

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

KTR-AdV

Produkttyp Version: 1.0.2-0
Produkttyp Status: freigegeben

Version: 1.0.0
Revision: 200014
Stand: 02.03.2020
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemProdT_KTR-AdV_PTV_1.0.2-0

Historie Produkttypversion und Produkttypsteckbrief

Historie Produkttypversion

Die Produkttypversion ändert sich, wenn sich die Anforderungslage für den Produkttyp ändert und die Umsetzung durch Produktentwicklungen ebenfalls betroffen ist.

Produkttypversion	Beschreibung der Änderung	Referenz
1.0.0-0	Initiale Version auf Dokumentenebene	[gemProdT_KTR-AdV_PTV1.0.0-0]
1.0.1-0	Aktualisierung auf R3.1.2	[gemProdT_KTR-AdV_PTV1.0.1-0]
1.0.2-0	Aktualisierung auf R3.1.2	[gemProdT_KTR-AdV_PTV1.0.2-0]

Historie Produkttypsteckbrief

Die Dokumentenversion des Produkttypsteckbriefs ändert sich mit jeder inhaltlichen oder redaktionellen Änderung des Produkttypsteckbriefs und seinen referenzierten Dokumenten. Redaktionelle Änderungen haben keine Auswirkung auf die Produkttypversion.

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	02.03.20		freigegeben	gematik

Inhaltsverzeichnis

1 Einführung	4
1.1 Zielsetzung und Einordnung des Dokumentes	4
1.2 Zielgruppe	4
1.3 Geltungsbereich	4
1.4 Abgrenzung des Dokumentes	5
1.5 Methodik	5
2 Dokumente	6
3 Blattanforderungen.....	8
3.1 Anforderungen zur funktionalen Eignung	8
3.1.1 Produkttest/Produktübergreifender Test	8
3.1.2 Herstellererklärung funktionale Eignung	21
3.2 Anforderungen zur sicherheitstechnischen Eignung	31
3.2.1 CC-Evaluierung	31
3.2.2 Sicherheitsgutachten	31
3.2.3 Herstellererklärung sicherheitstechnische Eignung.....	33
3.2.4 Zertifizierung nach Technischer Richtlinie	36
3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung	38
4 Produkttypspezifische Merkmale	39
4.1 Optionale Ausprägungen	39
5 Anhang A – Verzeichnisse	41
5.1 Abkürzungen	41
5.2 Tabellenverzeichnis	41
5.3 Referenzierte Dokumente	42

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an Herstellung und Betrieb von Produkten des Produkttyps KTR-AdV oder verweist auf Dokumente, in denen verbindliche Anforderungen mit ggf. anderer Notation zu finden sind. Die Anforderungen bilden die Grundlage für die Erteilung von Zulassungen, Zertifizierungen bzw. Bestätigungen durch die gematik (Wenn im weiteren Dokument vereinfachend der Begriff „Zulassung“ verwendet wird, so ist dies der besseren Lesbarkeit geschuldet und umfasst übergreifend neben dem Verfahren der Zulassung auch Zertifizierungen und Bestätigungen der gematik-Zulassungsstelle.).

Die Anforderungen werden über ihren Identifier, ihren Titel sowie die Dokumentenquelle referenziert. Die Anforderungen mit ihrem vollständigen, normativen Inhalt sind dem jeweils referenzierten Dokument zu entnehmen.

1.2 Zielgruppe

Der Produkttypsteckbrief richtet sich an KTR-AdV-Hersteller und -Anbieter sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Zulassungsverfahrens
- dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
- akkreditierten Materialprüflaboren
- Auditoren

Bei zentralen Diensten der TI-Plattform und fachanwendungsspezifischen Diensten beziehen sich Anforderungen, die sowohl an Anbieter als auch Hersteller gerichtet sind, jeweils auf den Anbieter als Zulassungsnehmer, bei dezentralen Produkten auf den Hersteller.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Leistungsbeschreibung) festgelegt und bekannt gegeben.

1.4 Abgrenzung des Dokumentes

Dieses Dokument macht keine Aussagen zur Aufteilung der Produktentwicklung bzw. Produktherstellung auf verschiedene Hersteller und Anbieter.

Dokumente zu den Zulassungsverfahren für den Produkttyp sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können der Homepage der gematik entnommen werden.

1.5 Methodik

Die im Dokument verzeichneten Anforderungen werden tabellarisch dargestellt. Die Tabellenspalten haben die folgende Bedeutung:

Afo-ID: Identifiziert die Anforderung eindeutig im Gesamtbestand aller Festlegungen der gematik.

Afo-Bezeichnung: Gibt den Titel einer Anforderung informativ wieder, um die thematische Einordnung zu erleichtern. Der vollständige Inhalt der Anforderung ist dem Dokument zu entnehmen, auf das die Quellenangabe verweist.

Quelle (Referenz): Verweist auf das Dokument, das die Anforderung definiert.

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Produkttyp normativen Anforderungen.

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion

Dokumenten Kürzel	Bezeichnung des Dokumentes	Version
gemSpec_SST_FD_VSDM	Schnittstellenspezifikation Fachdienste (UFS/VSDD/CMS)	1.6.0
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller	1.1.0
gemSpec_eGK_Fach_VSDM	Speicherstrukturen der eGK für die Fachanwendung VSDM	1.2.0
gemSpec_Systemprozesse_dezTI	Spezifikation Systemprozesse der dezentralen TI	1.2.0
gemSpec_TSL	Spezifikation TSL-Dienst	1.17.0
gemSpec_FLA_NFDM	Spezifikation Fachlogik der Fachanwendung NFDM in KTR-AdV (FLA-NFDM)	1.1.0
gemSpec_SST_VSDM	Schnittstellenspezifikation Transport VSDM	2.5.0
gemSpec_SST_PS_VSDM	Schnittstellenspezifikation Primärsysteme VSDM	1.5.0
gemSpec_FM_VSDM	Spezifikation Fachmodul VSDM	2.5.0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.13.0
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.8.0
gemSpec_KTR-AdV	Spezifikation KTR-AdV	1.6.0
gemKPT_Test	Testkonzept der TI	2.6.0
gemSpec_HSMProxy	Übergreifende Spezifikation HSM-Proxy	1.0.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.16.0
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	1.1.0

gemSpec_Net	Übergreifende Spezifikation Netzwerk	1.17.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.10.0

Errata

Neben den vorgenannten Dokumenten werden auf der Internetseite der gematik bei Bedarf Errata-Dokumente mit normativen Ergänzungen bzw. Korrekturen zu den Spezifikationsdokumenten veröffentlicht. Sofern in den Errata der vorliegende Produkttyp benannt wird, sind diese bei der Umsetzung des Produkttyps entsprechend der Vorgabe in der Dokumentenlandkarte zu berücksichtigen. Dabei kann eine abweichende Produkttypversion festgelegt werden.

3 Blattanforderungen

Die folgenden Abschnitte verzeichnen alle für den Produkttypen normativen Anforderungen, die für die Herstellung und den Betrieb von Produkten des Produkttyps notwendig sind (Blattanforderungen). Die Anforderungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der Zulassung, Zertifizierung bzw. Bestätigung.

