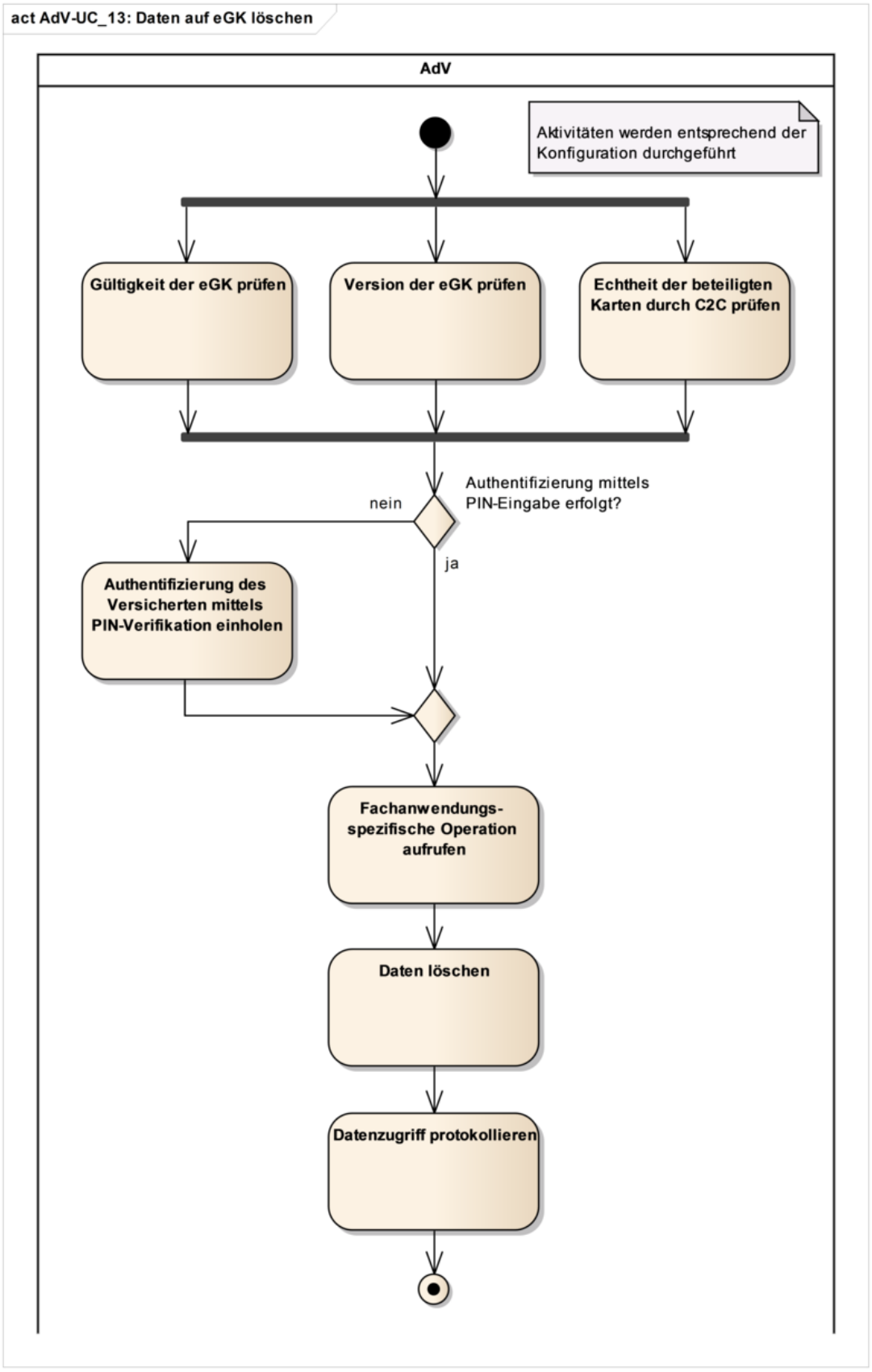

Abbildung 18: Darstellung AdV-UC_13: „Daten auf eGK löschen“

Tabelle 4: TAB_ADV_004 Anwendungsfall AdV-UC_13

ID	AdV-UC_13	
Name	Daten auf eGK löschen	
Kurzbeschreibung	Der Anwendungsfall löscht die Daten einer Anwendung von der eGK des Versicherten.	
Initiierender Akteur	Versicherter über AdV-Umgebung	
Vorbedingungen	Es sind Daten für die Anwendung auf der eGK gespeichert. Der Ordner auf der eGK ist nicht verborgen. Verifikation der PIN.CH erfolgreich durchgeführt.	
Eingangsdaten	Identifikator eGK Identifier der Anwendung Identifier der zu löschenden Daten	
Auslöser	Die Auswahl wird über die Benutzeroberfläche getroffen.	
Nachbedingungen	Die Daten der Anwendung sind nicht mehr auf der eGK gespeichert. Falls gefordert, ist der Zugriffsprotokolleintrag auf die eGK des Versicherten geschrieben.	
Ausgangsdaten	Statusinformation	
Bausteine		
ID	Aktivität	Details
	Bestimmen der anwendungsspezifischen Parameter für die Ausführung des Anwendungsfalls aus dem Informationsmodell	u. a. • Identifikator SM-B • Datei (mehrere möglich) • Optionale Teilschritte der Operation • Parameter der Operationen
AdV-ACT_51	Gültigkeit der eGK prüfen	

AdV-ACT_52	Version der eGK prüfen	Version von eGK lesen und prüfen
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	Freischaltung SM-B prüfen
Card-to-Card-Authentisierung		
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	
AdV-ACT_60	Aufruf einer fachanwendungsspezifischen Operation	Operation eines weiteren Fachmodules
AdV-ACT_57	Daten löschen	Mehrfacher Aufruf, falls mehrere Dateien konfiguriert.
AdV-ACT_61	Datenzugriff protokollieren	

3.5.5 Daten einer Anwendung auf eGK verbergen

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

Technisch wird der Zustand durch den Status des Ordners der freiwilligen Anwendung (z. B. DF.NFD) abgebildet.

AdV-A_2033 - Anwendungsfall AdV-UC_14: Anwendung auf eGK deaktivieren
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_14: „Anwendung auf eGK deaktivieren“ abbilden.
[<=]

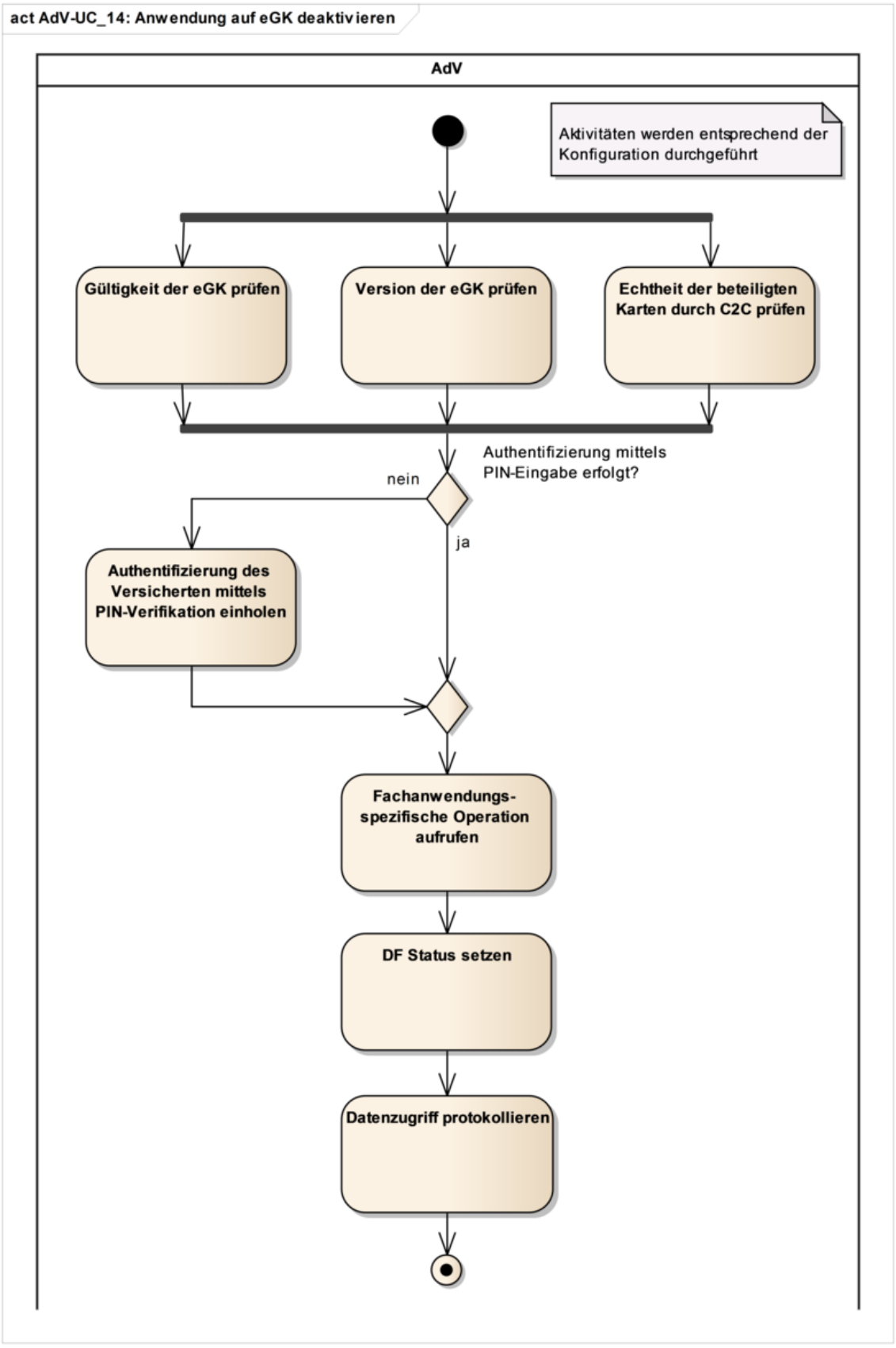

Abbildung 19: Darstellung AdV-UC_14: „Anwendung auf eGK deaktivieren“

Tabelle 5: TAB_ADV_005 Anwendungsfall AdV-UC_14

ID	**AdV-UC_14**	
Name	Anwendung auf eGK deaktivieren	
Kurzbeschreibung	Der Anwendungsfall deaktiviert den Ordner einer freiwilligen Anwendung und verbirgt somit die Daten dieser Anwendung auf der eGK des Versicherten.	
Initiierender Akteur	Versicherter über AdV-Umgebung	
Vorbedingungen	Der Ordner der Anwendung hat den Status aktiv. Verifikation der PIN.CH erfolgreich durchgeführt.	
Eingangsdaten	Identifikator eGK Identifier der Anwendung	
Auslöser	Die Auswahl wird über die Benutzeroberfläche getroffen.	
Nachbedingungen	Die Daten der Anwendung auf der eGK des Versicherten sind verborgen, d. h. der zugehörige Ordner ist deaktiviert.	
Ausgangsdaten	Statusinformation	
Bausteine		
ID	Aktivität	Details
	Bestimmen der anwendungsspezifischen Parameter für die Ausführung des Anwendungsfalls aus dem Informationsmodell	u. a. • Identifikator SM-B • Ordner • Optionale Teilschritte der Operation • Parameter der Operationen
AdV-ACT_51	Gültigkeit der eGK prüfen	

AdV-ACT_52	Version der eGK prüfen	Version von eGK lesen und prüfen
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	Freischaltung SM-B prüfen
Card-to-Card-Authentisierung		
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	
AdV-ACT_60	Aufruf einer fachanwendungsspezifischen Operation	Operation eines weiteren Fachmodules
AdV-ACT_58	Applikation deaktivieren	DF deaktivieren
AdV-ACT_61	Datenzugriff protokollieren	

3.5.6 Verborgene Daten auf eGK wieder sichtbar machen

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

Technisch wird der Zustand durch den Status des Ordners der freiwilligen Anwendung (z. B. DF.NFD) abgebildet.

AdV-A_2034 - Anwendungsfall AdV-UC_15: Anwendung auf eGK reaktivieren
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_15: „Anwendung auf eGK reaktivieren“ abbilden.
[<=]

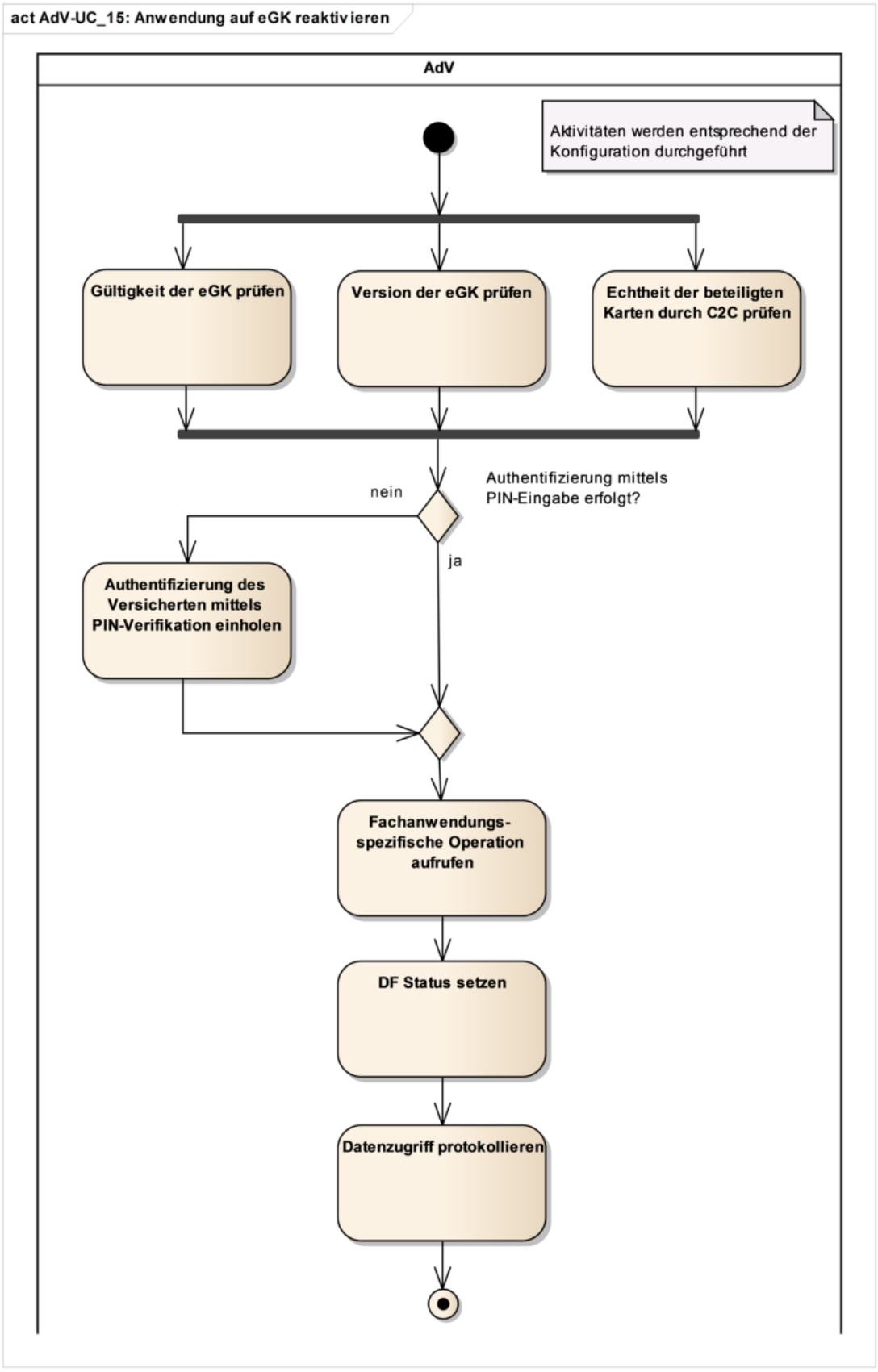

Abbildung 20: Darstellung AdV-UC_15: „Anwendung auf eGK reaktivieren“

Tabelle 6: TAB_ADV_006 Anwendungsfall AdV-UC_15

ID	**AdV-UC_15**	
Name	Anwendung auf eGK reaktivieren	
Kurzbeschreibung	Die zuvor durch den Versicherten verborgenen Daten einer Anwendung werden auf dessen eGK wieder sichtbar gemacht.	
Initiierender Akteur	Versicherter über AdV-Umgebung	
Vorbedingungen	Der Ordner der Anwendung hat den Status deaktiviert. Verifikation der PIN.CH erfolgreich durchgeführt.	
Eingangsdaten	Identifikator eGK Identifier der Anwendung	
Auslöser	Die Auswahl wird über die Benutzeroberfläche getroffen.	
Nachbedingungen	Die Daten der Anwendung auf der eGK des Versicherten sind sichtbar, d. h. der zugehörige Ordner ist aktiviert.	
Ausgangsdaten	Statusinformation	
Bausteine		
ID	Aktivität	Details
	Bestimmen der anwendungsspezifischen Parameter für die Ausführung des Anwendungsfall aus dem Informationsmodell	u. a. • Identifikator SM-B • Ordner • Optionale Teilschritte der Operation • Parameter der Operationen
AdV-ACT_51	Gültigkeit der eGK prüfen	
AdV-ACT_52	Version der eGK prüfen	Version von eGK lesen und prüfen

AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	Freischaltung SM-B prüfen
Card-to-Card-Authentisierung		
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	
AdV-ACT_60	Aufruf einer fachanwendungsspezifischen Operation	Operation eines weiteren Fachmodules
AdV-ACT_59	Applikation aktivieren	DF aktivieren
AdV-ACT_61	Datenzugriff protokollieren	

3.5.7 Daten von eGK zu eGK kopieren

Da die TI-Plattform in dem für ORS2.1 geplanten Ausbau nicht über das Leistungsmerkmal des Daten- und Berechtigungserhalts bei Kartenwechsel verfügt, wird diese Funktionalität direkt in den AdV-Komponenten implementiert. Eine durch die TI-Plattform bereitgestellte Lösung kann diese Projektumsetzung später ersetzen.

Wenn die Krankenkasse einen Kartentausch initiiert und der Versicherte eine neue eGK erhält, soll die Möglichkeit bestehen, die Daten freiwilliger Anwendungen von der alten auf die neue Karte zu übertragen.

Der Anwendungsfall stellt eine Funktionalität zum Kopieren von Daten der Anwendungen von der Quell-eGK auf ein Ziel-eGK zur Verfügung. Hierbei werden sowohl die Anwendungsdaten als auch die Informationen zur Einwilligung übertragen.