3.1 Anforderungen zur funktionalen Eignung

3.1.1 Produkttest/Produktübergreifender Test

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Produkttyps verzeichnet, deren Umsetzung im Zuge von Zulassungstests durch die gematik geprüft wird.

Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
VSDM-A_2563	Fachmodul VSDM: Abbruch nach Timeout	gemSpec_FM_VSDM
VSDM-A_2597	Fachmodul VSDM: Aktualisierungsaufträge ermitteln	gemSpec_FM_VSDM
VSDM-A_2601	Fachmodul VSDM: Aktualisierungsaufträge durchführen	gemSpec_FM_VSDM
VSDM-A_2636	Fachmodul VSDM: Protokollierung im einheitlichen Format	gemSpec_FM_VSDM
VSDM-A_2638	Fachmodul VSDM: Felder im Ablaufprotokoll	gemSpec_FM_VSDM
VSDM-A_2649	Fachmodul VSDM: Protokolldateien begrenzen auf 180 Tage, Datenschutz	gemSpec_FM_VSDM
VSDM-A_2650	Fachmodul VSDM: Vorgangsnummer bilden	gemSpec_FM_VSDM
VSDM-A_2651	Fachmodul VSDM: Felder im Fehler-Protokoll	gemSpec_FM_VSDM
VSDM-A_2749	Fachmodul VSDM: zugehörige Nachrichten zum Fehler	gemSpec_FM_VSDM
VSDM-A_2752	Fachmodul VSDM: Aktualisierungsaufträge einzeln ausführen	gemSpec_FM_VSDM
VSDM-A_2789	Fachmodul VSDM: keine Protokollierung von Schlüsselmaterial	gemSpec_FM_VSDM
VSDM-A_2944	Fachmodul VSDM: Debugprotokoll schreiben	gemSpec_FM_VSDM

A_15112	AdV-Server, AdV-App: Beidseitiges Card-to-Card mit Flagliste Null	gemSpec_KTR-AdV
A_15115	AdV-Server, AdV-App: Einseitiges Card-to-Card mit CVC „KTR-AdV“	gemSpec_KTR-AdV
A_15118	CV-Zertifikat für PIN Status Prüfung	gemSpec_KTR-AdV
AdV-A_2416	TLS-Verbindung zwischen AdV-Server und AdV-App	gemSpec_KTR-AdV
AdV-A_2424	Speichern der ICCSN zur Fehleranalyse	gemSpec_KTR-AdV
AdV-A_2494	Handbuch: Liste unterstützter Kartenterminals	gemSpec_KTR-AdV
AdV-A_2514	CV-Zertifikat für eGK-Freischaltung	gemSpec_KTR-AdV
AdV-A_2516	X.509-Zertifikat für eGK-Protokolleintrag	gemSpec_KTR-AdV
AdV-A_2532	Freischaltung der eGK	gemSpec_KTR-AdV
AdV-A_2556	nachvollziehbarer eGK-Protokolleintrag mit Bezug zum Anbieter	gemSpec_KTR-AdV
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_3702	Inhalt der Selbstauskunft von Produkten außer Karten	gemSpec_OM
GS-A_4941	Betriebsdokumentation der dezentralen Produkte der TI-Plattform	gemSpec_OM
GS-A_5025	Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation	gemSpec_OM
GS-A_5034	Inhalte der Betriebsdokumentation der dezentralen Produkte der TI-Plattform	gemSpec_OM
GS-A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM
GS-A_5252	Generische Fehlermeldungen außerhalb von WebServices	gemSpec_OM
A_17700	TSL-Auswertung ServiceTypeIdentifier "unspecified"	gemSpec_PKI
A_17820	Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach RSA (ECC-Migration)	gemSpec_PKI

A_17821	Wechsel des Vertrauensraumes mittels Cross-Zertifikaten (ECC-Migration)	gemSpec_PKI
GS-A_4655	TUC_PKI_004: Mathematische Prüfung der Zertifikatssignatur	gemSpec_PKI
GS-A_4661	kritische Erweiterungen in Zertifikaten	gemSpec_PKI
GS-A_4662	Bedingungen für TLS-Handshake	gemSpec_PKI
GS-A_4751	Fehlercodes bei TSL- und Zertifikatsprüfung	gemSpec_PKI
VSDM-A_2682	Fachmodul VSDM: Keine sicherheitsrelevanten Informationen im Fehlermeldungen	gemSpec_SST_PS_VSDM
VSDM-A_2214	Fachmodul VSDM: HTTP-Fehlermeldungen verarbeiten	gemSpec_SST_VSDM
VSDM-A_2217	Fachmodul VSDM: Nachrichten grundsätzlich nicht speichern	gemSpec_SST_VSDM
VSDM-A_2956	Fachmodul VSDM: generische Fehlermeldungen	gemSpec_SST_VSDM

Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test" spezifisch für die AdV-App

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
NFDM-A_2390	Fehlermeldungen inkl. Trace	gemSpec_FLA_NFDM
NFDM-A_2391	Vorgaben spezifische Fehlermeldungen	gemSpec_FLA_NFDM
NFDM-A_2392	Unterstützte Generationen der eGK	gemSpec_FLA_NFDM
NFDM-A_2393	Verbot Protokollierung medizinischer Daten	gemSpec_FLA_NFDM
NFDM-A_2394	Verbot Protokollierung Schlüsselmaterial	gemSpec_FLA_NFDM
NFDM-A_2395	Verbot Protokollierung personenbezogener Daten	gemSpec_FLA_NFDM
NFDM-A_2396	Zugriffsprotokollierung auf der eGK	gemSpec_FLA_NFDM
NFDM-A_2397	Verbot der persistenten Speicherung medizinischer Daten	gemSpec_FLA_NFDM
NFDM-A_2399	Terminalanzeigen für PIN-Eingabe	gemSpec_FLA_NFDM
NFDM-A_2400	ReadDPE	gemSpec_FLA_NFDM