AdV-A_2035 - Anwendungsfall AdV-UC_16: Daten von eGK zu eGK kopieren
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_16: „Daten von eGK zu eGK kopieren“ abbilden.
[<=]

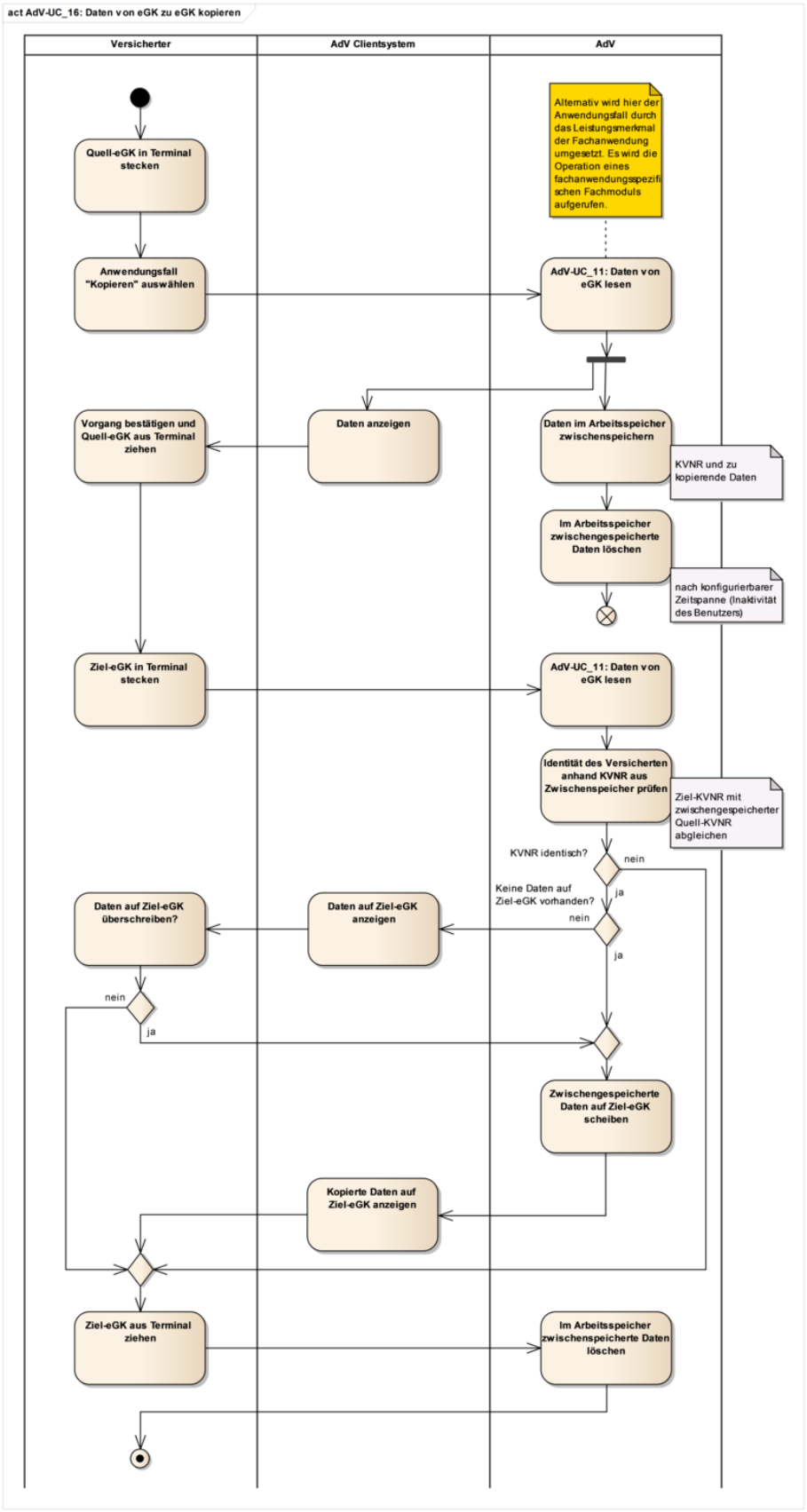

Abbildung 21: Darstellung AdV-UC_16: „Daten von eGK zu eGK kopieren“

Tabelle 7: TAB_ADV_007 Anwendungsfall AdV-UC_16

ID	AdV-UC_16
Name	Daten von eGK zu eGK kopieren
Kurzbeschreibung	Der Anwendungsfall kopiert die Daten von Fachanwendungen von einer ersetzten eGK zur neuen eGK desselben Versicherten.
Initiierender Akteur	Versicherter über AdV-Umgebung
Vorbedingungen	Der DF.HCA der Quell eGK ist aktiv. Die Ziel-eGK ist gültig.
Eingangsdaten	Die alte eGK (Quell-eGK) und neue eGK (Ziel-eGK) des Versicherten Identifier der Anwendungen, deren Daten zu übertragen sind.
Auslöser	Die Auswahl wird über die Benutzeroberfläche getroffen.
Nachbedingungen	Die Daten der Anwendung auf der Quell-eGK sind in Dateien des Ordners der Anwendung auf der Ziel-eGK gespeichert.
Ausgangsdaten	Statusinformation

Funktionale Ergänzungen

Die Prüfung der Gültigkeit der Quell-eGK wird darauf beschränkt, ob der HCA-Ordner der eGK aktiv ist.

Für die Umsetzung des Anwendungsfalls sind aus Gründen des Datenschutzes folgende Anforderungen zu erfüllen:

AdV-A_2159 - AdV-UC_16: Quell-eGK und Ziel-eGK eines Versicherten
Die Fachanwendung AdV MUSS im Anwendungsfall AdV-UC_16 sicherstellen, dass die Quell-eGK und Ziel-eGK demselben Versicherten gehören.**[**<=**]**

AdV-A_2036 - AdV-UC_16: Kein persistentes Speichern der Daten
Die Fachanwendung AdV DARF NICHT die im Anwendungsfall AdV-UC_16 zu übertragenden Daten persistent speichern, sondern nur temporär im Arbeitsspeicher halten.**[**<=**]**

AdV-A_2037 - AdV-UC_16: Löschen nach Übertragen
Die Fachanwendung AdV MUSS die im Anwendungsfall AdV-UC_16 zu übertragenden Daten zum Abschluss des Anwendungsfalls so aus dem temporären Arbeitsspeicher löschen, dass sie nicht wiederherstellbar sind.**[**<=**]**

AdV-A_2038 - AdV-UC_16: Abbruch nach Inaktivität des Versicherten
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_16 abbrechen und die temporär gespeicherten Daten nicht-wiederherstellbar löschen, wenn eine benötigte Interaktion des Versicherten nicht innerhalb eines festgelegten Zeitraumes erfolgt.
[<=**]**

3.6 Anwendungsfälle zu Kernfunktionen

3.6.1 Protokolldaten Management

3.6.1.1 Zugriffsprotokolle der eGK lesen

Mit diesem Anwendungsfall werden dem Versicherten die auf der eGK gespeicherten Protokolleinträge angezeigt.

AdV-A_2039 - Anwendungsfall AdV-UC_21: Zugriffprotokoll von eGK lesen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_21: „Zugriffprotokoll von eGK lesen“ abbilden.
[<=]

Tabelle 8: TAB_ADV_008 Anwendungsfall AdV-UC_21

ID	AdV-UC_21
Name	Zugriffprotokoll von eGK lesen
Kurzbeschreibung	Das Fachmodul AdV bzw. die AdV-App liest die Einträge des Zugriffprotokolls von der eGK des Versicherten. Die Daten werden im AdV-Terminal angezeigt.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_11 Daten von eGK lesen Parameter: eGK Identifier, „Protokoll“

Tabelle 9: TAB_ADV_009 Konfiguration AdV-UC_21

ID	Aktivität	Parameter
	Parameter aus Informationsmodell bestimmen	Datei EF.Logging SM-B
AdV-ACT_51	Gültigkeit der eGK prüfen	Nur Sperrung DF.HCA prüfen
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	eGK, SM-B
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	PIN.CH
AdV-ACT_55	Daten lesen	EF.Logging

Die Operation zum Anwendungsfall liefert eine Liste von Einträgen des Zugriffsprotokolls zurück. Eine Sortierung oder eine Gruppierung der Einträge, z. B. nach Anwendungen, kann in der GUI erfolgen.

AdV-A_2139 - Darstellung Protokolleinträge
Die Fachanwendung AdV MUSS die Einträge des Zugriffsprotokolls in einer für den Versicherten verständlichen Form derart anzeigen, dass der Versicherte daraus die Information ablesen kann, wer, wann und in welcher Umgebung auf die eGK des Versicherten zugegriffen hat.**[<=]**

3.6.2 PIN Management

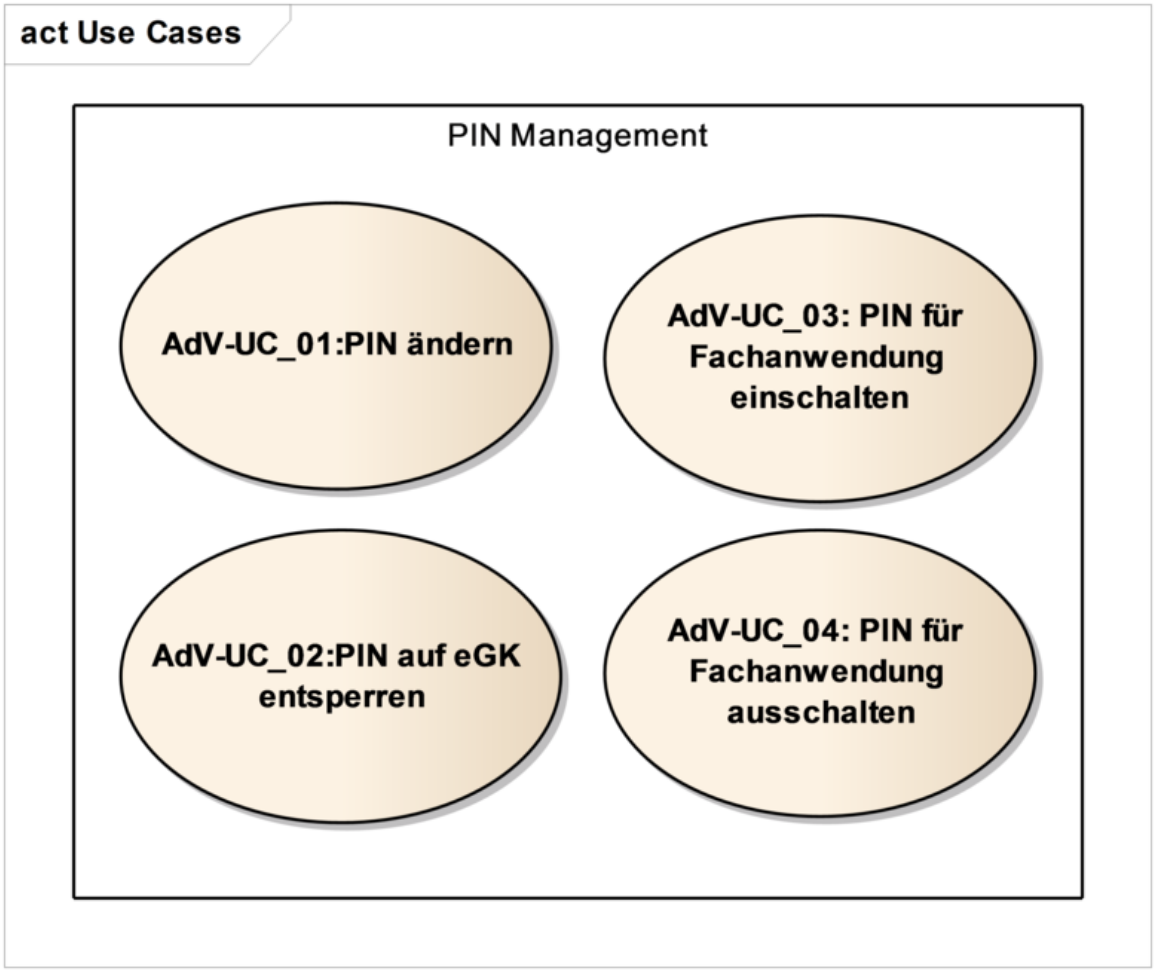

Abbildung 22: Übersicht Anwendungsfälle PIN-Management

Diese Anwendungsfälle stellen dem Versicherten Funktionalitäten zur Verwaltung seiner PIN-Objekte zur Verfügung. Ferner soll der Versicherte den aktuellen Status seiner PIN-Objekte einsehen können.

AdV-A_2543 - Anzeige des Status eines PIN-Objekts

Die Fachanwendung AdV MUSS dem Versicherten über die Benutzeroberfläche den aktuellen Status eines ausschaltbaren PIN-Objekts darstellen, damit der Versicherte entscheiden kann, ob er die jeweilige PIN ein- oder ausschalten möchte.

[<=]

3.6.2.1 PIN ändern

Der Versicherte kann die im Zusammenhang mit der eGK genutzten PINs ändern. Hierzu wird er bei der Ausführung des Anwendungsfalls aufgefordert, zunächst die bisher gültige und anschließend seine neue PIN am Kartenterminal einzugeben. Mit einer wiederholten Eingabe seiner neuen PIN bestätigt er die neue PIN.

AdV-A_2040 - Anwendungsfall AdV-UC_01: „PIN ändern“
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_01: „PIN ändern“ abbilden.**[<=]**

Tabelle 10: TAB_ADV_010 Anwendungsfall AdV-UC_01

ID	AdV-UC_01	
Name	PIN ändern	
Kurzbeschreibung	Der Versicherte ändert das Geheimnis für ein PIN-Objekt auf der eGK.	
Initiierender Akteur	Versicherter über AdV-Umgebung	
AdV-Umgebung	KTR-AdV-Umgebung, @home	
Vorbedingungen	keine	
Eingangsdaten	Identifikator eGK Identifikator des PIN-Objektes	
Auslöser	Am AdV-Terminal wird die Operation „change_PIN“ der Schnittstelle „I_PIN_Management“ aufgerufen.	
Nachbedingungen	Das Geheimnis des PIN-Objektes ist überschrieben.	
Ausgangsdaten	Statusinformation Anzahl der verbleibenden Versuche	
Bausteine		
Aktivität	Aufrufe	Details
AdV-ACT_52	Version der eGK prüfen	G2 und höher
TI-Plattformoperation	I_KV_Card_Unlocking::change_PIN	

Funktionale Ergänzungen

Das Objektsystem der eGK steuert, für welche PIN-Objekte der Anwendungsfall durchgeführt werden kann. Auf einer eGK der Generation 2 und höher können die PIN Objekte PIN.CH, PIN.QES und PIN.AMTS_REP durch den Versicherten geändert werden. Um die PIN.CH zu ändern, kann auch eine MRPIN beim Aufruf des Anwendungsfalls referenziert werden.

Die Funktionalität des Änderns von PIN-Objekten wird als Plattformleistung der Basis-TI zur Verfügung gestellt.

Abbildung 23: SD PIN ändern

3.6.2.2 PIN der eGK mit PUK entsperren

Ist eine PIN auf der eGK nach drei Fehleingaben gesperrt, kann die PIN mit diesem Anwendungsfall wieder freigeschaltet werden. Der Versicherte wird aufgefordert seinen Personal Unblocking Key (PUK) und eine neue PIN am Kartenterminal einzugeben.

AdV-A_2041 - Anwendungsfall AdV-UC_02: PIN auf eGK entsperren
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_02: „PIN auf eGK entsperren“ abbilden.**[<=]**

Tabelle 11: TAB_ADV_011 Anwendungsfall AdV-UC_02

ID	**AdV-UC_02**	
Name	PIN der eGK entsperren	
Kurzbeschreibung	Der Versicherte entsperrt eine blockierte PIN auf der eGK und legt eine neue PIN fest.	
Initiierender Akteur	Versicherter über AdV-Umgebung	
AdV-Umgebung	KTR-AdV-Umgebung, @home	
Vorbedingungen	PIN-Objekt ist blockiert	
Eingangsdaten	Identifikator eGK Identifikator des PIN-Objektes PIN-Setzungsmodus	
Auslöser	Die Auswahl wird über die Benutzeroberfläche getroffen.	
Nachbedingungen	PIN-Objekt ist entsperrt.	

Ausgangsdaten	Statusinformation Anzahl der verbleibenden Versuche des PUK	
Bausteine		
Aktivität	Aufrufe	Details
AdV-ACT_52	Version der eGK prüfen	G2 und höher
TI-Plattformoperation	I_KV_Card_Unlocking::unblock_PIN	

Funktionale Ergänzungen

Das Objektsystem der eGK steuert, für welche PIN-Objekte der Anwendungsfall durchgeführt werden kann. Auf einer eGK der Generation 2 und höher können die PIN-Objekte PIN.CH und PIN.QES mit ihrer PUK entsperrt werden. Für PIN.CH wird nach dem Entsperren die Eingabe einer neuen PIN gefordert. Für PIN.QES wird keine neue PIN gefordert. Das Entsperren der AMTS-Vertreter-PIN PIN.AMTS_REP erfolgt mit der PIN des Versicherten.

Die Funktionalität des Entsperrens von PIN-Objekten wird als Plattformleistung der Basis TI zur Verfügung gestellt.

Abbildung 24: SD PIN auf eGK entsperren

3.6.2.3 PIN für Fachanwendung einschalten

Wenn die Multireferenz-PIN einer Fachanwendung deaktiviert ist, dann kann der Versicherte diese PIN mit diesem Anwendungsfall aktivieren. Der Versicherte wird dafür zur Eingabe seiner PIN am Kartenterminal aufgefordert. Zuvor muss der Versicherte darauf hingewiesen werden, dass mit dem Einschalten der PIN für diese Fachanwendung, zusätzliche PIN-Eingaben notwendig werden, die einem höheren Schutz der Daten dienen.

AdV-A_2544 - Hinweis auf höheren Schutz der Daten bei aktivierter PIN
Die Fachanwendung AdV MUSS den Versicherten über die Benutzeroberfläche darüber informieren, dass das Einschalten einer PIN zu einem höheren Schutz der Daten und zusätzlichen PIN-Eingaben führt.**[<=]**

AdV-A_2042 - Anwendungsfall AdV-UC_03: PIN für Fachanwendung einschalten
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_03: „PIN für Fachanwendung einschalten“ abbilden.**[<=]**

Tabelle 12: TAB_ADV_012 Anwendungsfall AdV-UC_03

ID	AdV-UC_03	
Name	PIN für Fachanwendung einschalten	
Kurzbeschreibung	Der Versicherte aktiviert die PIN für eine Fachanwendung auf der eGK.	
Initiierender Akteur	Versicherter über AdV-Umgebung	
AdV-Umgebung	KTR-AdV-Umgebung, @home	
Vorbedingungen	PIN-Objekt ist deaktiviert Versicherte wurde auf erhöhten Schutz der Daten hingewiesen	
Eingangsdaten	Identifikator eGK Identifikator des PIN-Objektes	
Auslöser	Die Auswahl wird über die Benutzeroberfläche getroffen.	
Nachbedingungen	PIN-Objekt ist aktiviert	
Ausgangsdaten	Statusinformation Anzahl der verbleibenden Versuche	
Bausteine		
Aktivität	Aufrufe	Details
AdV-ACT_52	Version der eGK prüfen	G2 und höher
TI-Plattformoperation	I_KV_Card_Unlocking::enable_PIN	

Funktionale Ergänzungen

Das Objektsystem der eGK steuert, für welche PIN-Objekte der Anwendungsfall durchgeführt werden kann. Auf einer eGK G2 können die PIN-Objekte MRPIN.NFD und MRPIN.DPE aktiviert werden. Ab einer eGK G2.1 ist der Anwendungsfall auch mit der MRPIN.AMTS durchführbar.

Die Funktionalität der Aktivierung von PIN-Objekten wird in ORS2.1 als Plattformleistung der Basis-TI zur Verfügung gestellt.

3.6.2.4 PIN für Fachanwendung ausschalten

Um die Anzahl der PIN-Eingaben pro Kartensteckzyklus zu minimieren, kann der Versicherte für bestimmte Fachanwendungen die Multireferenz-PIN für diese Fachanwendung deaktivieren. Der Versicherte wird dafür zur Eingabe seiner PIN am Kartenterminal aufgefordert. Zuvor muss der Versicherte darauf hingewiesen werden, dass mit dem Ausschalten der PIN für diese Fachanwendung, zusätzliche PIN-Eingaben, die einem höheren Schutz der Daten dienen, entfallen.

AdV-A_2545 - Hinweis auf geringeren Schutz der Daten bei deaktivierter PIN
Die Fachanwendung AdV MUSS den Versicherten über die Benutzeroberfläche darüber informieren, dass das Ausschalten einer PIN den Schutz der Daten, zugunsten eines höheren Bedienungskomforts, verringert**. [<=]**

AdV-A_2043 - Anwendungsfall AdV-UC_04: PIN für Fachanwendung ausschalten
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_04: „PIN für Fachanwendung ausschalten“ abbilden.**[<=]**

Tabelle 13: TAB_ADV_013 Anwendungsfall AdV-UC_04

ID	AdV-UC_04	
Name	PIN für Fachanwendung ausschalten	
Kurzbeschreibung	Der Versicherte deaktiviert die PIN für eine Fachanwendung auf der eGK.	
Initiierender Akteur	Versicherter über AdV-Umgebung	
AdV-Umgebung	KTR-AdV-Umgebung, @home	
Vorbedingungen	PIN-Objekt ist aktiviert. Versicherte wurde auf verringerten Schutz der Daten hingewiesen.	
Eingangsdaten	Identifikator eGK Identifikator des PIN-Objektes	
Auslöser	Die Auswahl wird über die Benutzeroberfläche getroffen.	
Nachbedingungen	PIN-Objekt ist deaktiviert.	
Ausgangsdaten	Statusinformation	
Bausteine		
Aktivität	Aufrufe	Details
AdV-ACT_52	Version der eGK prüfen	G2 und höher

TI-Plattformoperation	I_KV_Card_Unlocking::disable_PIN	

Funktionale Ergänzungen

Das Objektsystem der eGK steuert, für welche PIN-Objekte der Anwendungsfall durchgeführt werden kann. Auf einer eGK G2 können die PIN-Objekte MRPIN.NFD und MRPIN.DPE deaktiviert werden. Ab einer eGK G2.1 ist der Anwendungsfall auch mit der MRPIN.AMTS durchführbar.

Die Funktionalität der Deaktivierung von PIN-Objekten wird in ORS2.1 als Plattformleistung der Basis-TI zur Verfügung gestellt.

3.6.3 Übergreifende Funktionen

3.6.3.1 Echtheit und Gültigkeit der eGK prüfen

Mit diesem Anwendungsfall werden die Echtheit und die technische Nutzbarkeit der eGK geprüft. Die Authentizität und Echtheit der eGK wird durch ein Card-to-Card mit der SM-B geprüft. Die eGK ist gültig, wenn der HCA-Ordner der eGK aktiv (nicht gesperrt) und das AUT-Zertifikat der eGK gültig ist.

AdV-A_2044 - Anwendungsfall AdV-UC_23: Echtheit und Gültigkeit der eGK prüfen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_23: „Echtheit und Gültigkeit der eGK prüfen“ abbilden.**[<=]**

Tabelle 14: TAB_ADV_014 Anwendungsfall AdV-UC_23

ID	AdV-UC_23	
Name	Echtheit und Gültigkeit der eGK prüfen	
Kurzbeschreibung	Der Anwendungsfall prüft die Echtheit und die Gültigkeit der eGK. Es wird geprüft, ob das AUT-Zertifikat bzw. das AUTN-Zertifikat im DF.ESIGN gesperrt oder abgelaufen ist und ob DF.HCA (Health Care Application) der eGK gesperrt ist.	
Initiierender Akteur	Versicherter über AdV-Umgebung	
AdV-Umgebung	KTR-AdV-Umgebung, @home	
Vorbedingungen	Keine	
Eingangsdaten	Identifikator eGK	
Auslöser	Die Auswahl wird über die Benutzeroberfläche getroffen.	
Nachbedingungen	Keine	

Ausgangsdaten	Status der eGK	
Bausteine		
ID	Aktivität	Details
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	
AdV-ACT_51	Gültigkeit der eGK prüfen	

3.6.3.2 Mit eGK verschlüsseln

In diesem Anwendungsfall kann der Versicherte ein Dokument mit dem öffentlichen Schlüssel seiner eGK verschlüsseln. Dabei soll ein hybrides Verschlüsselungsverfahren verwendet werden, in welchem das eigentliche Dokument aus Performancegründen mit einem symmetrischen Schlüssel verschlüsselt und der verwendete Schlüssel anschließend im asymmetrischen Verfahren mit dem öffentlichen Schlüssel eines auf der eGK vorhandenen Zertifikats verschlüsselt.

AdV-A_2045 - Anwendungsfall AdV-UC_25: Mit eGK verschlüsseln
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_25: „Mit eGK verschlüsseln“ abbilden.**[**<=**]**

Tabelle 15: TAB_ADV_015 Anwendungsfall AdV-UC_25

ID	AdV-UC_25	
Name	Mit eGK verschlüsseln	
Kurzbeschreibung	Der Anwendungsfall verschlüsselt ein Dokument.	
Initiierender Akteur	Versicherter über AdV-Umgebung	
AdV-Umgebung	KTR-AdV-Umgebung, @home	
Vorbedingungen	Keine	
Eingangsdaten	Identifikator eGK Identifikator des öffentlichen Schlüssels (C.ENC) Dokument	
Auslöser	Am KTR-AdV-Terminal oder @home wird die Operation „encrypt“ der Schnittstelle „I_Certificate“ aufgerufen.	
Nachbedingungen	Status und Ergebnis der Verschlüsselung liegen vor	

Ausgangsdaten	Verschlüsseltes Dokument und verschlüsselter symmetrischer Schlüssel	
Bausteine		
ID	Aktivität	Details
TI-Plattformoperation	I_Crypt_Operations::encrypt_Document gemäß [gemKPT_Arch_TIP]	

3.6.3.3 Mit eGK entschlüsseln

Mit diesem Anwendungsfall kann ein konform zum Anwendungsfall AdV-UC_25 verschlüsseltes Dokument entschlüsselt werden. Hierzu wird der zur Verschlüsselung verwendete symmetrische Schlüssel mit dem privaten Schlüssel der eGK entschlüsselt und anschließend das Dokument mit dem symmetrischen Schlüssel entschlüsselt.

AdV-A_2046 - Anwendungsfall AdV-UC_26: Mit eGK entschlüsseln
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_26: „Mit eGK entschlüsseln“ abbilden.**[<=]**

Tabelle 16: TAB_ADV_016 Anwendungsfall AdV-UC_26

ID	AdV-UC_26	
Name	Mit eGK entschlüsseln	
Kurzbeschreibung	Der Anwendungsfall entschlüsselt das übergebene Dokument unter Verwendung des referenzierten privaten Schlüssels der eGK.	
Initiierender Akteur	Versicherter über AdV-Umgebung	
AdV-Umgebung	KTR-AdV-Umgebung, @home	
Vorbedingungen	Das Dokument wurde mit Schlüsselmaterial der eGK verschlüsselt.	
Eingangsdaten	Identifikator eGK Identifikator des privaten Schlüssels (C.ENC) Verschlüsseltes Dokument mit verschlüsseltem symmetrischen Schlüssel	
Auslöser	Am KTR-AdV-Terminal oder @home wird die Operation „decrypt“ der Schnittstelle „I_Certificate“ aufgerufen.	
Nachbedingungen	Status und Ergebnis der Entschlüsselung liegen vor	

Ausgangsdaten	Entschlüsseltes Dokument	
Bausteine		
ID	Aktivität	Details
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	PIN.CH
TI-Plattformoperation	I_Crypt_Operations::decrypt_Document gemäß [gemKPT_Arch_TIP]	

3.6.3.4 Benutzerauthentifizierung mit eGK

Die Benutzerauthentifikation mit der eGK stellt Funktionen zur Verfügung, um Versicherte gegenüber Diensten oder Portalen zu authentifizieren. Versicherte werden dabei direkt über die eGK authentisiert.

Im technischen Ablauf der Benutzerauthentifizierung gegenüber einem Dienst oder Portal wird auf einem Authentisierungsrequest eine Signatur zwecks Authentisierung erstellt. Mit diesem Anwendungsfall kann der Versicherte einen Authentisierungsrequest mit dem privaten AUT-Schlüssel oder AUTN-Schlüssel seiner eGK signieren.

AdV-A_2047 - Anwendungsfall AdV-UC_27: Authentisierungsrequest mit eGK signieren
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_27: „Authentisierungsrequest mit eGK signieren“ abbilden.**[**<=**]**

Tabelle 17: TAB_ADV_017 Anwendungsfall AdV-UC_27

ID	AdV-UC_27	
Name	Authentisierungsrequest mit eGK signieren	
Kurzbeschreibung	Der Anwendungsfall signiert den übergebenen Hash-Wert unter Verwendung des referenzierten privaten Schlüssels der eGK.	
Initiierender Akteur	Versicherter in der AdV-Umgebung	
AdV-Umgebung	KTR-AdV-Umgebung, @home	
Vorbedingungen	In einem Authentisierungsprozess wurde ein Hash-Wert übergeben.	
Eingangsdaten	Identifikator eGK Identifikator des privaten Schlüssels (ID.CH.AUT, ID.CH.AUTN) Zu signierender Hash-Wert	

Auslöser	Am AdV-Terminal wird die Operation „authenticate“ der Schnittstelle „I_Certificate“ aufgerufen.	
Nachbedingungen	Status und Ergebnis des Signaturvorganges liegen vor.	
Ausgangsdaten	Signierter Hash-Wert	
Bausteine		
ID	Aktivität	Details
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	PIN.CH
TI-Plattformoperation	I_Sign_Operations::sign_Data gemäß [gemKPT_Arch_TIP]	

3.6.3.5 Zertifikat von eGK lesen

Mit diesem Anwendungsfall kann der Versicherte das ENC bzw. ENCV-Zertifikat der eGK auslesen. Das exportierte Zertifikat kann bspw. in einer externen Verschlüsselungssoftware genutzt werden.

Zukunftsthema: Falls eine eGK über ein qualifiziertes Signaturzertifikat C.QES (oder ggf. weitere Attributzertifikate) verfügt, können Attributzertifikaten ausgelesen werden, um eine anwendungsfallbezogene Auswahl unter diesen Attributzertifikaten vorzunehmen, die beim Signieren von Dokumenten mitgegeben werden, je nachdem, welche Attributzertifikate für das zu signierende Dokument passend sind.

AdV-A_2048 - Anwendungsfall AdV-UC_24: Zertifikat von eGK lesen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_24: „Zertifikat von eGK lesen“ abbilden.**[<=]**

Tabelle 18: TAB_ADV_018 Anwendungsfall AdV-UC_24

ID	AdV-UC_24	
Name	Zertifikat von eGK lesen	
Kurzbeschreibung	Der Anwendungsfall liest ein Zertifikat von der eGK des Versicherten.	
Initiierender Akteur	Versicherter über AdV-Umgebung	
AdV-Umgebung	KTR-AdV-Umgebung, @home	
Vorbedingungen	Keine	
Eingangsdaten	Identifikator eGK C.ENC oder C.ENCV als Identifikator des Zertifikats	

Auslöser	Die Auswahl wird über die Benutzeroberfläche getroffen.	
Nachbedingungen	Keine	
Ausgangsdaten	Zertifikat der eGK	
Bausteine		
ID	Aktivität	Details
TI-Plattformoperation	I_Sign_Operations::get_Certificate	

3.6.3.6 Datenübertragung bei Kartentausch

Mit diesem Anwendungsfall kann der Versicherte bei Austausch seiner eGK die Daten der medizinischen Fachanwendungen von der alten auf die neue eGK übertragen.

AdV-A_2071 - Anwendungsfall AdV-UC_28: Datenübertragung bei Kartentausch
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_28: „Datenübertragung bei Kartentausch“ abbilden.**[<=]**

Tabelle 19: TAB_ADV_057 Anwendungsfall AdV-UC_28

ID	AdV-UC_28
Name	Datenübertragung bei Kartentausch
Kurzbeschreibung	Die Daten und ggfs. die Einwilligungsdaten der medizinischen Fachanwendungen werden von der alten eGK auf die neue eGK des Versicherten übertragen. Dazu wählt der Versicherte diejenigen Fachanwendungen aus, deren Daten übertragen werden sollen
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_16 Daten von eGK zu eGK kopieren Parameter: eGK Identifier und „FA_DPE”

3.6.4 Einwilligungen und Verweise

Die in diesem Abschnitt dargestellten Anwendungsfälle von GDD sind für die Verwendung auf der eGK noch nicht abschließend spezifiziert. Daher erfolgt eine Umsetzung in den Produkttypen der AdV im aktuellen Stand nicht.

NFDM und eMP/AMTS speichern Informationen zur Einwilligung des Versicherten in die Nutzung dieser Fachanwendung in ihren Anwendungs-Ordnern (z. B. DF.AMTS/EF.EinwilligungAMTS). Das Verwalten von Einwilligungen dieser

Fachanwendungen sind fachanwendungsspezifische Anwendungsfälle (vgl. 3.7.2, 3.7.3 und 4).

Darüber hinaus können auf der eGK Informationen zur Einwilligung in die Nutzung in weitere freiwillige Anwendungen gespeichert werden. Die Daten zu den weiteren freiwilligen Anwendungen sind nicht auf der eGK abgelegt. Die Einwilligungseinträge dokumentieren, dass der Versicherte die Einwilligung erklärt hat.

Informationen über die Speicherorte der Daten der freiwilligen Anwendungen, die nicht auf der eGK gespeichert werden, sind in EF.Verweis abgelegt.

Auf der eGK können in EF.Einwilligung zehn Einwilligungen in weitere freiwillige Anwendungen gespeichert werden. Mit diesen Einträgen in EF.Einwilligung korrespondieren zehn Verweise für diese Anwendungen in EF.Verweis. Die Anwendungsfälle zum Verwalten der Einwilligungen betrachten die Einwilligungen und die korrespondierenden Verweise gemeinsam.

3.6.4.1 Einwilligungen und Verweise von der eGK lesen

Mit diesem Anwendungsfall werden dem Versicherten die auf der eGK in der Datei EF.Einwilligung gespeicherten Einwilligungen sowie die zugehörigen Verweise aus EF.Verweis angezeigt (siehe Kapitel 6.2.2).

AdV-A_2049 - Anwendungsfall AdV-UC_30: EF.Einwilligung von eGK lesen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_30: „EF.Einwilligung von eGK lesen“ abbilden.
[<=]

Tabelle 20: TAB_ADV_019 Anwendungsfall AdV-UC_30

ID	AdV-UC_30
Name	EF.Einwilligung von eGK lesen
Kurzbeschreibung	Das Fachmodul AdV bzw. die AdV-App liest alle Einträge aus EF.Einwilligung und die korrespondierenden Einträge aus EF.Verweis von der eGK des Versicherten.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_11 Daten von eGK lesen Parameter: eGK Identifier, „FA_CON“

Tabelle 21: TAB_ADV_020 Konfiguration AdV-UC_30

ID	Aktivität	Parameter
	Parameter aus Informationsmodell bestimmen	Dateien EF.Einwilligung, EF.Verweis SM-B

AdV-ACT_51	Gültigkeit der eGK prüfen	
AdV-ACT_52	Version der eGK prüfen	G2 und höher
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	eGK, SM-B
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	PIN.CH
AdV-ACT_55	Daten lesen	EF.Einwilligung
AdV-ACT_55	Daten lesen	EF.Verweis

3.6.4.2 Verweis auf der eGK schreiben

Es wird der Verweis für eine freiwillige Anwendung auf die eGK geschrieben.

AdV-A_2050 - Anwendungsfall AdV-UC_32: EF.Verweis auf eGK schreiben
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_32: „EF.Verweis auf eGK schreiben“ abbilden.
[<=]

Tabelle 22: TAB_ADV_021 Anwendungsfall AdV-UC_32

ID	AdV-UC_32
Name	EF.Verweis auf eGK schreiben
Kurzbeschreibung	Das Fachmodul AdV bzw. die AdV-App schreibt einen Eintrag in EF.Verweis auf der eGK des Versicherten.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	Basis-Anwendungsfall AdV-UC_12 Daten auf eGK schreiben Parameter: eGK Identifier, „FA_CON“, Identifier des Records, Daten für EF.Verweis

Tabelle 23: TAB_ADV_022 Konfiguration AdV-UC_32

ID	Aktivität	Parameter
	Parameter aus Informationsmodell bestimmen	Datei EF.Verweis SM-B
AdV-ACT_51	Gültigkeit der eGK prüfen	

AdV-ACT_52	Version der eGK prüfen	G2 und höher
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	eGK, SM-B
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	PIN.CH
AdV-ACT_56	Daten schreiben	EF.Verweis

3.6.4.3 Einwilligung und Verweis auf der eGK löschen

Mit diesem Anwendungsfall kann der Versicherte eine auf der eGK in der Datei EF.Einwilligung gespeicherte Einwilligung in eine weitere freiwillige Anwendung löschen.

Jede Einwilligung in eine weitere freiwillige Anwendung muss einzeln gelöscht werden. Dabei muss auch der korrespondierende Verweis in EF.Verweis gelöscht werden.

AdV-A_2051 - Anwendungsfall AdV-UC_31: EF.Einwilligung auf eGK löschen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_31: „EF.Einwilligung auf eGK löschen“ abbilden.
[<=]

Tabelle 24: TAB_ADV_023 Anwendungsfall AdV-UC_31

ID	AdV-UC_31
Name	EF.Einwilligung auf eGK löschen
Kurzbeschreibung	Das Fachmodul AdV bzw. die AdV-App löscht einen Eintrag in EF.Einwilligung sowie den zugehörigen Eintrag in EF.Verweis auf der eGK des Versicherten.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_13 Daten von eGK löschen Parameter: eGK Identifier, „FA_CON“, Identifier des Records

Tabelle 25: TAB_ADV_024 Konfiguration AdV-UC_31

ID	Aktivität	Parameter
	Parameter aus Informationsmodell bestimmen	Dateien EF.Einwilligung, EF.Verweis SM-B
AdV-ACT_51	Gültigkeit der eGK prüfen	

AdV-ACT_52	Version der eGK prüfen	G2 und höher
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	eGK, SM-B
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	PIN.CH
AdV-ACT_57	Daten löschen	EF.Einwilligung
AdV-ACT_56	Daten schreiben	EF.Verweis

3.7 Fachanwendungsspezifische Anwendungsfälle

Fachanwendungen müssen für die von ihnen verantworteten Daten eine fachliche Konzeption und technische Umsetzung für die erweiterten Verfahren und Lösungen zur Wahrnehmung der Rechte des Versicherten bereitstellen.

Die AdV-Lösungen bieten eine Umgebung für die Umsetzung dieser fachanwendungsspezifischen Anwendungsfälle. Die Fachlichkeit wird durch die Fachanwendungen verantwortet.

AdV-A_2052 - Konfiguration für fachanwendungsspezifischen Anwendungsfälle
Eine Fachanwendung MUSS zur Umsetzung eines fachanwendungsspezifischen Anwendungsfalls die Konfiguration für einen Basis-Anwendungsfall festlegen.
[<=]

Die Basis-Anwendungsfälle bieten die Möglichkeiten, Operationen von Fachmodulen der Fachanwendungen aufzurufen, um den Ablauf des Anwendungsfalls zu steuern (siehe Kapitel 3.5.1.10 Aktivität AdV-ACT_60: Aufruf einer fachanwendungsspezifischen Operation). Hierbei kapselt die Fachanwendung AdV die Aufrufe an die weiteren Fachmodule, in dem der Request des AdV-Clientsystem empfangen, die Ausführung an das zuständige Fachmodul delegiert und anschließend das Ergebnis an das AdV-Clientsystem zurückgegeben wird.

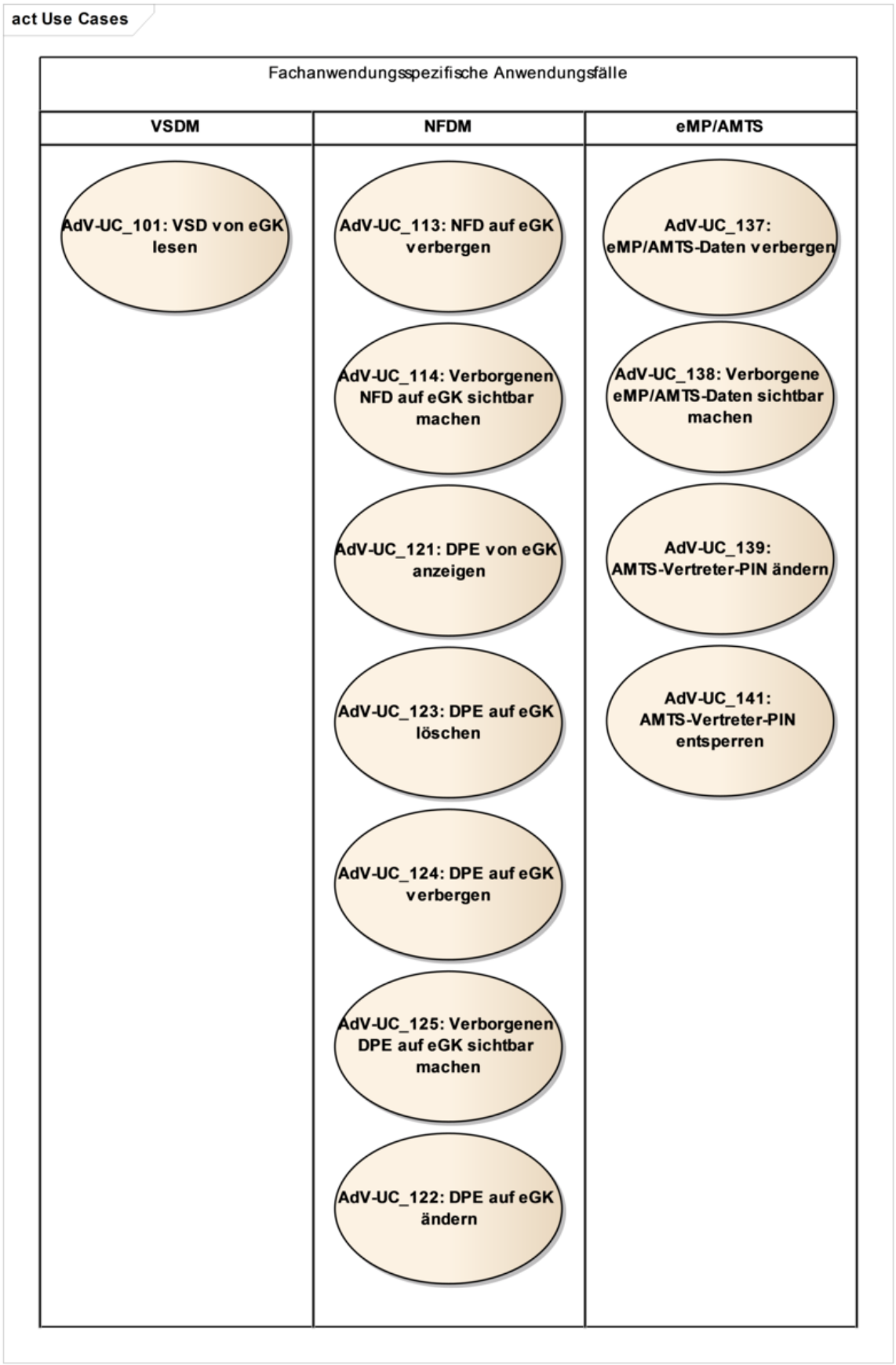

Abbildung 25: Übersicht fachanwendungsspezifische Anwendungsfälle

3.7.1 VSDM

3.7.1.1 Versichertenstammdaten von der eGK lesen

Mit diesem Anwendungsfall werden dem Versicherten die auf der eGK gespeicherten Versichertenstammdaten (VSD) angezeigt. Es wird eine Onlineprüfung und bei Vorhandensein eines Aktualisierungsauftrages ein Update durchgeführt.