NFDM-A_2401	WriteDPE	gemSpec_FLA_NFDM
NFDM-A_2402	EraseDPE	gemSpec_FLA_NFDM
NFDM-A_2403	Operation GetData	gemSpec_FLA_NFDM
NFDM-A_2404	Operation PutData	gemSpec_FLA_NFDM
NFDM-A_2405	Trace ohne Implementierungsdetails	gemSpec_FLA_NFDM
A_15133	ReadVSDAdV: Sicherheitszustand vor Aktualisierung zurücksetzen	gemSpec_FM_VSDM
VSDM-A_2586	ReadVSD: Protokollierung VSD-Aktualisierung	gemSpec_FM_VSDM
VSDM-A_2602	Fachmodul VSDM: Reihenfolge der Abarbeitung der Aktualisierungsaufträge	gemSpec_FM_VSDM
VSDM-A_2603	Fachmodul VSDM: Separate Aktualisierungen für mehrere UpdateIds	gemSpec_FM_VSDM
VSDM-A_2606	Fachmodul VSDM: Abbruch aller weiteren Aktualisierungen bei Fehler in einer Aktualisierung	gemSpec_FM_VSDM
VSDM-A_2607	Fachmodul VSDM: alte Versionen der eGK	gemSpec_FM_VSDM
VSDM-A_2654	Fachmodul VSDM: Abbruch wenn Protokoll nicht auf eGK geschrieben	gemSpec_FM_VSDM
VSDM-A_2668	Fachmodul VSDM: Endpunkt-Adresse des Intermediärs bilden	gemSpec_FM_VSDM
VSDM-A_2687	Fachmodul VSDM: unterstützte Versionen der eGK	gemSpec_FM_VSDM
VSDM-A_2784	ReadVSD: GVD nicht aus dem Container EF.VD lesen	gemSpec_FM_VSDM
VSDM-A_2979	Fachmodul VSDM: unterstützte Versionen der VSDM Speicherstrukturen auf der eGK	gemSpec_FM_VSDM
VSDM-A_3034	ReadVSDAdV: VD, PD und Status-Container lesen	gemSpec_FM_VSDM
VSDM-A_3035	ReadVSDAdV: gesperrte Gesundheitsanwendung	gemSpec_FM_VSDM
VSDM-A_3036	ReadVSDAdV: AUT-Zertifikat der eGK offline ungültig	gemSpec_FM_VSDM
VSDM-A_3037	ReadVSDAdV: AUT-Zertifikat der eGK online ungültig	gemSpec_FM_VSDM

VSDM-A_3038	ReadVSDAdV: technischer Fehler	gemSpec_FM_VSDM
VSDM-A_3039	ReadVSDAdV: GVD in Antwort enthalten	gemSpec_FM_VSDM
VSDM-A_3040	ReadVSDAdV: Echtheitsprüfung eGK	gemSpec_FM_VSDM
VSDM-A_3041	ReadVSDAdV: Echtheitsprüfung SM-B	gemSpec_FM_VSDM
VSDM-A_3042	ReadVSDAdV: inkonsistente VSD	gemSpec_FM_VSDM
VSDM-A_3043	Fachmodul VSDM: ReadVSDAdV - Aktualisierungsaufträge ermitteln	gemSpec_FM_VSDM
VSDM-A_3044	ReadVSDAdV: Aktualisierung durchführen	gemSpec_FM_VSDM
VSDM-A_3045	ReadVSDAdV: Kein VSD lesen wenn Gesundheitsanwendung im Ablauf gesperrt wird	gemSpec_FM_VSDM
VSDM-A_3046	ReadVSDAdV: Protokollierung VSD-Aktualisierung	gemSpec_FM_VSDM
VSDM-A_3047	ReadVSDAdV: Protokollierung GVD Lesen	gemSpec_FM_VSDM
VSDM-A_3061	ReadVSDAdV: Fehlermeldung wenn Gesundheitsanwendung im Ablauf gesperrt wird	gemSpec_FM_VSDM
VSDM-A_3062	ReadVSDAdV: Keine Fehlermeldung wenn Gesundheitsanwendung im Ablauf entsperrt wird	gemSpec_FM_VSDM
VSDM-A_3063	Fachmodul VSDM: ReadVSDAdV - Werte für StatusVD in Antwortnachricht	gemSpec_FM_VSDM
VSDM-A_3065	ReadVSDAdV: Authentisierung des Versicherten	gemSpec_FM_VSDM
A_15110	AdV-App: TLS-Verbindung zum AdV-Server initiieren	gemSpec_KTR-AdV
A_16395	Kein TLS Session-Resumption und Renegotiation	gemSpec_KTR-AdV
AdV-A_2410	Abmeldung des Nutzers nach 5 Minuten Inaktivität	gemSpec_KTR-AdV
AdV-A_2423	AdV-App: Erzeugen von FehlerLog-Einträgen	gemSpec_KTR-AdV
AdV-A_2429	AdV-App: Ablaufprotokoll	gemSpec_KTR-AdV
AdV-A_2431	AdV-App: PerformanceLog	gemSpec_KTR-AdV
AdV-A_2433	AdV-App: DebugLog	gemSpec_KTR-AdV

AdV-A_2435	AdV-App: SecurityLog	gemSpec_KTR-AdV
AdV-A_2439	AdV-App: Erweiterte Loglevel zur Bezeichnung der Granularität des FehlerLog	gemSpec_KTR-AdV
AdV-A_2441	AdV-App: Art der Protokollierung	gemSpec_KTR-AdV
AdV-A_2443	AdV-App: Zugriff auf Protokolldateien	gemSpec_KTR-AdV
AdV-A_2444	AdV-App Fehlerverarbeitung	gemSpec_KTR-AdV
AdV-A_2445	AdV-App: Starten einer Sitzung	gemSpec_KTR-AdV
AdV-A_2446	AdV-App: Warnung eGK nicht ziehen	gemSpec_KTR-AdV
AdV-A_2447	AdV-App: Menüpunkt zum Beenden einer Sitzung	gemSpec_KTR-AdV
AdV-A_2448	AdV-App: Ziehen der eGK des Versicherten	gemSpec_KTR-AdV
AdV-A_2449	AdV-App: Beenden einer Sitzung in AdV-App	gemSpec_KTR-AdV
AdV-A_2450	AdV-App: Darstellung einer neutralen Anzeige	gemSpec_KTR-AdV
AdV-A_2451	AdV-App: Übergreifende Vorbedingung	gemSpec_KTR-AdV
AdV-A_2452	AdV-App: Zulässigkeit der Anwendungsfälle	gemSpec_KTR-AdV
AdV-A_2453	AdV-UC_14: Anwendung auf eGK deaktivieren	gemSpec_KTR-AdV
AdV-A_2454	AdV-UC_15: Anwendung auf eGK reaktivieren	gemSpec_KTR-AdV
AdV-A_2455	AdV-UC_03 „PIN für Fachanwendung einschalten“	gemSpec_KTR-AdV
AdV-A_2456	AdV-UC_04 Hinweis bei ausgeschaltetem PIN	gemSpec_KTR-AdV
AdV-A_2457	AdV-UC_04 „PIN für Fachanwendung ausschalten“	gemSpec_KTR-AdV
AdV-A_2458	AdV-UC_01: PIN ändern	gemSpec_KTR-AdV
AdV-A_2459	AdV-UC_02: PIN der eGK entsperren	gemSpec_KTR-AdV
AdV-A_2460	AdV-App: VSD von eGK anzeigen	gemSpec_KTR-AdV

AdV-A_2461	AdV-App: Decodierung von Schlüsselwerten im Zugriffsprotokoll	gemSpec_KTR-AdV
AdV-A_2462	AdV-App: Decodierung von Schlüsselwerten im Zugriffsprotokoll – Fachmodul	gemSpec_KTR-AdV
AdV-A_2463	AdV-App: Zugriffsprotokoll anzeigen	gemSpec_KTR-AdV
AdV-A_2464	AdV-App: Filtern von Protokolleinträgen	gemSpec_KTR-AdV
AdV-A_2465	AdV-App: Versicherten-PIN ändern	gemSpec_KTR-AdV
AdV-A_2466	AdV-App: Versicherten-PIN entsperren	gemSpec_KTR-AdV
AdV-A_2467	AdV-App: AdV-UC_02: Abbruch der AdV-Sitzung	gemSpec_KTR-AdV
AdV-A_2468	AdV-App: Hinweis bei verborgenem Notfalldatensatz	gemSpec_KTR-AdV
AdV-A_2469	AdV-App: NFD auf eGK verbergen	gemSpec_KTR-AdV
AdV-A_2470	AdV-App: Verborgene NFD auf eGK sichtbar machen	gemSpec_KTR-AdV
AdV-A_2471	AdV-App: PIN für NFD einschalten	gemSpec_KTR-AdV
AdV-A_2472	AdV-App: PIN für NFD ausschalten	gemSpec_KTR-AdV
AdV-A_2473	AdV-App: Hinweis bei verborgenem DPE	gemSpec_KTR-AdV
AdV-A_2474	AdV-App: DPE von eGK anzeigen	gemSpec_KTR-AdV
AdV-A_2475	AdV-App: Persönliche Erklärung (DPE) auf eGK ändern	gemSpec_KTR-AdV
AdV-A_2476	AdV-App: Persönliche Erklärung (DPE) auf eGK löschen	gemSpec_KTR-AdV
AdV-A_2477	AdV-App: PIN für DPE einschalten	gemSpec_KTR-AdV
AdV-A_2478	AdV-App: PIN für DPE ausschalten	gemSpec_KTR-AdV
AdV-A_2479	AdV-App: Datensatz Persönliche Erklärungen (DPE) auf eGK verbergen	gemSpec_KTR-AdV
AdV-A_2480	AdV-App: Verborgenen DPE auf eGK sichtbar machen	gemSpec_KTR-AdV
AdV-A_2481	AdV-App: AMTS-Vertreter-PIN ändern	gemSpec_KTR-AdV
AdV-A_2482	AdV-App: AMTS-Vertreter-PIN entsperren	gemSpec_KTR-AdV

AdV-A_2483	AdV-App: eMP/AMTS-Datensatz verbergen	gemSpec_KTR-AdV
AdV-A_2484	AdV-App: Verborgenen eMP/AMTS-Datensatz sichtbar machen	gemSpec_KTR-AdV
AdV-A_2485	AdV-App: PIN für AMTS einschalten	gemSpec_KTR-AdV
AdV-A_2486	AdV-App: PIN für AMTS ausschalten	gemSpec_KTR-AdV
AdV-A_2487	AdV-App: AdV-UC_25: „Mit eGK verschlüsseln“	gemSpec_KTR-AdV
AdV-A_2488	AdV-App: AdV-UC_26: „Mit eGK entschlüsseln“	gemSpec_KTR-AdV
AdV-A_2489	AdV-App: AdV-UC_27: „Authentisierungsrequest mit eGK signieren“	gemSpec_KTR-AdV
AdV-A_2490	AdV-App: AdV-UC_24: Zertifikat von eGK lesen	gemSpec_KTR-AdV
AdV-A_2492	Transportschnittstelle für Kartenkommandos	gemSpec_KTR-AdV
AdV-A_2493	Ergänzende Standards für Transportschnittstelle	gemSpec_KTR-AdV
AdV-A_2495	Klasse 1: PIN-Eingabe	gemSpec_KTR-AdV
AdV-A_2496	Klasse 1: PIN-Eingabe Geheimnis	gemSpec_KTR-AdV
AdV-A_2497	Klasse 1: PIN-Eingabe Eingabefeedback	gemSpec_KTR-AdV
AdV-A_2498	Klasse 1: PIN-Eingabe Eingabvalidierung	gemSpec_KTR-AdV
AdV-A_2500	Klasse 2: PIN-Eingabe	gemSpec_KTR-AdV
AdV-A_2502	Klasse 2: PIN-Eingabe Eingabefeedback	gemSpec_KTR-AdV
AdV-A_2503	Klasse 3: PIN-Eingabe	gemSpec_KTR-AdV
AdV-A_2505	Klasse 3: PIN-Eingabe Eingabefeedback	gemSpec_KTR-AdV
AdV-A_2535	Anzeige des Status eines PIN-Objekts	gemSpec_KTR-AdV
AdV-A_2547	Empfehlung: Hinweistext zu Fachanwendung	gemSpec_KTR-AdV
AdV-A_2548	Auswahl der zu kopierenden Daten durch den Versicherten	gemSpec_KTR-AdV

AdV-A_2549	Reaktion auf Kartenevents während Anwendungsfall Datenübertragung bei Kartentausch	gemSpec_KTR-AdV
AdV-A_2550	Aufrechterhaltung der Sitzung des Versicherten bei gezogener Karte während Anwendungsfall Datenübertragung bei Kartentausch	gemSpec_KTR-AdV
AdV-A_2551	Keine Neuansmeldung des Versicherten bei Stecken der eGK während Anwendungsfall Datenübertragung bei Kartentausch	gemSpec_KTR-AdV
AdV-A_2552	Anzeige einer Aufforderung zum Kartenwechsel	gemSpec_KTR-AdV
AdV-A_2553	AdV-App: Datenübertragung bei Kartentausch durchführen	gemSpec_KTR-AdV
AdV-A_2568	Warnung des Nutzers vor Abmeldung nach Inaktivität	gemSpec_KTR-AdV
GS-A_4384	TLS-Verbindungen	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_3816	Festlegung sicherheitsrelevanter Fehler	gemSpec_OM
GS-A_3856-02	Struktur der Fehlermeldungen	gemSpec_OM
GS-A_4547	Generische Fehlermeldungen	gemSpec_OM
VSDM-A_2318	Fachmodul VSDM: Kommando-APDUs unverändert durchreichen	gemSpec_SST_FD_VSDM
VSDM-A_2552	Fachmodul VSDM: Abbruch bei unerwarteten Statuscode	gemSpec_SST_FD_VSDM
VSDM-A_2690	Fachmodul VSDM: Fehlercode bei nicht konsistenten VSD	gemSpec_SST_PS_VSDM
VSDM-A_2692	Fachmodul VSDM: Lesen oder Dekomprimieren der VSD von der eGK scheitert	gemSpec_SST_PS_VSDM
VSDM-A_2982	Fachmodul VSDM: Fehlermeldung: SM-B nicht freigeschaltet	gemSpec_SST_PS_VSDM
VSDM-A_2973	Speicherstruktur des Containers EF.PD auf eGK	gemSpec_eGK_Fach_VSDM

VSDM-A_2974	Speicherstruktur des Containers EF.VD auf eGK	gemSpec_eGK_Fach_VSDM
VSDM-A_2975	Speicherstruktur des Containers EF.GVD auf eGK	gemSpec_eGK_Fach_VSDM
VSDM-A_2976	Speicherstruktur des Containers EF.StatusVD auf der eGK	gemSpec_eGK_Fach_VSDM

Tabelle 4: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test" spezifisch für den AdV-Server