Es gelten die übergreifenden Anforderungen der Fachanwendung VSDM aus [gemSysL_VSDM].

AdV-A_2054 - Anwendungsfall AdV-UC_101: VSD von eGK lesen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_101: „VSD von eGK lesen“ abbilden.
[<=]

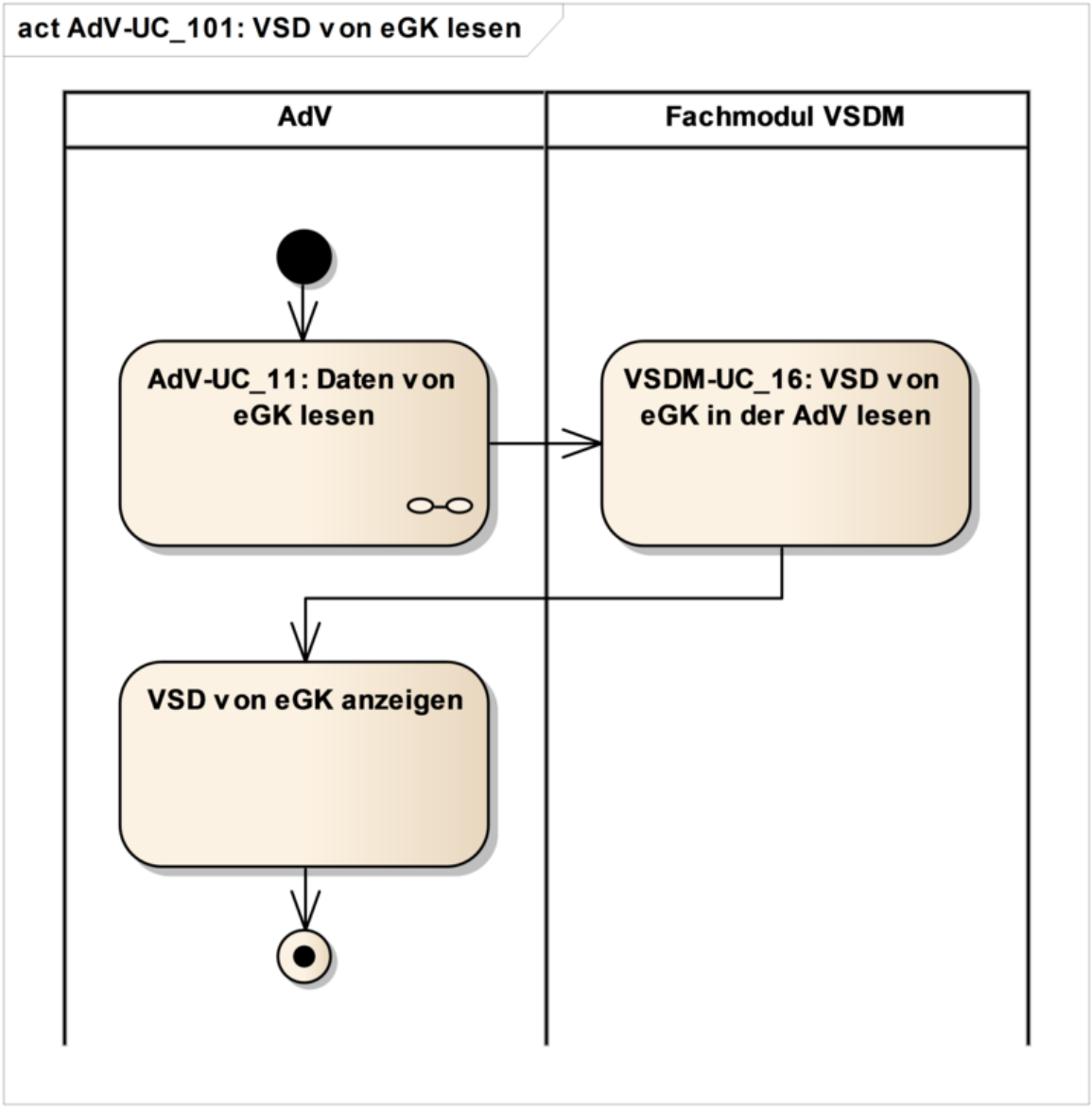

Abbildung 26: Darstellung AdV-UC_101: „VSD von eGK lesen“

Tabelle 26: TAB_ADV_025 Anwendungsfall AdV-UC_101

ID	AdV-UC_101
Name	VSD von eGK anzeigen
Kurzbeschreibung	Lesen der Versichertenstammdaten von der eGK des Versicherten.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_11 Daten von eGK lesen Parameter: eGK Identifier, „FA_VSDM“

Tabelle 27: TAB_ADV_026 Konfiguration AdV-UC_101

ID	Aktivität	Parameter
	Parameter aus Informationsmodell bestimmen	SM-B
AdV-ACT_60	Aufruf einer fachanwendungsspezifischen Operation	I_VSDService.ReadVSDAdV Parameter: Identifier der eGK Identifier der SM-B

Die Operation `I_VSDService.ReadVSDAdV` ist in [gemSysL_VSDM] beschrieben.

3.7.2 NFDM

Die Anwendungsfälle für das Notfalldaten-Management basieren auf der Beschreibung der fachlichen und funktionalen Abläufe in [gemSysL_NFDM].

Wo möglich, werden die in [gemSysL_NFDM] modellierten Leistungsmerkmale genutzt. Für die weiteren Anwendungsfälle werden Konfigurationen für die Basis-Anwendungsfälle der allgemeinen Anwendungsverwaltung (siehe 3.5) beschrieben.

Es gelten die übergreifenden Vorbedingungen für Anwendungsfälle der Leistungsmerkmale aus [gemSysL_NFDM].

Der Datensatz ‚Persönlichen Erklärungen‘ (Erklärung zur Organ- und/oder Gewebespende, Vorsorgevollmacht, Patientenverfügung) wird unabhängig vom Notfalldatensatz behandelt.

AdV-A_2135 - NFD: Hinweis auf verborgene Daten
Die Fachanwendung AdV MUSS dem Versicherten beim Aufruf der Anwendungsfälle zum NFD einen Hinweis anzeigen, wenn die eGK des Versicherten bereits einen verborgenen Notfalldatensatz enthält und den Versicherten darüber informieren, dass der Notfalldatensatz des Versicherten derzeit verborgen ist und somit im Notfall nicht gelesen werden kann.**[**<=**]**

AdV-A_2136 - DPE: Hinweis auf verborgene Daten
Die Fachanwendung AdV MUSS dem Versicherten beim Aufruf der Anwendungsfälle zum DPE einen Hinweis anzeigen, wenn die eGK des Versicherten bereits verborgene persönliche Erklärungen enthält und den Versicherten darüber informieren, dass die persönlichen Erklärungen des Versicherten derzeit verborgen sind und somit im Notfall nicht gelesen werden können.**[<=]**

3.7.2.1 NFD auf eGK verbergen

Mit diesem Anwendungsfall kann der Versicherte den Notfalldatensatz auf seiner eGK verbergen.

AdV-A_2057 - Anwendungsfall AdV-UC_113: NFD auf eGK verbergen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_113: „NFD auf eGK verbergen“ abbilden.**[<=]**

Tabelle 28: TAB_ADV_031 Anwendungsfall AdV-UC_113

ID	AdV-UC_113
Name	NFD auf eGK verbergen
Kurzbeschreibung	Der NFD auf der eGK des Versicherten wird verborgen.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_14 Anwendung deaktivieren Parameter: Identifier eGK, „FA_NFD“

Tabelle 29: TAB_ADV_032 Konfiguration AdV-UC_113

ID	**Aktivität**	
	Parameter aus Informationsmodell bestimmen	Ordner: DF.NFD SM-B
AdV-ACT_51	Gültigkeit der eGK prüfen	Ja
AdV-ACT_52	Version der eGK prüfen	G2 und höher
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	eGK, SM-B
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	abh. von eGK-Kartengeneration
AdV-ACT_58	Applikation deaktivieren	DF.NFD deaktivieren

AdV-ACT_61	Datenzugriff protokollieren	

3.7.2.2 Verborgenen NFD auf eGK sichtbar machen

Mit diesem Anwendungsfall kann der Versicherte den verborgenen Notfalldatensatz auf seiner eGK wieder sichtbar machen.

AdV-A_2058 - Anwendungsfall AdV-UC_114: Verborgenen NFD auf eGK sichtbar machen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_114: „Verborgenen NFD auf eGK sichtbar machen“ abbilden.**[<=]**

Tabelle 30: TAB_ADV_033 Anwendungsfall AdV-UC_114

ID	AdV-UC_114
Name	Verborgenen NFD auf eGK sichtbar machen
Kurzbeschreibung	Der verborgene NFD auf der eGK des Versicherten wird wieder sichtbar gemacht.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_15 Anwendung reaktivieren Parameter: Identifier eGK, „FA_NFD“

Tabelle 31: TAB_ADV_034 Konfiguration AdV-UC_114

ID	Aktivität	Details
	Parameter aus Informationsmodell bestimmen	Ordner: DF.NFD SM-B
AdV-ACT_51	Gültigkeit der eGK prüfen	Ja
AdV-ACT_52	Version der eGK prüfen	G2 und höher
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	eGK, SM-B
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	abh. von eGK-Kartengeneration
AdV-ACT_59	Applikation aktivieren	DF.NFD aktivieren
AdV-ACT_61	Datenzugriff protokollieren	

3.7.2.3 DPE von eGK anzeigen

Mit diesem Anwendungsfall wird dem Versicherten der auf der eGK gespeicherte Datensatz ‚Persönliche Erklärungen' angezeigt.

AdV-A_2059 - Anwendungsfall AdV-UC_121: DPE von eGK anzeigen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_121: „DPE von eGK anzeigen" abbilden.**[<=]**

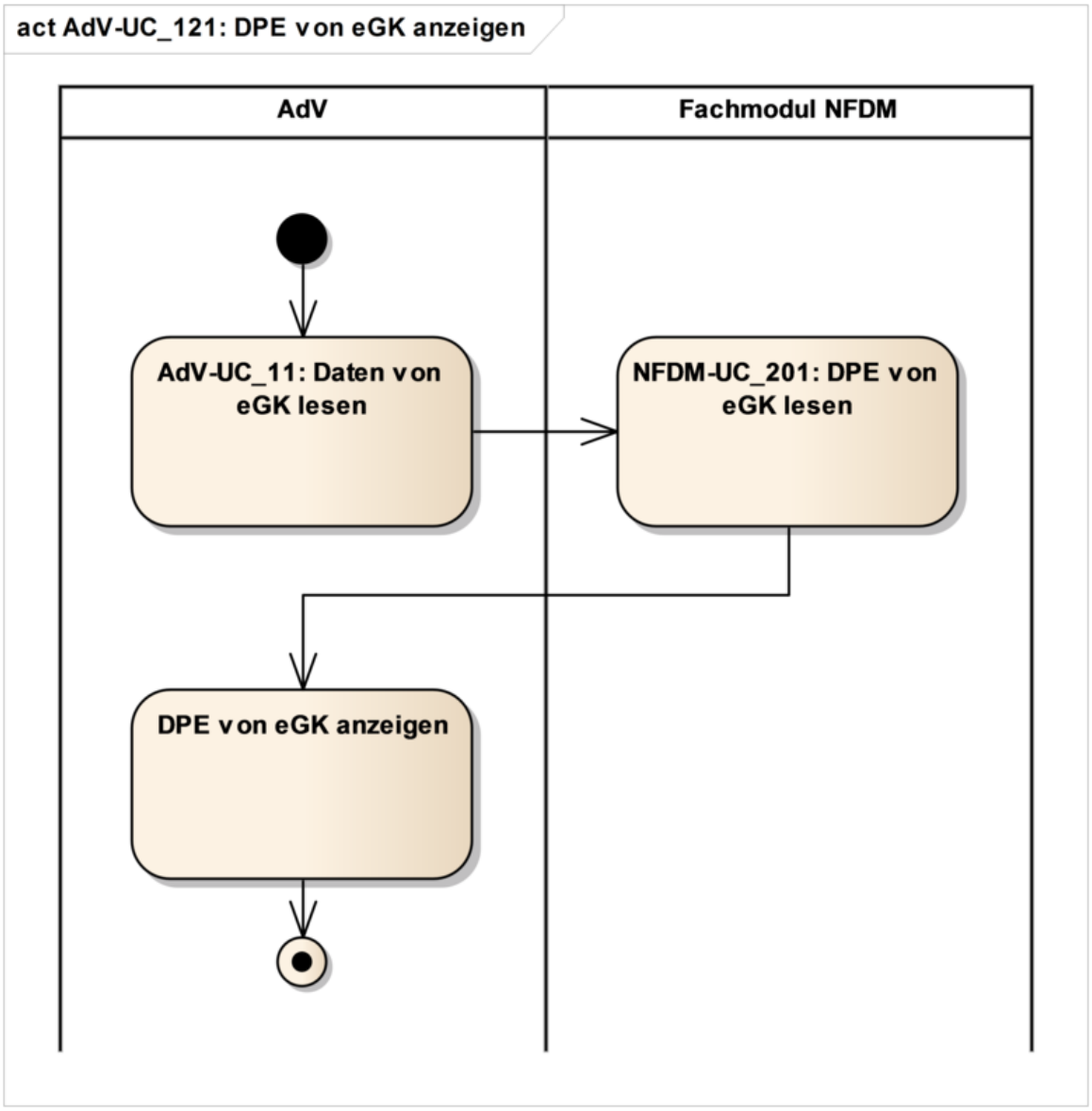

Abbildung 27: Darstellung AdV-UC_121: „DPE von eGK anzeigen"

Tabelle 32: TAB_ADV_035 Anwendungsfall AdV-UC_121

ID	AdV-UC_121
Name	DPE von eGK anzeigen

Kurzbeschreibung	Der DPE wird von der eGK des Versicherten gelesen. Die Daten werden im AdV-Terminal angezeigt.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_11 Daten von eGK lesen Parameter: eGK Identifier, „FA_DPE“

Tabelle 33: TAB_ADV_036 Konfiguration AdV-UC_121

ID	Aktivität	
	Parameter aus Informationsmodell bestimmen	SM-B
AdV-ACT_60	Aufruf einer fachanwendungsspezifischen Operation	I_DPE_Management.ReadDPE Parameter: Notfallindikator = FALSE Aktualisierungsindikator = FALSE Aufrufkontext Identifikator eGK Identifikator SM-B

Die Operation `I_DPE_Management.ReadDPE` ist in [gemSysL_NFDM] beschrieben.

3.7.2.4 DPE auf eGK ändern

Der Versicherte kann mit diesem Anwendungsfall den auf der eGK gespeicherten Datensatz ‚Persönliche Erklärungen‘ ändern. Dafür wird der DPE von der eGK gelesen, dem Versicherten angezeigt und zum Editieren angeboten. Nach dem Editieren wird der geänderte Datensatz auf die eGK geschrieben.

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

AdV-A_2060 - Anwendungsfall AdV-UC_122: DPE auf eGK ändern
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_122: „DPE auf eGK ändern“ abbilden.**[<=]**

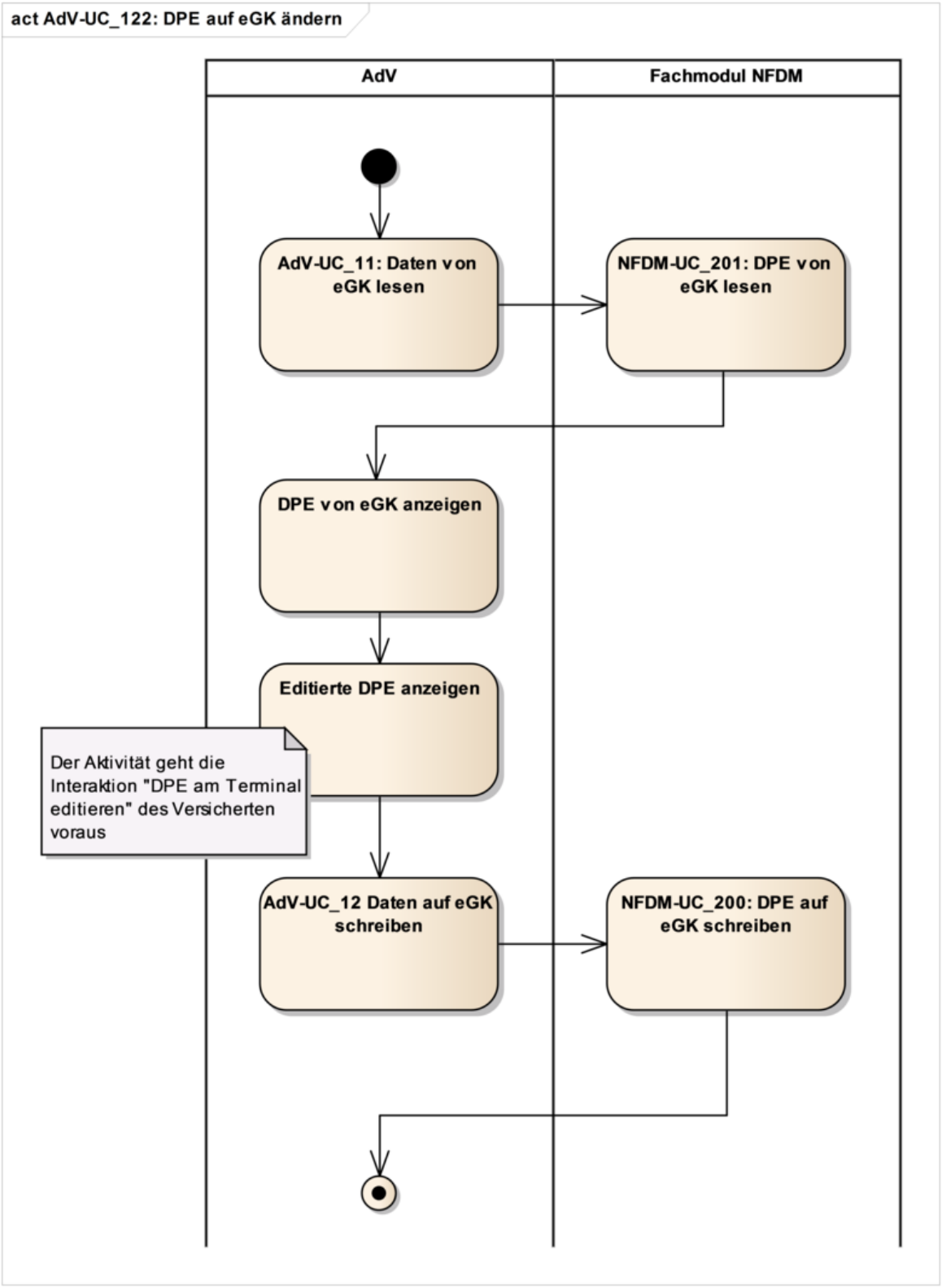

Abbildung 28: Darstellung AdV-UC_122: „DPE auf eGK ändern“

Tabelle 34: TAB_ADV_037 Anwendungsfall AdV-UC_122

ID	AdV-UC_122
Name	DPE auf eGK ändern
Kurzbeschreibung	Der DPE wird von der eGK gelesen und dem Versicherten im AdV-Terminal angezeigt. Nach einer Änderung des DPE durch den Versicherten wird der DPE auf dessen eGK geschrieben.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_11 Daten von eGK lesen Parameter: eGK Identifier, „FA_DPE“ und AdV-UC_12 Daten auf eGK schreiben Parameter: eGK Identifier, „FA_DPE“, DPE

Tabelle 35: TAB_ADV_096 Konfiguration AdV-UC_122 - AdV-UC_11

ID	Aktivität	
	Parameter aus Informationsmodell bestimmen	SM-B
AdV-ACT_60	Aufruf einer fachanwendungsspezifischen Operation	I_DPE_Management.ReadDPE Parameter: Notfallindikator = FALSE Aktualisierungsindikator = TRUE Aufrufkontext Identifikator eGK Identifikator SM-B

Tabelle 36: TAB_ADV_038 Konfiguration AdV-UC_122 - AdV-UC_12

ID	Aktivität	
	Parameter aus Informationsmodell bestimmen	SM-B

AdV-ACT_60	Aufruf einer fachanwendungsspezifischen Operation	I_DPE_Management.WriteDPE Parameter: DPE Aufrufkontext Identifikator eGK Identifikator SM-B

Die Operationen `I_DPE_Management.ReadDPE` und `I_DPE_Management.WriteDPE` sind in [gemSysL_NFDM] beschrieben.