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
VSDM-A_2565	Fachmodul VSDM: parallele Verarbeitung	gemSpec_FM_VSDM
VSDM-A_3007	Fachmodul VSDM: Ermitteln der URL des zugeordneten VSDM Intermediärs	gemSpec_FM_VSDM
A_15114	AdV-Server: Prüfung Status PIN.CH der eGK	gemSpec_KTR-AdV
AdV-A_2421	AdV-Server: Schnittstelle Internet - Ablehnung unzulässiger Verbindungen	gemSpec_KTR-AdV
AdV-A_2422	AdV-Server: Erzeugung von FehlerLog-Einträgen	gemSpec_KTR-AdV
AdV-A_2428	AdV-Server: Ablaufprotokoll	gemSpec_KTR-AdV
AdV-A_2430	AdV-Server: PerformanceLog	gemSpec_KTR-AdV
AdV-A_2432	AdV-Server: DebugLog	gemSpec_KTR-AdV
AdV-A_2434	AdV-Server: SecurityLog	gemSpec_KTR-AdV
AdV-A_2438	AdV-Server: Erweiterte Loglevel zur Bezeichnung der Granularität des FehlerLog	gemSpec_KTR-AdV
AdV-A_2440	AdV-Server: Art der Protokollierung	gemSpec_KTR-AdV
AdV-A_2515	X.509-Zertifikat für TLS-gesicherte Verbindung	gemSpec_KTR-AdV
AdV-A_2570	SM-B des Herausgebers der eGK verwenden	gemSpec_KTR-AdV
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_3832	DNS-Protokoll, Resolver-Implementierungen	gemSpec_Net
GS-A_3842	DNS, Verwendung von iterativen queries zwischen Nameservern	gemSpec_Net
GS-A_3930	Nameserver-Implementierungen, TTL	gemSpec_Net

GS-A_3931	DNSSEC-Protokoll, Nameserver-Implementierungen	gemSpec_Net
GS-A_3932	Abfrage der in der Topologie am nächsten stehenden Nameservers	gemSpec_Net
GS-A_3934	NTP-Client-Implementierungen, Protokoll NTPv4	gemSpec_Net
GS-A_3937	NTP-Client-Implementierungen, Association Mode und Polling Intervall	gemSpec_Net
GS-A_4036	Möglichkeit des Einsatzes von Hochverfügbarkeitsprotokollen	gemSpec_Net
GS-A_4763	Einsatz von Hochverfügbarkeitsprotokollen	gemSpec_Net
GS-A_4832	Path MTU Discovery und ICMP Response	gemSpec_Net
A_17688	Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)	gemSpec_PKI
A_17689	Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach ECC-RSA (ECC-Migration)	gemSpec_PKI
A_17690	Nutzung der Hash-Datei für TSL (ECC-Migration)	gemSpec_PKI
GS-A_4637	TUCs, Durchführung Fehlerüberprüfung	gemSpec_PKI
GS-A_4642	TUC_PKI_001: Periodische Aktualisierung TI-Vertrauensraum	gemSpec_PKI
GS-A_4643	TUC_PKI_013: Import TI-Vertrauensanker aus TSL	gemSpec_PKI
GS-A_4647	TUC_PKI_016: Download der TSL-Datei	gemSpec_PKI
GS-A_4648	TUC_PKI_019: Prüfung der Aktualität der TSL	gemSpec_PKI
GS-A_4649	TUC_PKI_020: XML-Dokument validieren	gemSpec_PKI
GS-A_4650	TUC_PKI_011: Prüfung des TSL-Signer-Zertifikates	gemSpec_PKI
GS-A_4651	TUC_PKI_012: XML-Signatur-Prüfung	gemSpec_PKI
GS-A_4652	TUC_PKI_018: Zertifikatsprüfung in der TI	gemSpec_PKI
GS-A_4653	TUC_PKI_002: Gültigkeitsprüfung des Zertifikats	gemSpec_PKI
GS-A_4654	TUC_PKI_003: CA-Zertifikat finden	gemSpec_PKI

GS-A_4656	TUC_PKI_005: Adresse für Status- und Sperrprüfung ermitteln	gemSpec_PKI
GS-A_4657	TUC_PKI_006: OCSP-Abfrage	gemSpec_PKI
GS-A_4660	TUC_PKI_009: Rollenermittlung	gemSpec_PKI
GS-A_4663	Zertifikats-Prüfparameter für den TLS-Handshake	gemSpec_PKI
GS-A_4749	TUC_PKI_007: Prüfung Zertifikatstyp	gemSpec_PKI
GS-A_4829	TUCs, Fehlerbehandlung	gemSpec_PKI
GS-A_4899	TSL Update-Prüfintervall	gemSpec_PKI
GS-A_4957	Beschränkungen OCSP-Request	gemSpec_PKI
GS-A_5077	FQDN-Prüfung beim TLS-Handshake	gemSpec_PKI
GS-A_5215	Festlegung der zeitlichen Toleranzen in einer OCSP-Response	gemSpec_PKI
GS-A_5336	Zertifikatsprüfung nach Ablauf TSL-Graceperiod	gemSpec_PKI
VSDM-A_2282	Fachmodul VSDM: RequestHeader bei Aufruf GetUpdateFlags	gemSpec_SST_FD_VSDM
VSDM-A_2285	Fachmodul VSDM: optionale Updates nicht ausführen	gemSpec_SST_FD_VSDM
VSDM-A_2298	Fachmodul VSDM: Sessioninformation für GetNextCommandPackage übernehmen	gemSpec_SST_FD_VSDM
VSDM-A_2303	Fachmodul VSDM: Request-Header bei Aufruf PerformUpdates	gemSpec_SST_FD_VSDM
VSDM-A_2308	Fachmodul VSDM: Operation PerformUpdates aufrufen	gemSpec_SST_FD_VSDM
VSDM-A_2310	Fachmodul VSDM: Operation GetUpdateFlags aufrufen	gemSpec_SST_FD_VSDM
VSDM-A_2311	Fachmodul VSDM: Operation GetNextCommandPackage aufrufen	gemSpec_SST_FD_VSDM
VSDM-A_2318	Fachmodul VSDM: Kommando-APDUs unverändert durchreichen	gemSpec_SST_FD_VSDM
VSDM-A_2321	Fachmodul VSDM: Request-Header bei Aufruf GetNextCommandPackage	gemSpec_SST_FD_VSDM
VSDM-A_2335	Fachmodul VSDM: AdditionalInfo nicht nutzen	gemSpec_SST_FD_VSDM

VSDM-A_2553	Fachmodul VSDM: Response bei unerwarteten Statuscode	gemSpec_SST_FD_VSDM
VSDM-A_3008	Fachmodul VSDM: Response bei Abbruch	gemSpec_SST_FD_VSDM
VSDM-A_2189	Fachmodul VSDM: WS-I Basic Profile in der Version 1.2 umsetzen	gemSpec_SST_VSDM
VSDM-A_2190	Fachmodul VSDM: Nachrichten konform zu WSDL- und Schemadateien	gemSpec_SST_VSDM
VSDM-A_2194	Fachmodul VSDM: mit TLS-Client X.509-Zertifikat authentifizieren	gemSpec_SST_VSDM
VSDM-A_2199	Fachmodul VSDM: HTTP-Komprimierung nutzen	gemSpec_SST_VSDM
VSDM-A_2200	Fachmodul VSDM: HTTP-Komprimierung unterstützen	gemSpec_SST_VSDM
VSDM-A_2202	Fachmodul VSDM: nur spezifizierte Header-Elemente	gemSpec_SST_VSDM
VSDM-A_2203	Fachmodul VSDM: keine Whitespaces	gemSpec_SST_VSDM
VSDM-A_2204	Fachmodul VSDM: Antwortnachrichten validieren	gemSpec_SST_VSDM
VSDM-A_2205	Fachmodul VSDM: invalide Antwortnachrichten erkennen	gemSpec_SST_VSDM
VSDM-A_2206	Fachmodul VSDM: auf zulässige Werte validieren	gemSpec_SST_VSDM
VSDM-A_2207	Fachmodul VSDM: Toleranz gegenüber zusätzlichen Elementen	gemSpec_SST_VSDM
VSDM-A_2209	Fachmodul VSDM: Endpunkt-Adresse mit Lokalisierungsinformation bilden	gemSpec_SST_VSDM
VSDM-A_2211	Fachmodul VSDM: Lokalisierungsinformationen gemäß dem Schema bilden	gemSpec_SST_VSDM
VSDM-A_2212	Fachmodul VSDM: Sessionformationen gemäß Schema bilden	gemSpec_SST_VSDM
VSDM-A_2213	Fachmodul VSDM: SOAP Faults ohne gematik-Fehlerstruktur verarbeiten	gemSpec_SST_VSDM
VSDM-A_2215	Fachmodul VSDM: Header-Feld "Via" auswerten	gemSpec_SST_VSDM
VSDM-A_2216	Fachmodul VSDM: gematik SOAP Faults verarbeiten	gemSpec_SST_VSDM

VSDM-A_2218	Fachmodul VSDM: Fehlermeldung speichern	gemSpec_SST_VSDM
VSDM-A_2219	Fachmodul VSDM: Anfragenachricht zu einer Fehlermeldung speichern	gemSpec_SST_VSDM
VSDM-A_2225	Fachmodul VSDM, Intermediär VSDM: TLS Session Resumption mittels Session-ID nutzen	gemSpec_SST_VSDM
VSDM-A_2226	Fachanwendung VSDM: Verbindung offen halten	gemSpec_SST_VSDM
VSDM-A_2235	Fachmodul VSDM: Trennzeichen in der URL	gemSpec_SST_VSDM
VSDM-A_2312	Fachmodul VSDM: Toleranz gegenüber nicht verarbeiteten Elementen	gemSpec_SST_VSDM
VSDM-A_3003	Verschlüsselter Transport durch Fachmodul VSDM	gemSpec_SST_VSDM
VSDM-A_3066	Fachmodul VSDM: Kein Pipelining	gemSpec_SST_VSDM
TIP1-A_5120	Clients des TSL-Dienstes: HTTP-Komprimierung unterstützen	gemSpec_TSL

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Produkttyps verzeichnet, deren durchgeführte bzw. geplante Umsetzung und Beachtung der Hersteller bzw. der Anbieter durch eine Herstellererklärung bestätigt bzw. zugesagt.

Tabelle 5: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_2162	Kryptographisches Material in Entwicklungs- und Testumgebungen	gemKPT_Test
TIP1-A_2805	Zeitnahe Anpassung von Produktkonfigurationen	gemKPT_Test
TIP1-A_4191	Keine Echtdaten in RU und TU	gemKPT_Test
TIP1-A_5052	Dauerhafte Verfügbarkeit in der RU	gemKPT_Test
TIP1-A_6079	Updates von Referenzobjekten	gemKPT_Test
TIP1-A_6080	Softwarestand von Referenzobjekten	gemKPT_Test
TIP1-A_6081	Bereitstellung der Referenzobjekte	gemKPT_Test

TIP1-A_6088	Unterstützung bei Fehlernachstellung	gemKPT_Test
TIP1-A_6093	Ausprägung der Referenzobjekte	gemKPT_Test
TIP1-A_6518	Eigenverantwortlicher Test: TDI	gemKPT_Test
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6523	Zulassungstest: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6524	Testdokumentation gemäß Vorlagen	gemKPT_Test
TIP1-A_6526	Produkttypen: Bereitstellung	gemKPT_Test
TIP1-A_6529	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	gemKPT_Test
TIP1-A_6532	Zulassung eines neuen Produkts: Aufgaben der TDI	gemKPT_Test
TIP1-A_6533	Zulassung eines neuen Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1-A_6536	Zulassung eines geänderten Produkts: Aufgaben der TDI	gemKPT_Test
TIP1-A_6537	Zulassung eines geänderten Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1-A_6772	Partnerprodukte bei Interoperabilitätstests	gemKPT_Test
TIP1-A_7335	Bereitstellung der Testdokumentation	gemKPT_Test
TIP1-A_7358	Qualität des Produktmusters	gemKPT_Test
VSDM-A_2635	Fachmodul VSDM: keine Protokollierung von medizinischen Daten	gemSpec_FM_VSDM
VSDM-A_2644	Fachmodul VSDM: Protokolldateien kopieren	gemSpec_FM_VSDM
VSDM-A_2649	Fachmodul VSDM: Protokolldateien begrenzen auf 180 Tage, Datenschutz	gemSpec_FM_VSDM

VSDM-A_2874	Fachmodul VSDM: keine Protokollierung von personenbezogenen Daten	gemSpec_FM_VSDM
AdV-A_2436	Verfügbarkeit interner Logdaten	gemSpec_KTR-AdV
AdV-A_2501	Klasse 2: PIN-Eingabe Fehlkonfiguration	gemSpec_KTR-AdV
AdV-A_2504	Klasse 3: PIN-Eingabe Fehlkonfiguration	gemSpec_KTR-AdV
AdV-A_2506	Übergabeschnittstelle PIN/PUK-Geheimnis	gemSpec_KTR-AdV
AdV-A_2507	Umsetzung ENV_TUC_SECRET_INPUT	gemSpec_KTR-AdV
AdV-A_2508	Transportschnittstelle für Card-2-Card	gemSpec_KTR-AdV
AdV-A_2510	Proxy-Funktion des Consumer Adapters für die AdV-App	gemSpec_KTR-AdV
AdV-A_2533	Kartenbezogene Benutzerrollen der KTR-AdV	gemSpec_KTR-AdV
AdV-A_2534	Ausführung von Anwendungsfällen mit lokalen Mitteln	gemSpec_KTR-AdV
AdV-A_2546	AdV-App: Sichere Verteilung	gemSpec_KTR-AdV
AdV-A_2555	Minimalprinzip Karteninteraktion	gemSpec_KTR-AdV
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	gemSpec_Krypt
A_17775	TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)	gemSpec_Krypt
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_3696	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM
GS-A_3697	Anlass der Erhöhung von Versionsnummern	gemSpec_OM
GS-A_3804	Eigenschaften eines FehlerLog-Eintrags	gemSpec_OM