3.7.2.5 DPE auf eGK löschen

Mit diesem Anwendungsfall kann der Versicherteden auf der eGK gespeicherten Datensatz ‚Persönliche Erklärungen' löschen.

AdV-A_2061 - Anwendungsfall AdV-UC_123: DPE auf eGK löschen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_123: „DPE auf eGK löschen" abbilden.**[<=]**

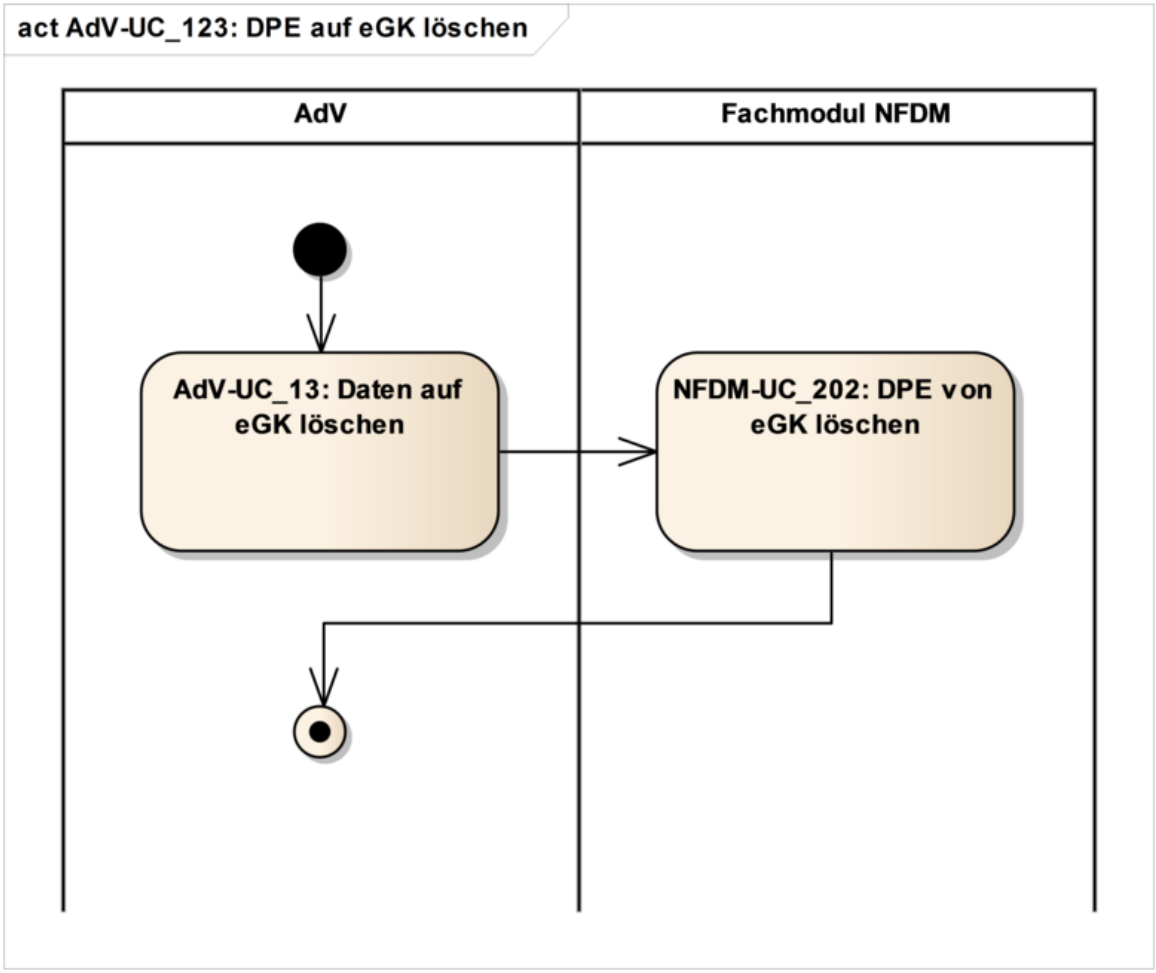

Abbildung 29: Darstellung AdV-UC_123: „DPE auf eGK löschen"

Tabelle 37: TAB_ADV_039 Anwendungsfall AdV-UC_123

ID	AdV-UC_123
Name	DPE auf eGK löschen
Kurzbeschreibung	Der DPE des Versicherten wird von dessen eGK gelöscht.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_13 Daten auf eGK löschen Parameter: eGK Identifier, „FA_DPE“

Tabelle 38: TAB_ADV_040 Konfiguration AdV-UC_123

ID	Aktivität	
	Parameter aus Informationsmodell bestimmen	SM-B
AdV-ACT_60	Aufruf einer fachanwendungsspezifischen Operation	I_DPE_Management.EraseDPE Parameter: Aufrufkontext Identifikator eGK Identifikator SM-B

Die Operation `I_DPE_Management.EraseDPE` ist in [gemSysL_NFDM] beschrieben.

3.7.2.6 DPE auf eGK verbergen

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

AdV-A_2062 - Anwendungsfall AdV-UC_124: DPE auf eGK verbergen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_124: „DPE auf eGK verbergen“ abbilden.**[<=]**

Tabelle 39: TAB_ADV_041 Anwendungsfall AdV-UC_124

ID	AdV-UC_124
Name	DPE auf eGK verbergen
Kurzbeschreibung	Der DPE auf der eGK des Versicherten wird verborgen.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_14 Anwendung deaktivieren Parameter: Identifier eGK, „FA_DPE“

Tabelle 40: TAB_ADV_042 Konfiguration AdV-UC_124

ID	Aktivität	Details
	Parameter aus Informationsmodell bestimmen	Ordner: DF.DPE SM-B
AdV-ACT_51	Gültigkeit der eGK prüfen	
AdV-ACT_52	Version der eGK prüfen	G2 und höher
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	eGK, SM-B
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	abh. von eGK-Kartengeneration
AdV-ACT_58	Applikation deaktivieren	DF.DPE deaktivieren
AdV-ACT_61	Datenzugriff protokollieren	

3.7.2.7 Verborgenen DPE auf eGK sichtbar machen

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

AdV-A_2063 - Anwendungsfall AdV-UC_125: Verborgenen DPE auf eGK sichtbar machen

Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_125: „Verborgenen DPE auf eGK sichtbar machen" abbilden.**[<=]**

Tabelle 41: TAB_ADV_043 Anwendungsfall AdV-UC_125

ID	AdV-UC_125
Name	Verborgenen DPE auf eGK sichtbar machen
Kurzbeschreibung	Der verborgene DPE auf der eGK des Versicherten wird wieder sichtbar gemacht.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_15 Anwendung reaktivieren Parameter: Identifier eGK, „FA_DPE"

Tabelle 42: TAB_ADV_044 Konfiguration AdV-UC_125

ID	Aktivität	Details
	Parameter aus Informationsmodell bestimmen	Ordner: DF.DPE SM-B
AdV-ACT_51	Gültigkeit der eGK prüfen	
AdV-ACT_52	Version der eGK prüfen	G2 und höher
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	eGK, SM-B
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	abh. von eGK-Kartengeneration
AdV-ACT_59	Applikation aktivieren	DF.DPE aktivieren
AdV-ACT_61	Datenzugriff protokollieren	

3.7.3 eMP/AMTS

Die Anwendungsfälle für das eMP/AMTS-Management basieren auf der Beschreibung der fachlichen und funktionalen Abläufe in [gemSysL_AMTS_A].

Wo möglich werden die in [gemSysL_AMTS_A] modellierten Leistungsmerkmale genutzt. Für die weiteren Anwendungsfälle werden Konfigurationen für die Basis-Anwendungsfälle der allgemeinen Anwendungsverwaltung (siehe 3.5) beschrieben.

Es gelten die übergreifenden Vorbedingungen für Anwendungsfälle der Leistungsmerkmale aus [gemSysL_AMTS_A].

AdV-A_2160 - Hinweis beim Deaktivieren der AMTS-PIN
Die Fachanwendung AdV MUSS sicherstellen, dass dem Versicherten vor dem Deaktivieren der AMTS-PIN der explizite Hinweis gegeben wird, dass unberechtigte Dritte bei abgeschalteter PIN Zugriff auf die eMP/AMTS-Daten in einer Leistungserbringer-Umgebung erlangen können.**[<=]**

3.7.3.1 eMP/AMTS-Datensatz auf eGK verbergen

Mit diesem Anwendungsfall kann der Versicherte die Daten der Anwendung eMP/AMTS auf seiner eGK verbergen.

AdV-A_2067 - Anwendungsfall AdV-UC_137: eMP/AMTS auf eGK verbergen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_137: „eMP/AMTS auf eGK verbergen“ abbilden.**[<=]**

Tabelle 43: TAB_ADV_051 Anwendungsfall: AdV-UC_137

ID	AdV-UC_137
Name	eMP/AMTS auf eGK verbergen
Kurzbeschreibung	Das Fachmodul AdV verbirgt die eMP/AMTS-Daten auf der eGK des Versicherten.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_14 Anwendung deaktivieren Parameter: Identifier eGK, „FA_AMTS“

Tabelle 44: TAB_ADV_052 Konfiguration AdV-UC_137

ID	Aktivität	
	Parameter aus Informationsmodell bestimmen	Ordner: DF.AMTS SM-B
AdV-ACT_51	Gültigkeit der eGK prüfen	
AdV-ACT_52	Version der eGK prüfen	G2 und höher
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	eGK, SM-B
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	abh. von eGK-Kartengeneration
AdV-ACT_58	Applikation deaktivieren	DF.AMTS deaktivieren
AdV-ACT_61	Datenzugriff protokollieren	

3.7.3.2 Verborgenen eMP/AMTS-Datensatz auf eGK sichtbar machen

Mit diesem Anwendungsfall kann der Versicherte die verborgenen Daten der Anwendung eMP/AMTS auf seiner eGK wieder sichtbar machen.

AdV-A_2068 - Anwendungsfall AdV-UC_138: Verborgenen eMP/AMTS-Datensatz auf eGK sichtbar machen
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_138: „Verborgenen eMP/AMTS-Datensatz auf eGK sichtbar machen“ abbilden.**[**<=**]**

Tabelle 45: TAB_ADV_053 Anwendungsfall AdV-UC_138

ID	AdV-UC_138
Name	Verborgenen eMP/AMTS-Datensatz sichtbar machen
Kurzbeschreibung	Das Fachmodul AdV macht die verborgenen eMP/AMTS-Daten auf der eGK des Versicherten wieder sichtbar.
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Basis-Anwendungsfall	AdV-UC_15 Anwendung reaktivieren Parameter: Identifier eGK, „FA_AMTS“

Tabelle 46: TAB_ADV_054 Konfiguration AdV-UC_138

ID	**Aktivität**	
	Parameter aus Informationsmodell bestimmen	Ordner: DF.AMTS SM-B
AdV-ACT_51	Gültigkeit der eGK prüfen	
AdV-ACT_52	Version der eGK prüfen	G2 und höher
AdV-ACT_53	Echtheit der beteiligten Karten durch C2C prüfen	eGK, SM-B
AdV-ACT_54	Authentifizierung des Versicherten mittels PIN-Verifikation einholen	abh. von eGK-Kartengeneration
AdV-ACT_59	Applikation aktivieren	DF.AMTS aktivieren
AdV-ACT_61	Datenzugriff protokollieren	

3.7.3.3 AMTS-Vertreter-PIN auf der eGK ändern

Mit diesem Anwendungsfall kann der Versicherte die Vertreter-PIN für die Anwendung eMP/AMTS auf seiner eGK ändern. Für eine Änderungserlaubnis wird der Versicherte zur Eingabe der Versicherten-PIN aufgefordert.

AdV-A_2069 - Anwendungsfall AdV-UC_139: AMTS-Vertreter-PIN auf der eGK ändern

Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_139: „AMTS-Vertreter-PIN auf der eGK ändern“ abbilden.**[<=]**

Tabelle 47: TAB_ADV_055 Anwendungsfall AdV-UC_139

ID	AdV-UC_139
Name	AMTS-Vertreter-PIN ändern
Kurzbeschreibung	Änderung der Vertreter-PIN AMTS auf der eGK
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Anwendungsfall	AdV-UC_01 PIN ändern Parameter: Identifier eGK, PIN.AMTS_REP

3.7.3.4 AMTS-Vertreter-PIN auf der eGK entsperren

Mit diesem Anwendungsfall kann der Versicherte die Vertreter-PIN für die Anwendung eMP/AMTS auf seiner eGK entsperren. Für eine Entsperrerlaubnis wird der Versicherte zur Eingabe der Versicherten-PIN aufgefordert.

AdV-A_2070 - Anwendungsfall AdV-UC_141: AMTS-Vertreter-PIN auf der eGK entsperren
Die Fachanwendung AdV MUSS den Anwendungsfall AdV-UC_141: „AMTS-Vertreter-PIN auf der eGK entsperren“ abbilden.**[<=]**

Tabelle 48: TAB_ADV_056 Anwendungsfall AdV-UC_141

ID	AdV-UC_141
Name	AMTS-Vertreter-PIN entsperren
Kurzbeschreibung	Entsperren der Vertreter-PIN AMTS auf der eGK
AdV-Umgebung	KTR-AdV-Umgebung, @home
Umsetzung durch Anwendungsfall	AdV-UC_02 PIN auf eGK entsperren Parameter: Identifier eGK, PIN.AMTS_REP

4 Externe Schnittstellen

Die externen Schnittstellen sind im Kapitel 2.2 deklariert worden. Nachfolgend werden die Operationen der externen Schnittstellen definiert. Von der AdV werden Clientsystemem folgende Interfaces angeboten:

- Zertifikats-Nutzung. Über diese Schnittstelle kann der Versicherte auf Zertifikate seiner eGK zugreifen, etwa um die öffentliche Zertifikate auszulesen, oder um eine Online-Gültigkeitsprüfung durchzuführen. Die Funktionen für das Ver- und Entschlüsselns sowie das Signieren können genutzt werden.

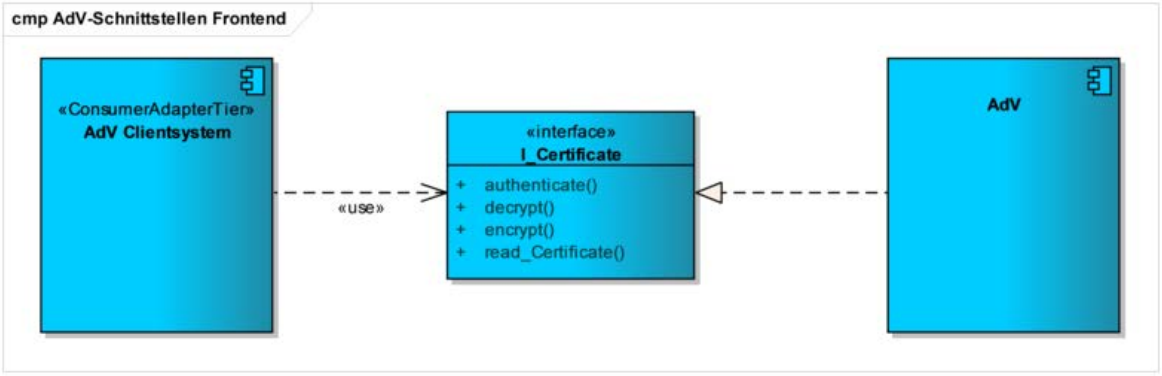

Abbildung 30: Schnittstellen zwischen AdV-Terminal und Fachmodul AdV

Die Anwendungsfälle zum Management von Anwendungen, dem PIN-Management und der Fachanwendungen werden über die von der AdV angebotene graphische Benutzeroberfläche ausgelöst. Für sie wird keine externe Schnittstelle angeboten.

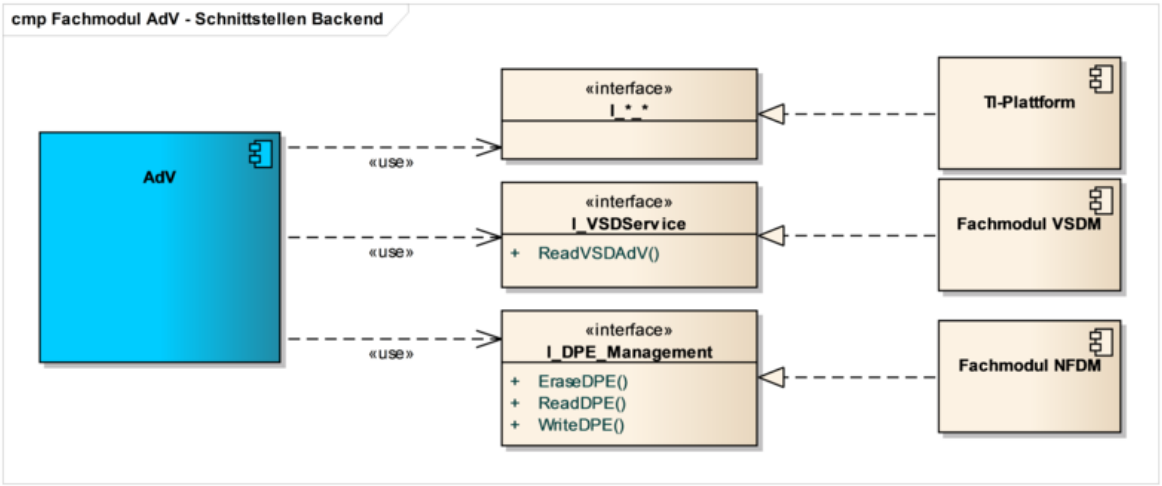

Abbildung 31: Schnittstellen zwischen Fachmodul AdV und Backend-Komponenten

Funktionalitäten, die nicht über einen Aufruf von Schnittstellen der fachanwendungsspezifischen Fachmodule realisiert werden können, werden vom AdV mit Hilfe von TIP Operationen umgesetzt.