GS-A_3807	Fehlerspeicherung ereignisgesteuerter Nachrichtenverarbeitung	gemSpec_OM
GS-A_3813	Datenschutzvorgaben Fehlermeldungen	gemSpec_OM
GS-A_4541	Nutzung der Produkttypversion zur Kompatibilitätsprüfung	gemSpec_OM
GS-A_4542	Spezifikationsgrundlage für Produkte	gemSpec_OM
GS-A_4864	Logging-Vorgaben nach dem Übergang zum Produktivbetrieb	gemSpec_OM
GS-A_5018	Sicherheitsrelevanter Fehler an organisatorischen Schnittstellen	gemSpec_OM
GS-A_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS-A_5039	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM
GS-A_4640	Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung	gemSpec_PKI
VSDM-A_2682	Fachmodul VSDM: Keine sicherheitsrelevanten Informationen im Fehlermeldungen	gemSpec_SST_PS_VSDM
VSDM-A_2217	Fachmodul VSDM: Nachrichten grundsätzlich nicht speichern	gemSpec_SST_VSDM
A_18072	Ablauf der Zertifikatsprüfung in der TI	gemSpec_Systemprozesse_dezTI
TIP1-A_6889	Eingabeschnittstelle für PIN	gemSpec_Systemprozesse_dezTI
TIP1-A_6890	Eingabeschnittstelle für PUK	gemSpec_Systemprozesse_dezTI
TIP1-A_6891	Eingabeschnittstelle für newPIN	gemSpec_Systemprozesse_dezTI
TIP1-A_6892	Umgebungsschnittstelle für Card-2-Card	gemSpec_Systemprozesse_dezTI
TIP1-A_6893	Umgebungsschnittstelle für Kartenkommandos	gemSpec_Systemprozesse_dezTI
TIP1-A_6894	Konfiguration des Kartenzugriffs	gemSpec_Systemprozesse_dezTI
TIP1-A_6895	Festlegung des Zugriffsprofils zur Rollenauthentisierung gegenüber einer eGK	gemSpec_Systemprozesse_dezTI

TIP1-A_6898	Leistung zu Statusinformationen zu einer Karte	gemSpec_Systemprozesse_dezTI
TIP1-A_6899	Liste verfügbarer Informationen zu einer SmartCard	gemSpec_Systemprozesse_dezTI
TIP1-A_6901	Prüfkriterien der Gültigkeit der eGK	gemSpec_Systemprozesse_dezTI
TIP1-A_6902	Prüfergebnis der Echtheit_und_Gültigkeit der eGK	gemSpec_Systemprozesse_dezTI
TIP1-A_6903	Leistung zur Änderung einer PIN	gemSpec_Systemprozesse_dezTI
TIP1-A_6904	Aufrufparameter zum Ändern einer PIN	gemSpec_Systemprozesse_dezTI
TIP1-A_6905	Ergebnis der Änderung einer PIN	gemSpec_Systemprozesse_dezTI
TIP1-A_6906	Leistung zum Einschalten einer PIN	gemSpec_Systemprozesse_dezTI
TIP1-A_6907	Aufrufparameter zum Einschalten einer PIN	gemSpec_Systemprozesse_dezTI
TIP1-A_6908	Ergebnis des Einschaltens einer PIN	gemSpec_Systemprozesse_dezTI
TIP1-A_6909	Leistung zum Abschalten einer PIN	gemSpec_Systemprozesse_dezTI
TIP1-A_6910	Aufrufparameter zum Abschalten einer PIN	gemSpec_Systemprozesse_dezTI
TIP1-A_6911	Ergebnis des Abschaltens einer PIN	gemSpec_Systemprozesse_dezTI
TIP1-A_6912	Leistung zum Entsperren einer PIN mittels PUK	gemSpec_Systemprozesse_dezTI
TIP1-A_6913	Aufrufparameter zum Entsperren einer PIN mittels PUK	gemSpec_Systemprozesse_dezTI
TIP1-A_6914	Ergebnis der Entsperrung einer PIN mittels PUK	gemSpec_Systemprozesse_dezTI
TIP1-A_6915	Leistung zur Benutzerverifikation	gemSpec_Systemprozesse_dezTI
TIP1-A_6916	Aufrufparameter der Benutzerverifikation	gemSpec_Systemprozesse_dezTI
TIP1-A_6917	Ergebnis der Leistung zur Eingabe einer PIN	gemSpec_Systemprozesse_dezTI
TIP1-A_6918	Leistung zum Aktivieren einer Anwendung	gemSpec_Systemprozesse_dezTI
TIP1-A_6919	Aufrufparameter zum Aktivieren einer Anwendung	gemSpec_Systemprozesse_dezTI

TIP1-A_6920	Ergebnis der Leistung zur Aktivieren einer Anwendung	gemSpec_Systemprozesse_dezTI
TIP1-A_6921	Leistung zum Deaktivieren einer Anwendung	gemSpec_Systemprozesse_dezTI
TIP1-A_6922	Aufrufparameter zum Deaktivieren einer Anwendung	gemSpec_Systemprozesse_dezTI
TIP1-A_6923	Ergebnis der Leistung zur Deaktivieren einer Anwendung	gemSpec_Systemprozesse_dezTI
TIP1-A_6924	Leistung zum Auslesen einer Zufallszahl	gemSpec_Systemprozesse_dezTI
TIP1-A_6925	Aufrufparameter für das Auslesen einer Zufallszahl	gemSpec_Systemprozesse_dezTI
TIP1-A_6926	Ergebnis des Auslesens einer Zufallszahl	gemSpec_Systemprozesse_dezTI
TIP1-A_6927	Leistung zum Lesen einer Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6928	Aufrufparameter für das Lesen einer Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6929	Optionale Parameter für das Lesen einer Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6930	Ergebnis des Lesens des Inhalts einer Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6931	Leistung zum Schreiben von Daten in eine transparente Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6932	Aufrufparameter für das Schreiben einer transparenten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6933	Ergebnis des Schreibens von Datei in eine transparente Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6934	Leistung zum Aktualisieren von Daten in einer transparenten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6935	Aufrufparameter zum Aktualisieren von Daten in einer transparenten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6936	Optionalen Parameter für das Aktualisieren von Datei in einer transparenten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6937	Ergebnis der Aktualisierung von Daten einer transparenten Datei	gemSpec_Systemprozesse_dezTI

TIP1-A_6938	Leistung des Löschsens einer transparenten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6939	Aufrufparameter zum Löschen einer transparenten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6940	Ergebnis der Löschoption einer transparenten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6941	Leistung zum Rücksetzen einer transparenten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6942	Aufrufparameter zum Rücksetzen einer transparenten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6943	Optionalen Parameter für das Rücksetzen des Inhalts einer transparenten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6944	Ergebnis des Rücksetzens einer transparenten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6945	Leistung zum Lesen einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6946	Aufrufparameter für das Lesen einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6947	Optionale Parameter für das Lesen einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6948	Ergebnis des Lesens einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6951	Leistung zum Schreiben von Daten in eine strukturierte Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6952	Aufrufparameter zum Schreiben von Daten in eine strukturierte Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6953	Ergebnis der Schreiboperation in einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6954	Leistung zum Anfügen von Daten in einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6955	Aufrufparameter zum Anfügen von Daten in einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6956	Ergebnis der Anfügeoperation in einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6958	Aufrufparameter der Zugriffsprotokollierung	gemSpec_Systemprozesse_dezTI