4.1 Zertifikatsverwaltung

Das Interface `I_Certificate` stellt Operationen bereit, die Anwendungsfälle zur Nutzung der Zertifikate-Objekte auf der eGK initiieren

4.1.1 Operation read_Certificate

Die Operation `read_Certificate` initiiert den Anwendungsfall AdV-UC_24: „Zertifikat von eGK lesen“.

AdV-A_2090 - Operation read_Certificate
Die AdV-App MUSS Clientsystemen die Operation `read_Certificate` mit den Parametern der Tabelle TAB_ADV_082 bereitstellen.

Tabelle 49: TAB_ADV_082 Parameter der Operation read_Certificate

	Parameter	Beschreibung
Eingangs-Parameter	Identifier der eGK	Merkmal zur Identifizierung der eGK, deren Zertifikat ausgelesen werden soll.
	Identifier des Zertifikates	Merkmal zur Referenzierung des Zertifikates, das ausgelesen werden soll. (`C.ENC` oder `C.ENCV`).
Ausgangs-Parameter	Statusinformation	Ergebnis der Operation
	Zertifikat	Exportiertes Zertifikat.

[<=]

4.1.2 Operation encrypt

Die Operation `encrypt` initiiert den Anwendungsfall AdV-UC_25: „Mit eGK verschlüsseln“.

Beim hybriden Verschlüsseln von Plaintext werden ausschließlich Verschlüsselungszertifikate der eGK verwendet. Es können keine separaten Verschlüsselungszertifikate übergeben werden. Der symmetrische Schlüssel wird während der Operation erzeugt. Die Operation verhält sich konform zu [TR-03112-4#3.5.1] (Crypto Services/Encipher).

AdV-A_2091 - Operation encrypt
Die AdV-App MUSS Clientsystemen die Operation `encrypt` mit den Parametern der Tabelle TAB_ADV_083 bereitstellen.

Tabelle 50: TAB_ADV_083 Parameter der Operation encrypt

	Parameter	Beschreibung
Eingangs-	Identifier der eGK	Merkmal zur Identifizierung der eGK, deren

Parameter		Verschlüsselungszertifikate verwendet werden sollen.
	Identifier des Verschlüsselungs-Zertifikates	Merkmal zur Identifizierung des Zertifikates der eGK, mit dem verschlüsselt werden soll (ENC oder ENCV).
	Plaintext	Übergabe der zu verschlüsselnden Daten (Plaintext).
Ausgangs-Parameter	Statusinformation	Ergebnis der Operation
	Ciphertext	Rückgabe des Ciphertextes

[<=]

4.1.3 Operation decrypt

Die Operation `decrypt` initiiert den Anwendungsfall AdV-UC_26: „Mit eGK entschlüsseln“.

Beim Entschlüsseln hybrid verschlüsselter Dokumente wird Ciphertext entschlüsselt, wie er in der Schnittstelle `encrypt` verschlüsselt wurde. Die Operation verhält sich konform zu [TR-03112-4#3.5.2] (Crypto Services/Decipher).

AdV-A_2092 - Operation decrypt
Die AdV-App MUSS Clientsystemen die Operation `decrypt` mit den Parametern der Tabelle TAB_ADV_084 bereitstellen.

Tabelle 51: TAB_ADV_084 Parameter der Operation decrypt

	Parameter	Beschreibung
Eingangs-Parameter	Identifier der eGK	Merkmal zur Identifizierung der eGK, deren Schlüsselmaterial verwendet werden soll.
	Identifier des Entschlüsselungs-Zertifikates	Merkmal zur Identifizierung den privaten Schlüssel auf der eGK, mit dem entschlüsselt werden soll (ENC oder ENCV).
	Ciphertext	Enthält den Ciphertext, der entschlüsselt werden soll.
Ausgangs-Parameter	Statusinformation	Ergebnis der Operation
	Plaintext	Rückgabe des Plaintextes

[<=]

4.1.4 Operation authenticate

Die Operation `authenticate` initiiert den Anwendungsfall AdV-UC_27: „Authentisierungsrequest mit eGK signieren“.

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

AdV-A_2093 - Operation authenticate
Die AdV-App MUSS Clientsystemen die Operation `authenticate` mit den Parametern der Tabelle TAB_ADV_085 bereitstellen.

Tabelle 52: TAB_ADV_085 Parameter der Operation authenticate

	Parameter	Beschreibung
Eingangs-Parameter	Identifier der eGK	Merkmal zur Identifizierung der eGK, deren Schlüsselmaterial verwendet werden soll.
	Identifier des Zertifikates	Merkmal zur Referenzierung des Zertifikates, welches verwendet wird (AUT oder AUTN).
	Message	Die zu signierenden Daten gemäß [TR-03112-7#3.5.5]
Ausgangs-Parameter	Statusinformation	Gibt den Status des Signierens an.
	Signatur	Enthält im Erfolgsfalle die Signatur.

[<=]

5 Systemzerlegung (Deployment)

5.1 Übersicht

Die AdV in einer Umgebung im Auftrag der Kostenträger schließt die Lösung für die @home-Umgebung ein.

Die Systemzerlegung ordnet die Komponenten der Fachanwendung AdV den Zonen gemäß Zonenmodell der TI aus [gemKPT_Arch_TIP] zu.

Komponenten der AdV in einer Umgebung im Auftrag der Kostenträger:

- Produkttyp KTR-AdV mit den Komponenten AdV-Server und AdV-App
- Produkttyp Kostenträger-AdV-Terminal (KTR-AdV-Terminal)

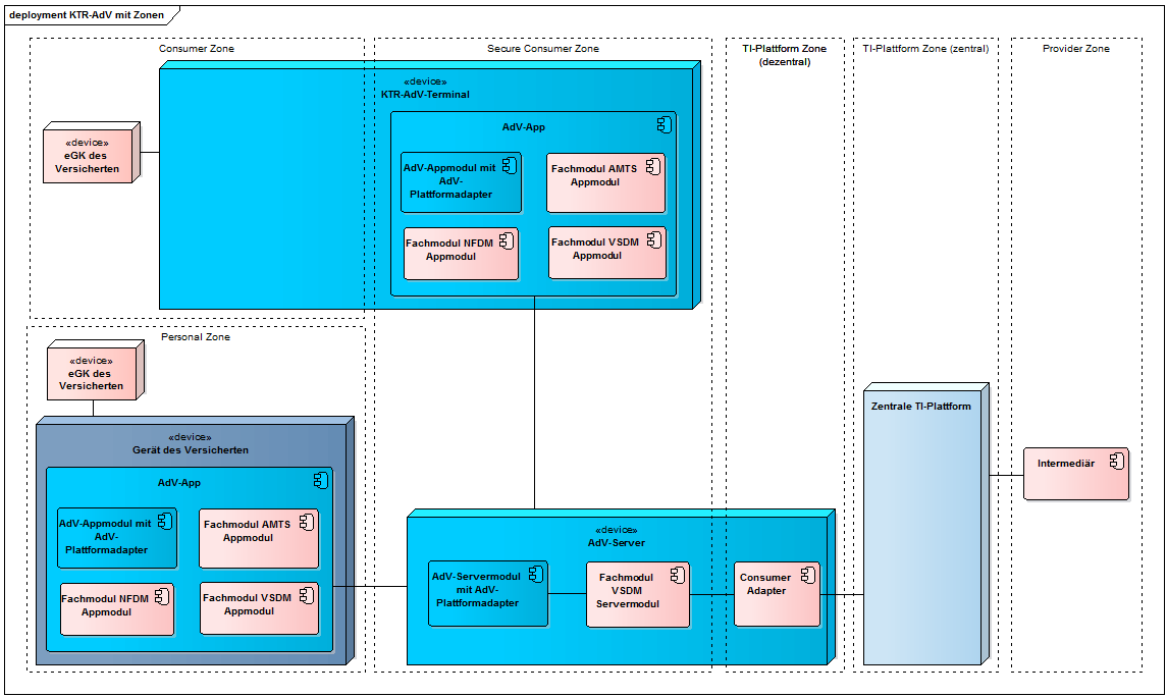

Abbildung 32: Systemzerlegung AdV in der Kostenträger-Umgebung

Die AdV-Lösung in der Umgebung des Versicherten (@home) verfolgt denselben Architekturansatz wie die AdV in einer Umgebung im Auftrag der Kostenträger. Ein Unterschied beider Lösungen besteht darin, dass bei der Systemzerlegung der AdV in einer Umgebung im Auftrag der Kostenträger mit dem KTR-AdV-Terminal ein Produkttyp der TI entsteht, an den Anforderungen für ein öffentlich zugängliches Gerät gestellt werden. Die Hardware der @home-Umgebung (Gerät des Versicherten) unterliegt als private Umgebung der Kontrolle und Verantwortlichkeit des Versicherten, dem einzig die AdV-App zur Verwendung auf seinem privaten Gerät, sowie Hinweise zur Verwendung von Kartenterminals, zur Verfügung gestellt werden.

Der Produkttyp KTR-AdV stellt gemäß Architekturkonzept [gemKPT_ArchTIP] ein RZ-Consumer in der dezentralen Zone der TI-Plattform dar. Zugriffe auf Dienste der zentralen TI-Plattform werden über die logische Komponente ConsumerAdapter gekapselt. Als Produkttyp der Fachanwendung AdV realisiert die KTR-AdV Funktionalität

in „Building Blocks“ des Zonenmodells der TI gemäß [gemKPT_ArchTIP] der Consumer Zone, Personal Zone, der Secure Consumer Zone und der TI-Plattform Zone dezentral. Entsprechend der Kommunikationsmatrix TI [gemKPT_ArchTIP] sind Kommunikationsbeziehungen von der KTR-AdV nur in Richtung der TI-Plattform zentral, in die Provider Zone und in die Existing Application Zone zulässig, wobei letztere über keinen Anwendungsfall in den Anwendungen des Versicherten verfügen. Gemäß Kommunikationsmatrix sind keine Kommunikationsbeziehungen aus der TI-Plattform zentral, aus der Providerzone oder aus der Existing Application Zone in Richtung KTR-AdV zulässig. Die Einhaltung dieser Kommunikationsregeln obliegt dem Zugangspunkt der KTR-AdV in die TI (z. B. über einen SZZP).

5.2 Übergreifende Anforderungen an AdV-Komponenten

Es gelten übergreifende Anforderungen des Datenschutzes und der Informationssicherheit.

AdV-A_2148 - Kein persistentes Speichern personenbezogener Daten
Eine AdV-Komponente DARF personenbezogene Daten NICHT persistent speichern.**[**<=**]**

AdV-A_2149 - Kein persistentes Speichern medizinischer Daten
Eine AdV-Komponente DARF medizinische Daten NICHT persistent speichern.**[**<=**]**

AdV-A_2162 - Temporäre Sitzungsdaten
Eine AdV-Komponente MUSS temporäre Daten und Daten des Versicherten im Arbeitsspeicher nach dem Beenden einer Sitzung des Versicherten löschen.**[**<=**]**

AdV-A_2150 - Informationstechnische Trennung von anderen Komponenten
Der Anbieter der AdV MUSS sicherstellen, dass die AdV-Komponenten informationstechnisch von anderen Komponenten getrennt sind.
[<=**]**

AdV-A_2155 - Vertraulichkeit der in den AdV-Komponenten verarbeiteten Daten
Die AdV-Komponenten MÜSSEN bei der Kommunikation untereinander die Vertraulichkeit der übertragenen Daten sicherstellen.
[<=**]**

AdV-A_2156 - Authentizität der AdV-Komponenten in der AdV-Umgebung
Die AdV-Komponenten MÜSSEN bei der Kommunikation untereinander die Authentizität der beteiligten AdV-Komponenten sicherstellen.**[**<=**]**

Die Mensch-System-Interaktion soll so gestaltet werden, dass Versicherte in der Lage sind, die AdV-Anwendungsfälle selbstständig, d. h. insbesondere ohne Unterstützung Dritter, zu nutzen.

AdV-A_2098 - Zugänglichkeit für Versicherte
Das AdV-Clientsystem SOLL die Vorgaben zur Ergonomie nach [DIN EN ISO 9241-171], „Ergonomie der Mensch-System-Interaktion, Teil 171: Leitlinien für die Zugänglichkeit von Software“ in der zum Zeitpunkt der Zulassungsbeantragung gültigen Fassung umsetzen.**[**<=**]**

Es muss berücksichtigt werden, dass der Versicherte gegebenenfalls nicht intuitiv mit einem Computersystem interagieren kann. Daher sollen dem Versicherten Informationen zur Nutzung der AdV bereitgestellt werden.

AdV-A_2163 - Unterstützung und Informationen für den Versicherten bei der Durchführung von Anwendungsfällen
Die Fachanwendung AdV MUSS dem Versicherten eine geeignete Hilfe und Informationen bei der Durchführung aller Anwendungsfälle anbieten.
Dies beinhaltet insbesondere die Zugriffe auf die eGK, Fehlerfälle und Konsequenzen sowie die Abgrenzung von anderen, auf der eGK vorhandenen, Fachanwendungen.**[<=]**

AdV-A_2164 - Anzeige der fachanwendungsspezifischen Daten
Die Fachanwendung AdV MUSS im Rahmen fachlicher Anwendungsfälle alle gelieferten Daten vollständig und für den Versicherten gut lesbar darstellen.**[<=]**

AdV-A_2099 - Barrierefreiheit
Das AdV-Terminal MUSS für Versicherte mit Aktivitätseinschränkungen Unterstützungsleistungen anbieten, mindestens für Personen, die zeitweilig oder dauerhaft nicht sehen können und für Personen mit eingeschränktem Sehvermögen.**[<=]**

AdV-A_2165 - Hinweis zum Ziehen der eGK
Das AdV-Clientsystem MUSS den Versicherten darauf hinweisen, dass die eGK nicht während der Durchführung eines Anwendungsfalls gezogen werden darf, ausser es ist im Ablauf des Anwendungsfalls vorgesehen.**[<=]**

AdV-A_2166 - Hinweis zur Vermeidung von Inkonsistenzen, Status einer Operation
Das AdV-Clientsystem MUSS den Versicherten darauf hinweisen, wann ein Anwendungsfall beendet oder abgebrochen wurde und die eGK gezogen werden darf.**[<=]**

AdV-A_2167 - Sichtschutz
Das AdV-Terminal SOLL gewährleisten, dass der Versicherte die Anwendungsfälle der AdV in öffentlich zugänglichen Umgebungen unbeobachtet durchführen kann.**[<=]**

Entsprechend dem Beschluss des Lenkungsausschusses vom 04.05.2017 sind die Bedingungen, unter denen ein AdV-Terminal eine Ausführungsumgebung für zusätzliche Anwendungen darstellen kann, noch zu klären.

Um die Akzeptanz für die Bereitstellung einer AdV-Umgebung zu erhöhen, soll auf dem AdV-Terminal die Möglichkeit bestehen, weitere von der TI unabhängige Anwendungen mit Mehrwert für den Versicherten anzubieten.

AdV-A_2100 - Verwendung zusätzlicher Software
Das AdV-Terminal KANN bei Wahrung aller gestellten Sicherheitsanforderungen eine Ablaufumgebung für weitere Anwendungen innerhalb der TI (gemäß WAusÜv) und zusätzliche Gesundheitsanwendungen außerhalb der TI sein, die nicht zum im Projektauftrag definierten Umfang der AdV gehören.
[<=]

Zusätzliche Gesundheitsanwendungen außerhalb der TI nutzen die Hardware des AdV-Terminals ausschließlich als Ablaufumgebung und dürfen die Anwendungen der TI nicht beeinflussen.

5.3 Systemschnitt AdV in einer Umgebung im Auftrag der Kostenträger/@home

Mit der AdV in einer Umgebung im Auftrag der Kostenträger werden für den Versicherten AdV-Lösungen im Bereich des Gesundheitswesens (z. B. in der Geschäftsstelle einer Krankenkasse) und in der @home-Umgebung bereitgestellt.

Die Geschäftsstellen der Krankenkassen sind in eine IT-Infrastruktur mit Anbindungen an Rechenzentren eingebunden. Um diese IT-Infrastruktur nach zu nutzen, wird eine Architektur mit Rechenzentrum-basierten Servern gewählt, die eine Anbindung an die TI und eine Erreichbarkeit weiterer kassenspezifischer Anwendungen ermöglicht. In den Rechenzentren werden SM-Bs in Form von Hardware Security Modulen betrieben, die eine remote Card-to-Card-Authentisierung mit der dezentral ausgelesenen eGK durchführen können.

In der Umgebung des Versicherten wird dieser Architekturansatz ebenfalls verfolgt, sodass auch hier eine Card-to-Card-Authentifizierung erfolgen kann.

Die Verarbeitung der AdV-Daten erfolgt lokal in den KTR-AdV-Umgebungen unter direkter dezentraler Kartenkommunikation, so dass auf die Verwendung von SICCT/Netzwerk-Kartenterminals verzichtet werden kann. Die Nutzung der kontaktlosen Kartenschnittstelle der eGK ist möglich.

5.3.1 Produkttyp KTR-AdV als AdV-Server mit AdV-App

Die KTR-AdV bietet Leistungen an, die der Consumer Zone, Personal Zone, Secure Consumer Zone und TI-Plattform Zone dezentral zugeordnet werden, und

- wird im Auftrag der Krankenkasse betrieben,
- bindet die @home-Umgebung über das Internet, sowie KTR-AdV-Terminals über Netzwerke der Geschäftsstelle an,
- stellt den Kostenträger-Umgebungen sowie der @home-Umgebung die AdV-App für die in Kapitel 3 genannten Anwendungsfälle zur Verfügung,
- initiiert die Kommunikation Richtung Services der zentralen TI und gesicherter fachanwendungsspezifischer Dienste und
- stellt ein Routing zwischen den Benutzerschnittstellen des Versicherten und weiteren kassenspezifischen Anwendungen bereit.

Zu jedem AdV-Server korrespondiert eine AdV-App, die über den AdV-Server bereitgestellt wird. Die AdV-App ist der einzige berechtigte Client, der Operationen an der Schnittstelle des AdV-Servers aufrufen darf.

Der Versicherte interagiert mit der AdV-App, die im KTR-AdV-Terminal bzw. in der Umgebung des Versicherten läuft und über die der Versicherte sämtliche Anwendungsfälle startet.

AdV-A_2117 - AdV-Server: Schnittstellen in die zentrale TI
Der AdV-Server MUSS Schnittstellen zu Fachdiensten und Dienste der zentralen TI unterstützen.**[**<=**]**

AdV-A_2118 - KTR-AdV: Clientsystemschnittstellen
Die KTR-AdV MUSS eine AdV-App zur Nutzung der Schnittstellen `I_Application_Management`, `I_PIN_Management` und `I_Certificate` durch den Versicherten bereitstellen.**[**<=**]**

Eine Übersicht der Schnittstellen in der KTR-AdV findet sich in Abbildung 3.

AdV-A_2170 - KTR-AdV: Interfaces für Fachanwendungen
Der AdV-Server und die AdV-App MÜSSEN den Fachanwendungen zur Realisierung ihrer Anwendungsfälle alle benötigten Schnittstellen der TI-Plattform anbieten.**[**<=**]**

AdV-A_2171 - AdV-Server: Zugriff nur durch berechtigte AdV-App
Der AdV-Server MUSS alle Anfragen nicht-autorisierter AdV- bzw. anderer Apps und Anwendungen verwerfen.**[**<=**]**

AdV-A_2119 - AdV-Server: SM-B für KTR-AdV Umgebung nutzen
Die KTR-AdV MUSS Anwendungsfälle mit der Identität einer SM-B für die KTR-AdV umsetzen.**[<=]**

AdV-A_2120 - AdV-App Deployment
Die AdV-App MUSS im KTR-AdV-Terminal bzw. in der Umgebung des Versicherten deployed sein. Die AdV-App MUSS lokal mit Browser und Kartenterminal und bei Bedarf remote mit dem AdV-Server interagieren.**[<=]**

AdV-A_2121 - AdV-App: Marktübliche Webbrowser
Die AdV-App MUSS gebräuchliche Webbrowser unterstützen, ohne im Browser eine spezielle Erweiterung zu erfordern.**[<=]**

AdV-A_2174 - AdV-App: Qualitätsvorgaben für das Clientsystem
Die AdV-App MUSS den Vorgaben der Fachanwendung AdV zu folgenden Kriterien entsprechen:

- Qualitätsvorgaben an das UI-Design
- Visualisierungsvorgaben von Anwendungsdaten
- Erklärungs- und Hilfe-Texte
- Vorgaben zur Barrierefreiheit.

[<=]

Die Fachanwendungen sind verantwortlich für Bereitstellung ihrer fachanwendungsspezifischen Daten und für die Vorgaben zur Anzeige der Daten.

AdV-A_2175 - AdV-App: Umsetzung von Anzeigevorgaben
Die AdV-App MUSS die Visualisierungsvorgaben für die Darstellung der Anwendungsdaten berücksichtigen, wenn diese durch die Fachanwendung vorgegeben werden.**[<=]**

AdV-A_2122 - AdV-App: CT-API-Schnittstellen
Die AdV-App MUSS gebräuchliche CT-API-Kartenleser unterstützen.**[<=]**

AdV-A_2123 - AdV-App: Unterstützung NFC
Die AdV-App KANN NFC für die Nutzung der kontaktlosen Schnittstelle der eGK unterstützen.**[<=]**

Die Kartenzugriffe werden von der AdV-App lokal am KTR-AdV-Terminal bzw. in der Umgebung des Versicherten ausgeführt.

Mit einer remote Card-to-Card-Authentisierung zwischen eGK und SM-B wird die Authentizität der beteiligten Komponenten überprüft und die eGK für die Durchführung der AdV-Anwendungsfälle freigeschaltet.

AdV-A_2124 - AdV-Server, AdV-App: Remote Card-to-Card
Die AdV-App und der AdV-Server MÜSSEN eine remote Card-to-Card-Authentisierung zwischen der eGK im Zugriff der AdV-App und der SM-B am AdV-Server umsetzen.**[<=]**

Die zentrale TI ist für die AdV-Terminal/@home-Umgebung nur über den AdV-Server erreichbar. Die PKI und die Schnittstellen in die TI werden von der KTR-AdV nach Vorgaben der TI genutzt.

Der AdV-Server wird in einem Rechenzentrum der Krankenkassen betrieben, die in sicherheitstechnischer und betrieblicher Hinsicht den Regelungen des SGB unterliegen.

AdV-A_2116 - AdV-Server: Betrieb in Rechenzentren im Auftrag der Krankenkassen
Der Anbieter einer KTR-AdV MUSS den AdV-Server in einem Rechenzentrum im Auftrag der Krankenkassen betreiben.**[<=]**

AdV-A_2125 - AdV-Server: Selbstschutz
Der AdV-Server MUSS Sicherheitsmechanismen besitzen, die ihn gegen unbefugte Zugriffe aus dem Internet schützen.**[<=]**

AdV-A_2154 - KTR-AdV: Keine Informationen über Versicherte
Der Hersteller der KTR-AdV MUSS technisch sicherstellen, dass die Verarbeitung der Daten des Versicherten lokal in der AdV-App geschieht und nur in zulässigen Anwendungsfällen an den AdV-Server übertragen werden.
[<=]

AdV-A_2569 - KTR-AdV: Keine Informationen über Versicherte aus Fachanwendungen
Der Betreiber und der Anbieter der KTR-AdV DÜRFEN Informationen des Versicherten über die Verwendung von medizinischen Fachanwendungen oder deren Daten NICHT erlangen.**[<=]**

5.3.2 Produkttyp KTR-AdV-Terminal

Ein AdV-Terminal ist ein für die eigenständige Nutzung von AdV durch Versicherte in Umgebungen des Gesundheitswesens konzipiertes Benutzerendgerät.

Das KTR-AdV-Terminal ist Bestandteil der Consumer Zone und

- stellt dem Versicherten ein Benutzerinterface für die AdV zur Verfügung und
- stellt die Ausführungsumgebung der durch den AdV-Server bereitgestellten AdV-App dar.

Das KTR-AdV-Terminal muss aus Bedienelementen zur eigenständigen Nutzung des Versicherten bestehen.

AdV-A_2126 - KTR-AdV-Terminal: Hardwareumfang
Das KTR-AdV-Terminal MUSS ein Kartenterminal, eine Anzeigeeinheit und Bedienelemente (z. B. mit Möglichkeit zur Texteingabe) umfassen, die für Versicherte zugänglich sind.**[<=]**

AdV-A_2127 - KTR-AdV-Terminal: Kartenterminal und Treiber
Das KTR-AdV-Terminal SOLL ein fest verbautes CT-API-Kartenterminal samt Treiber umfassen.**[<=]**

AdV-A_2128 - KTR-AdV-Terminal: Kartenterminal und Treiber (kontaktlos)
Das KTR-AdV-Terminal KANN die kontaktlose Schnittstelle der eGK nutzen.**[<=]**

Der AdV-Server stellt mit der AdV-App eine sichere Ablaufumgebung für die AdV-Anwendungsfälle bereit.

AdV-A_2129 - KTR-AdV-Terminal: Browser
Das KTR-AdV-Terminal KANN einen marktüblichen Browser umfassen, der mit der AdV-App interagieren kann.**[<=]**

AdV-A_2172 - KTR-AdV-Terminal: Schutz vorhandener Schnittstellen
Das KTR-AdV-Terminal MUSS sicherstellen, dass ggf. vorhandene Schnittstellen des Terminals nicht genutzt werden können, um Daten der Versicherten unautorisiert einzusehen oder zu verändern.**[<=]**

AdV-A_2173 - KTR-AdV-Terminal: Technische Maßnahmen zum Schutz verarbeiteter Daten
Das KTR-AdV-Terminal MUSS sicherstellen, dass die im Terminal verarbeiteten Daten durch technische Maßnahmen im Hinblick auf ihre Schutzbedürftigkeit angemessen geschützt werden.**[<=]**

5.3.3 @home-Umgebung

Die @home-Umgebung ist eine private, nicht öffentlich zugängliche Umgebung des Versicherten, über die dieser die alleinige Kontrolle hat. Sie ist kein Produkttyp der TI.

Die KTR-AdV stellt für den Versicherten @home eine AdV-App, sowie Empfehlungen zur Nutzung von AdV in seiner privaten Umgebung bereit.

Die @home-Umgebung ist Bestandteil der Personal Zone und

- stellt dem Versicherten ein Nutzerinterface für die AdV zur Verfügung,
- nutzt die durch den AdV-Server bereitgestellte AdV-App.

Die @home-Umgebung enthält Geräte, etwa Kartenterminal, sowie einen Computer mit geeigneten Bedienelementen, die der Versicherte zur Nutzung der AdV-App benötigt. Die @home-Umgebung kann einen marktüblichen Browser enthalten, der mit der AdV-App interagiert.

AN_@H_1: Die Versicherten übernehmen die Verantwortung dafür, ihre eigenen IT-Systeme (GdV) in der Umgebung des Versicherten auf das für die clientseitige Nutzung des AdV-Servers angemessene Sicherheitsniveau zu bringen.

Die Einhaltung der Annahme AN_@H_1 obliegt dem Versicherten selbst.

AdV-A_2131 - Empfehlung von Kartenlesern @home
Der Anbieter der KTR-AdV MUSS dem Versicherten Empfehlungen für geeignete Kartenleser in der @home-Umgebung bereitstellen.**[<=]**

5.3.4 Nutzung des eCard-API-Framework

Lösungen für die AdV in einer Umgebung im Auftrag der Kostenträger sollen mit einem standardbasierten Vorgehen umgesetzt werden. Es eröffnet die Möglichkeit, AdV-Komponenten mit etablierten Verfahren zur Sicherheitsbestätigung vereinbar zu machen.

Die Kommunikation zwischen eGK, Kartenleser, AdV-App und AdV-Server in den Umgebungen der Kostenträger und der @home-Umgebung und den evaluierten Rechenzentren kann gemäß den Technischen Richtlinien [TR-03112](Die eCard – API wird durch das BSI bereitgestellt, siehe auch https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03112/index_htm.html), [TR-03124](Der eID-Client zur Authentisierung des Versicherten für die Echtheitsprüfung der eGK https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03124/index_htm.html) und [TR-03130](Der eID-Server zur Freischaltung der eGK mittels Identität einer SM-B für die KTR-AdV https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03130/tr-03130.html) des BSI erfolgen.

Ein standardbasiertes Vorgehen konform zu den technischen Richtlinien des BSI fokussiert sich dabei auf diejenigen Aspekte, die für die Nutzung der eGK durch Versicherte in der KTR- und @home-Umgebung relevant sind.

5.3.4.1 Schichtenarchitektur

In der AdV in einer Umgebung im Auftrag der Kostenträger und @home kommen Komponenten zum Einsatz, die dem Versicherten Anwendungsfälle auf bzw. mit seiner eGK und ggfs. über eine Browseroberfläche ermöglichen. Für den lokalen Zugriff auf die eGK des Versicherten stellt das BSI das eCard-API-Framework [TR-03112] zur Verfügung.

Ferner stellt das BSI mit den Richtlinien [TR-03124] und [TR-03130] zur Verwendung elektronischer Identitäten (eID) einen Mechanismus bereit, mit dem sich die eGK des

Versicherten und eine SM-B mit Identität für die KTR-AdV via Card-to-Card gegenseitig authentisieren können.

Die folgende Abbildung zeigt den Aufbau des eCard-API-Frameworks [1] zur Anbindung der eGK des Versicherten an die AdV-App. Die übrigen Technischen Richtlinien bauen auf diese auf.

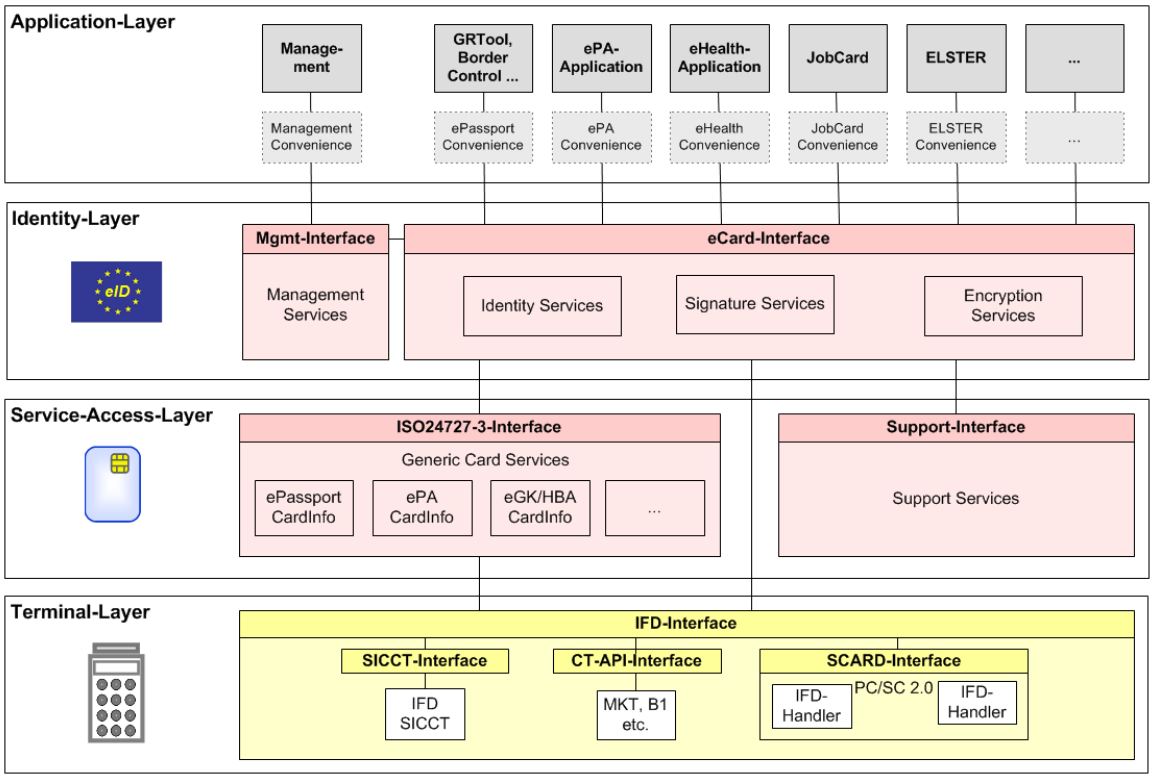

Abbildung 33: Architekturschichten der AdV-eCard-API

Im Rahmen der eCard-API-Architektur werden vor allem die in Abbildung 33 blau markierten Systemteile von AdV genutzt, nicht aber das vollständige eCard-API-Framework.

Der Application Layer beinhaltet die AdV-Anwendungslogik in der AdV-App und nutzt die verschiedenen Schnittstellen der eCard-API für den Zugriff auf die eGK.

Der Identity-Layer stellt der AdV-Anwendungslogik Schnittstellen für Authentisierungs- und Kryptooperationen der eGK bereit.

Der Service-Access-Layer stellt der AdV-Anwendungslogik Smartcard-Schnittstellen gemäß [ISO24727-3] für das Lesen und Schreiben von Daten von der/auf die eGK bereit. Zur Abbildung von Schnittstellenoperationen auf Kartenkommandos ist ein CardInfo-File für die jeweilige Version der eGK erforderlich.

Über den Terminal-Layer kann die AdV-App einerseits Operationen auf dem angebundenen Kartenlesegerät ausführen (z. B. Textausgabe auf einem Kartenterminaldisplay). Daneben kann die AdV-App Kartenkommandos direkt an die gesteckte eGK weiterleiten.

Die AdV-App verwendet ein lokal über die CT-API-Schnittstelle angebundenes Kartenterminal.

Die AdV-App setzt die AdV-Anwendungsfälle der Systemlösung AdV [gemSysL_AdV], sowie weitere relevante Anforderungen der TI, z. B. in Bezug auf Netzwerkkommunikation und PKI um und bedient sich dabei der Schnittstellen der eCard-API soweit ein Zugriff auf die eGK erforderlich ist.

5.3.4.2 Kommunikationsmuster

Zur Authentisierung und Freischaltung der eGK können die [TR-03124] und [TR-03130] auf Basis der eCard-API verwendet werden. Das Kommunikationsmuster der zugrunde liegenden Card-to-Card-Authentisierung ist in der folgenden Abbildung dargestellt.

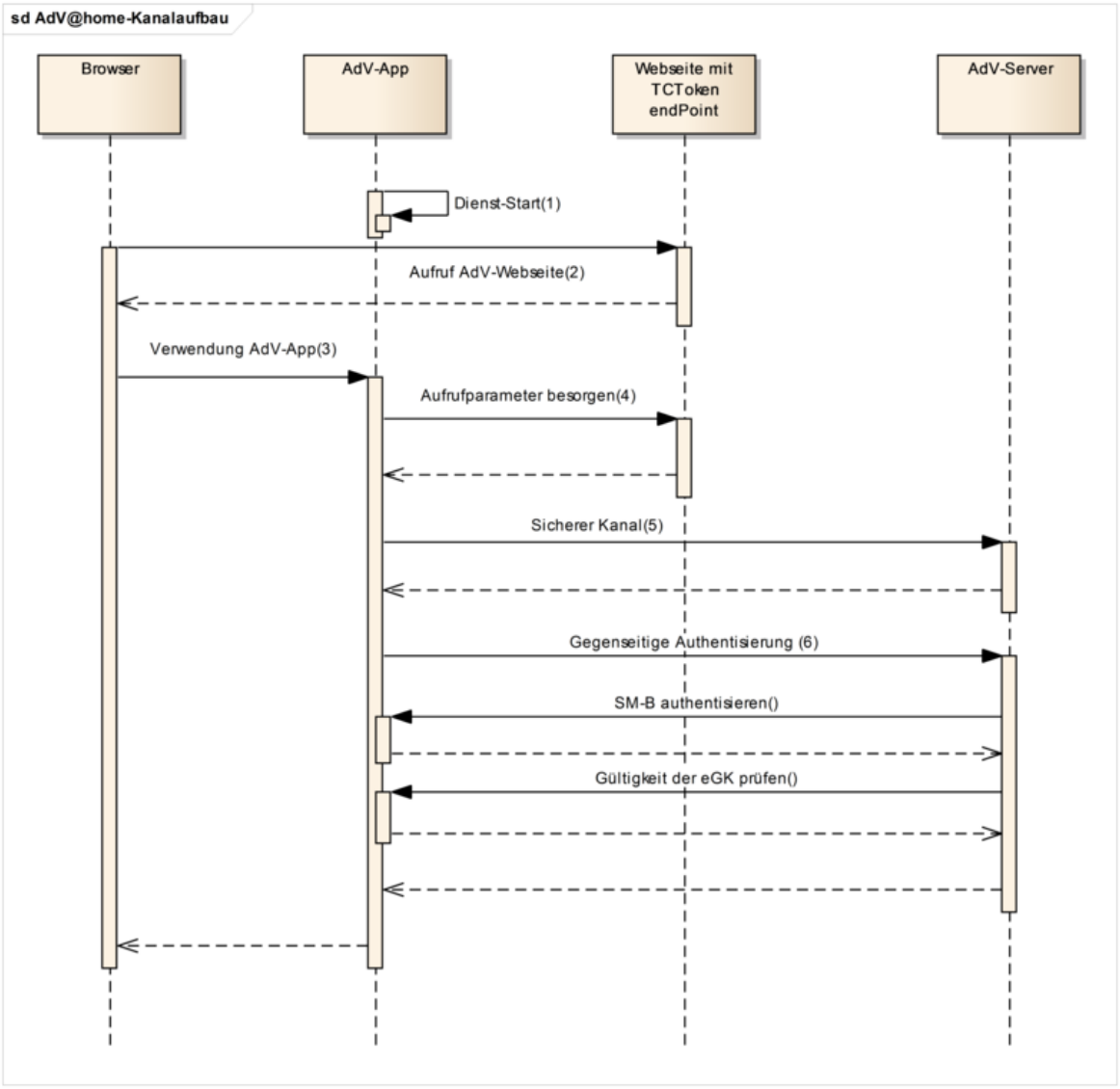

Abbildung 34: Aufbau sicherer Kanal und gegenseitige Authentisierung

Kommunikationsfluss zum Aufbau eines sicheren Kanals von der AdV-App zum AdV-Server mit anschließender Card-to-Card-Authentisierung

1. Die AdV-App wird als Dienst auf dem Benutzerendgerät gestartet,
2. der Versicherte steuert über eine Webseite eines Kostenträgers die Nutzung von AdV mit seiner eGK an,

3. der Versicherte wird von der Webseite des Kostenträgers auf die lokale Adresse des AdV-App-Dienstes weitergeleitet und erhält die Adresse eines Tokenservers (z.B. Tokenserver in der Hoheit des gleichen Kostenträgers),
4. die AdV-App besorgt das Token vom Tokenserver, dessen Adresse in (3) mitgeteilt wurde.
5. Die AdV-App baut einen sicheren Kanal zum AdV-Server auf.
6. Die AdV-App initiiert die Authentisierung zwischen AdV-App und AdV-Server. Während der Authentisierung prüft der AdV-Server mit Hilfe der Public Key Infrastructure (PKI) die Echtheit der eGK. Die eGK authentisiert umgekehrt die Identität der SM-B des Kostenträgers.

Nach Abschluss des Handshakes zwischen der eGK im Zugriff der AdV-App und einer SM-B im Zugriff des AdV-Servers gelangt die eGK in einen Sicherheitszustand, der eine lokale Ausführung von AdV-Anwendungsfällen in den Umgebungen im Auftrag der Kostenträger ermöglicht.

5.4 Administration der Anwendungen des Versicherten

Der folgende Abschnitt skizziert das Konzept der Administration der an der AdV beteiligten Komponenten. Die Administration ist ein Umsetzungskonzept für geschultes Personal, welches Anpassungen an der Konfiguration der Systemkomponenten vornimmt, um eine Betriebsbereitschaft initial herzustellen und im laufenden Betrieb sicherzustellen.

AdV-A_2176 - Protokollierung von fachlichen Fehlern
Die Fachanwendung AdV MUSS fachliche Fehler außerhalb der eGK protokollieren und die Protokolleinträge derart gestalten, dass eine Fehleranalyse zur Behebung des Problems ermöglicht wird.**[**<=**]**

5.4.1 Allgemeines

Zum Schutz vor Manipulation oder unbeabsichtigter Fehlkonfiguration durch Dritte müssen alle Komponenten einen Administrationsmodus oder -bereich haben, der durch gesonderte Zugriffsrechte geschützt ist.

AdV-A_2141 - Geschützter Administrationsbereich
Alle AdV-Komponenten mit konfigurierbaren Parametern MÜSSEN einen zugriffsgeschützten Bereich besitzen, der nur für den Administrator zugänglich ist.**[**<=**]**

AdV-A_2142 - Administrationsparameter
Der Anbieter der AdV MUSS sicherstellen, dass der Administrator sämtliche konfigurierbaren Parameter der Komponente einsehen und ändern kann.**[**<=**]**

Die konkreten Anforderungen an konfigurierbare Parameter ergeben sich auf Spezifikationsebene.

AdV-A_2143 - Logging-Informationen der AdV-Komponente anzeigen
Eine AdV-Komponente KANN im Administrationsbereich Logging-Informationen darstellen.**[**<=**]**

Folgende Log-Typen können dargestellt werden: EventLog, SecurityLog, Ablaufprotokoll, PerformanceLog, DebugLog.

AdV-A_2177 - Verbot der Protokollierung medizinischer Daten
Die Fachanwendung AdV DARF medizinische Daten NICHT protokollieren.**[**<=**]**

AdV-A_2178 - Verbot der Protokollierung personenbezogener Daten
Die Fachanwendung AdV DARF personenbezogene Daten NICHT protokollieren, wenn Sie nicht im Zusammenhang mit einem Systemfehler stehen oder für eine Fehlerbehebung nicht zwingend erforderlich sind.**[<=]**

5.4.2 Verwaltete Artefakte

Die folgenden Anforderungen ergeben sich aus der Systemzerlegung. Kommen durch Anpassungen weitere Komponenten hinzu, soll für diese ebenso eine Administratorschnittstelle vorgesehen werden.

AdV-A_2146 - Administration AdV-Server
Der AdV-Server MUSS eine Administrationsschnittstelle bereitstellen, über die der Betreiber des AdV-Servers die für den Betrieb erforderlichen Parameter verwaltet.**[<=]**

AdV-A_2147 - Administration KTR-AdV-Terminal
Das KTR-AdV-Terminal MUSS über eine zugriffsgeschützte Administrationsschnittstelle verfügen, über welche die für den Betrieb des KTR-AdV-Terminals erforderlichen Parameter verwaltet werden.**[<=]**

6 Informationsmodell

6.1 Fachliches Informationsmodell

Die Fachanwendungen der eGK haben das technische Informationsmodell der auf der eGK des Versicherten gespeicherten Anwendungsdaten in den Dokumenten der Tabelle TAB_ADV_091 festgelegt.

Tabelle 53: TAB_ADV_091 Informationsmodell der Fachanwendungen

Anwendung	Referenzen	Ordner/Dateien auf der eGK
VSDM	[gemSysL_VSDM#6.2]	EF.PD, EF.VD, EF.GVD
NFDM	[gemSpec_InfoNFDM]	DF.NFD, DF.DPE
eMP/AMTS	[gemSysL_AMTS_A]	DF.AMTS

6.2 Technisches Informationsmodell

6.2.1 Zugriffs-Protokollierung

Einträge in die Zugriffsprotokollierung auf die eGK beinhalten Informationen darüber, wer zu welchem Zeitpunkt welche Art Zugriff auf die eGK hatte.

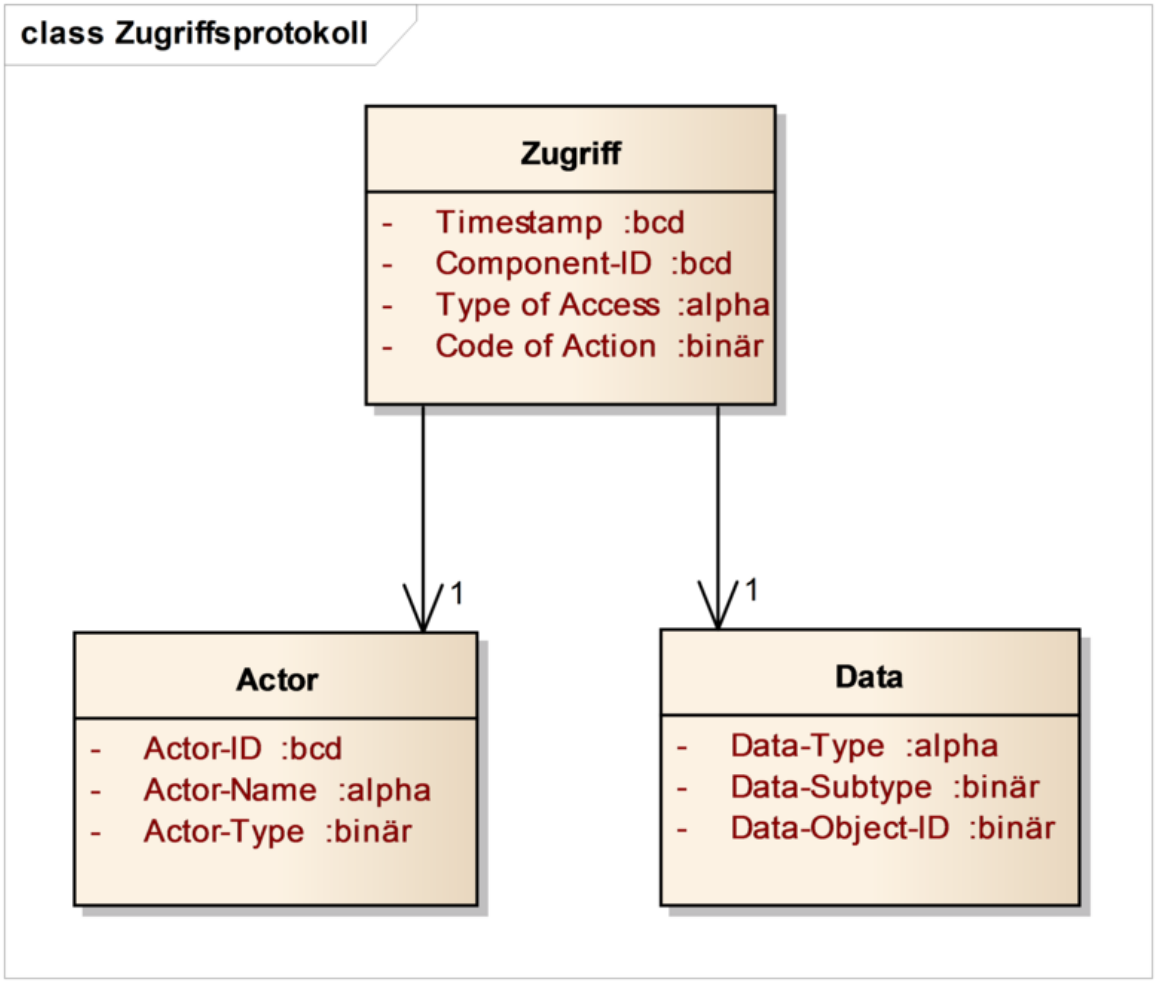

Abbildung 35: Informationsmodell Zugriffsprotokoll

Die Einträge Component-ID (zur Identifizierung involvierter technischer Komponenten) und Actor-ID sind optional. Die Belegung der Werte wird durch die Fachanwendungen spezifiziert (siehe [gemSpec_Karten_Fach_TIP]).

Die Tabelle TAB_ADV_092 listet beispielhafte Protokolleinträge für zwei Aktionen aus VSDM (siehe [gemSpec_FM_VSDM#Tab_FM_VSDM_06]).

Tabelle 54: TAB_ADV_092 Beispiele für Protokolleinträge VSDM

Aktion	Data-Type	Type of Access	Actor-ID	Actor-Name	Auslöser
Lesen der geschützten VSD	1	R	ICCSN HBA/ SM-B	Name des Akteurs	Erfolgreicher, lesender Zugriff auf die geschützten Versichertendaten.
Aktualisierung der eGK (VSD)	1	U	ICCSN HBA/ SM-B	Name des Akteurs	Durchführen einer erfolgreichen VSD-Aktualisierung (ServiceType VSD im Aktualisierungsauftrag).

6.2.2 Weitere freiwillige Anwendungen

In 10 Einträgen können zu einer weiteren TI-basierten weiteren freiwilligen Anwendung auf der eGK jeweils ein Verweis, sowie eine Einwilligung verwaltet werden. Die Zuordnung zwischen Verweis und Einwilligung erfolgt durch die Reihenfolge der Einträge (siehe [gemeGK_Fach#7,8]).

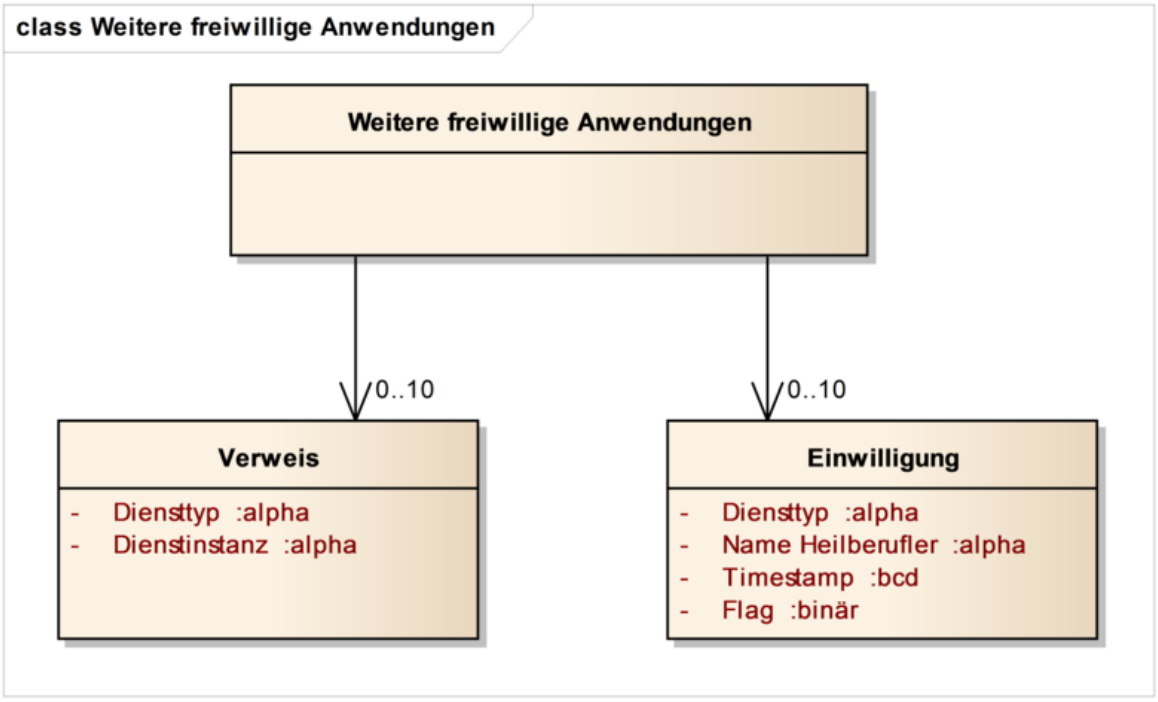

Abbildung 36: Informationsmodell Weitere freiwillige Anwendungen

7 Ergänzungen zum Leistungsumfang

Bereits jetzt bekannte Zukunftsthemen der AdV sind (s.a. [gemAnforderungen_AdV#5):

- Übergreifendes Leistungsmerkmal Daten- und Berechtigungserhalt
- Ausbaustufen von ORS2.1-Anwendungen:
  - Zukunftsthemen NFDM
  - Zukunftsthemen eMP/AMTS
- Neu hinzu kommende Anwendungen, insbesondere:
  - Elektronische Organspendeerklärung
  - Elektronisches Patientenfach
  - Gesundheitsdatendienste (Verwaltung von Einwilligungen und Verweisen zu GDD)
- Unterstützung nachladbarer Konfigurationen für AdV-Anwendungsfälle nach Einführung eines modularen Konnektors

Beispielhaft wird das Leistungsmerkmal geschildert, das AdV der zukünftigen Anwendung elektronisches Patientenfach bereitstellt.

Die Fachanwendung AdV stellt Versicherten Grundlagen zur Verfügung, die vom Patientenfach genutzt werden können:

- Schnittstellen zum Authentisieren, Verschlüsseln und Entschlüsseln von Daten mit der eGK
- Komponenten zur eigenständigen Nutzung für Versicherte

Die Fachanwendung AdV schafft in diesem Sinne die Voraussetzungen für den Zugang des Versicherten zum Patientenfach.

8 Lieferumfang

Die Dokumentenlandkarte (Abbildung 1) gibt einen Überblick über die Dokumente, welche im Rahmen des Projektes AdV in der Konzeptions- und Spezifikationsphase bereitgestellt werden.

Tabelle 55: TAB_ADV_093 Lieferumfang Projekt AdV

Dokument	
[gemSysL_AdV]	Systemspezifisches Konzept Anwendungen des Versicherten (AdV)
[gemKPT_Betr]	Betriebskonzept Im Rahmen von ORS2.1 erstellt.
[gemKPT_Test]	Testkonzept Im Rahmen von ORS2.1 erstellt.
[gemSpec_KTR-AdV]	Spezifikation KTR-AdV
[gemSpec_KTR-AdV-Terminal]	Spezifikation KTR-AdV-Terminal
[gemSpec_FM_AMTS]	Spezifikation Fachmodul AMTS Im Rahmen des Projektes AMTS erstellt.
[gemSpec_FM_NFDM]	Spezifikation Fachmodul NFDM Im Rahmen des Projektes NFDM erstellt.
[gemSpec_FM_VSDM]	Spezifikation Fachmodul VSDM Im Rahmen des Projektes VSDM erstellt.

9 Anhang A – Verzeichnisse

9.1 Abkürzungen

Abkürzung	Bedeutung
AdV	Anwendungen des Versicherten
AMTS	Fachanwendung Arzneimitteltherapiesicherheit
C2C	Card-to-Card-Authentisierung
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
GDD	Gesundheitsdatendienst
HCA	Health Care Application
HSM	Hardware Security Module
KSR	Konfigurations- und Software-Repository
KTR	Kostenträger
KTR-AdV	AdV in einer Umgebung im Auftrag der Kostenträger
LE	Leistungserbringer
NFD	Notfalldatensatz
NFDM	Notfalldatenmanagement
n/a	entfällt
PD	Persönliche Versichertendaten
PIN	Personal Identification Number

PUK	Personal Unblocking Key
SM-B	Sammelbegriff für SMC-B und HSM-B
TI	Telematikinfrastruktur
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.

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

9.3 Abbildungsverzeichnis

9.4 Tabellenverzeichnis

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 entnehmen Sie bitte der aktuellen, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

[Quelle]	**Herausgeber (Erscheinungsdatum): Titel**
[gemAnforderungen_AdV]	gematik: Anforderungskatalog Anwendungen des Versicherten (AdV)
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemeGK_Fach]	gematik: Speicherstrukturen der eGK für Gesundheitsanwendungen (Version 1.6.0 vom 18.03.2008)
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemSysL_AMTS_A]	gematik: Systemspezifisches Konzept AMTS Stufe A
[gemSpec_FM_VSDM]	gematik: Spezifikation Fachmodul VSDM
[gemSpec_InfoNFDM]	gematik: Informationsmodell Notfalldaten-Management (NFDM)

[gemSpec_eGK_ObjSys]	gematik: Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem
[gemSpec_Karten_Fach_TIP]	Befüllvorschriften für die Plattformanteile der Karten der TI
[gemSysL_NFDM]	gematik: Systemspezifisches Konzept Notfalldaten-Management (NFDM)
[gemSysL_VSDM]	gematik: Systemspezifisches Konzept Versichertenstammdatenmanagement (VSDM)

9.5.2 Weitere Dokumente

[Quelle]	**Herausgeber (Erscheinungsdatum): Titel**
[DIN EN ISO 9241-171]	DIN EN ISO 9241-171, Ergonomie der Mensch-System-Interaktion, Teil 171: Leitlinien für die Zugänglichkeit von Software
[ISO/IEC 24727-3]	ISO 24727 - Identification cards — Integrated Circuit Card Programming Interfaces — Part 3: Application interface
[ISO/IEC 24727-4]	ISO 24727 - Identification Cards — Integrated Circuit Cards Programming Interfaces — Part 4: API Administration, 2007. ISO/IEC.
[Kruchten]	Philippe B. Kruchten, The 4+1 View Model of Architecture
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt (zuletzt geprüft am 14.12.2006)
[TR-03112]	BSI: Technische Richtlinie TR-03112, eCard-API-Framework
[TR-03112-1]	BSI: Technical Guideline TR-03112-1 eCard-API-Framework – Overview Version 1.1.5 draft 7. April 2015
[TR-03112-4]	BSI: Technical Guideline TR-03112-4 eCard-API-Framework – ISO 24727-3-Interface Version 1.1.5 7. April 2015

[TR-03112-5]	BSI: Technical Guideline TR-03112-5 eCard-API-Framework – Support-Interface Version 1.1.5 7. April 2015
[TR-03112-6]	BSI: Technical Guideline TR-03112-6 eCard-API-Framework – IFD-Interface Version 1.1.5 7. April 2015
[TR-03112-7]	BSI: Technical Guideline TR-03112-7 eCard-API-Framework – Protocols Version 1.1.5 7. April 2015
[TR-03119]	BSI: Technische Richtlinie TR-03119: Requirements for Smart Card Readers supporting eID and eSign based on Extended Access Control
[TR-03124]	BSI: Technical Guideline TR-03124: eID-Client
[TR-03130]	BSI: Technische Richtlinie TR-03130: eID-Server

10 Anhang B – Übersicht Anwendungsfälle

Die Tabelle TAB_ADV_094 bietet eine Übersicht über die durch den Versicherten in den einzelnen Umgebungen ausführbaren Anwendungsfälle.

Tabelle 56: TAB_ADV_094 Übersicht Anwendungsfälle

Anwendung	Anwendungsfälle	Umgebung im Auftrag des KTR	Umgebung des Versicherten
Anwend-ungsüber-greifend	Zugriffprotokoll von eGK lesen	X	X
	PIN ändern	X	X
	PIN auf eGK entsperren	X	X
	PIN für Fachanwendung einschalten	X	X
	PIN für Fachanwendung ausschalten	X	X
	Echtheit und Gültigkeit der eGK prüfen	X	X
	Mit eGK verschlüsseln	X	X
	Mit eGK entschlüsseln	X	X
	Authentisierungsrequest mit eGK signieren	X	X
	Zertifikat von eGK lesen	X	X
	EF.Einwilligung von eGK lesen	X	X
	EF.Verweis auf eGK schreiben	X	X
	EF.Einwilligung auf eGK löschen	X	X

	Datenübertragung bei Kartentausch	X	X
VSDM	VSD von eGK lesen	X	X
NFDM	NFD von eGK anzeigen		
	NFD auf eGK löschen		
	NFD auf eGK verbergen	X	X
	Verborgene NFD auf eGK sichtbar machen	X	X
DPE	DPE von eGK anzeigen	X	X
	DPE auf eGK ändern	X	X
	DPE auf eGK löschen	X	X
	DPE auf eGK verbergen	X	X
	Verborgene DPE auf eGK sichtbar machen	X	X
eMP/AMTS	eMP/AMTS-Daten von eGK anzeigen		
	Einwilligung AMTS von eGK anzeigen		
	Einwilligung AMTS auf eGK löschen		
	eMP/AMTS auf eGK verbergen	X	X
	Verborgenen eMP/AMTS-Datensatz auf eGK sichtbar machen	X	X
	AMTS-Vertreter-PIN auf der eGK ändern	X	X

	AMTS-Vertreter-PIN auf der eGK entsperren	X	X

11 Anhang C

Die Tabelle TAB_ADV_095 bietet eine Übersicht der in der Konfiguration der Basis-Anwendungsfälle genutzten Identifier von Anwendungen.

Tabelle 57 : TAB_ADV_095 Identifier von Anwendungen

Code	Bedeutung
FA_AMTS	Anwendung eMP/AMTS
FA_AMTS_CON	Einwilligung in die Nutzung der Anwendung eMP/AMTS
FA_CON	Einwilligungen und Verweise zu weiteren freiwilligen Anwendungen
FA_DPE	DPE (Anwendung NFDM)
FA_NFD	NFD (Anwendung NFDM)
FA_VSDM	Fachanwendung VSDM
Protokoll	Zugriffprotokoll der eGK