TIP1-A_6960	Leistung zum Löschen von Daten in einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6961	Aufrufparameter zum Löschen von Daten in einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6962	Optionale Parameter für das Löschen von Daten einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6963	Ergebnis der Löschoperation in einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6964	Leistung zum Rücksetzen eines Datensatzes in einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6965	Aufrufparameter zum Rücksetzen eines Datensatzes in einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6966	Ergebnis des Rücksetzens eines Datensatzes in einer strukturierten Datei	gemSpec_Systemprozesse_dezTI
TIP1-A_6967	Leistung zum Öffnen eines transparenten Kanals	gemSpec_Systemprozesse_dezTI
TIP1-A_6968	Ergebnis des Öffnens eines transparenten Kanals	gemSpec_Systemprozesse_dezTI
TIP1-A_6969	Leistung der transparenten Kommunikation zur Karte	gemSpec_Systemprozesse_dezTI
TIP1-A_6970	Aufrufparameter zur transparenten Kommunikation zur Karte	gemSpec_Systemprozesse_dezTI
TIP1-A_6971	Ergebnis der transparenten Kommunikation zur Karte	gemSpec_Systemprozesse_dezTI
TIP1-A_6972	Leistung zum Schließen eines transparenten Kanals	gemSpec_Systemprozesse_dezTI
TIP1-A_6973	Ergebnis des Schließens eines transparenten Kanals	gemSpec_Systemprozesse_dezTI
TIP1-A_6974	Leistung zur TLS-Verbindung mit gegenseitiger Authentisierung	gemSpec_Systemprozesse_dezTI
TIP1-A_6975	Aufrufparameter zur TLS-Verbindung mit gegenseitiger Authentisierung	gemSpec_Systemprozesse_dezTI
TIP1-A_6976	Aufbau der TLS-Verbindung mit gegenseitiger Authentisierung	gemSpec_Systemprozesse_dezTI
TIP1-A_6977	Auflösen von URI in IP-Adresse	gemSpec_Systemprozesse_dezTI

TIP1-A_6979	Leistung der nonQES-Signatur	gemSpec_Systemprozesse_dezTI
TIP1-A_6980	Aufrufparameter der nonQES-Signatur	gemSpec_Systemprozesse_dezTI
TIP1-A_6981	Ergebnis der nonQES-Signatur	gemSpec_Systemprozesse_dezTI
TIP1-A_6982	Leistung zum hybriden Verschlüsseln	gemSpec_Systemprozesse_dezTI
TIP1-A_6983	Aufrufparameter zum hybriden Verschlüsseln	gemSpec_Systemprozesse_dezTI
TIP1-A_6984	Ablauf der hybriden Verschlüsselung eines Dokuments	gemSpec_Systemprozesse_dezTI
TIP1-A_6985	Leistung zum hybriden Entschlüsseln	gemSpec_Systemprozesse_dezTI
TIP1-A_6986	Aufrufparameter zum hybriden Entschlüsseln	gemSpec_Systemprozesse_dezTI
TIP1-A_6987	Ablauf der hybriden Entschlüsselung eines Dokuments	gemSpec_Systemprozesse_dezTI
TIP1-A_6991	Leistung zur Prüfung eines Zertifikats in der TI	gemSpec_Systemprozesse_dezTI
TIP1-A_6992	Aufrufparameter der Zertifikatsprüfung in der TI	gemSpec_Systemprozesse_dezTI
TIP1-A_6993	Ergebnis der Zertifikatsprüfung in der TI	gemSpec_Systemprozesse_dezTI
TIP1-A_7017	Statusinformationen im Rahmen der PIN-Verifikation	gemSpec_Systemprozesse_dezTI
TIP1-A_7018	Statusinformationen im Rahmen von Card-2-Card	gemSpec_Systemprozesse_dezTI
TIP1-A_7019	Konfiguration der Rollen des Benutzers einer Karte	gemSpec_Systemprozesse_dezTI
TIP1-A_7020	Leistung zum Rücksetzen einer Karte	gemSpec_Systemprozesse_dezTI

Tabelle 6: Anforderungen zur funktionalen Eignung "Herstellererklärung" spezifisch für die AdV-App

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_6087	Zugang zur Adminschnittstelle bei dezentralen Produkten	gemKPT_Test
A_15111	AdV-App: Institutskennzeichen an AdV-Server senden	gemSpec_KTR-AdV

AdV-A_2437	AdV-App: Kein Logging auf Geräten des Versicherten	gemSpec_KTR-AdV
AdV-A_2572	AdV-App: interner Truststore	gemSpec_KTR-AdV
TIP1-A_6896	Initialisierung CardProxy für eGK	gemSpec_Systemprozesse_dezTI
TIP1-A_6949	Leistung zum Lesen des Zugriffprotokolls auf der eGK	gemSpec_Systemprozesse_dezTI
TIP1-A_6950	Ergebnis des Auslesens des Zugriffprotokolls der eGK	gemSpec_Systemprozesse_dezTI
TIP1-A_6957	Leistung zum Protokollieren des eGK-Zugriffs	gemSpec_Systemprozesse_dezTI
TIP1-A_6959	Hinzufügen eines Protokolleintrags auf die eGK	gemSpec_Systemprozesse_dezTI
TIP1-A_6996	Aufbereitung Zugriffsprotokolleinträge	gemSpec_Systemprozesse_dezTI

Tabelle 7: Anforderungen zur funktionalen Eignung "Herstellererklärung" spezifisch für den AdV-Server

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
AdV-A_2509	Kapselung der Zugriffe auf Dienste der zentralen TI-Plattform	gemSpec_KTR-AdV
GS-A_4013	Nutzung von UDP/TCP-Portbereichen	gemSpec_Net
GS-A_4024	Nutzung IP-Adressbereiche	gemSpec_Net
GS-A_4033	Statisches Routing TI-Übergabepunkte	gemSpec_Net
GS-A_4646	TUC_PKI_017: Lokalisierung TSL Download-Adressen	gemSpec_PKI
GS-A_4898	TSL-Grace-Period einer TSL	gemSpec_PKI
GS-A_5506	Performance – AdV-Server – Verfügbarkeit	gemSpec_Perf
VSDM-A_2208	Fachmodul VSDM: beliebige Reihenfolge der Header-Elemente	gemSpec_SST_VSDM
TIP1-A_6897	Initialisierung CardProxy für SM-B	gemSpec_Systemprozesse_dezTI
TIP1-A_6978	Synchronisierung mit Zeitdienst	gemSpec_Systemprozesse_dezTI

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 CC-Evaluierung

Eine Zertifizierung nach ITSEC [ITSEC] oder Common Criteria ist nicht erforderlich.

Tabelle 8: Anforderungen zur sicherheitstechnischen Eignung "CC-Evaluierung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Es liegen keine Anforderungen vor	

3.2.2 Sicherheitsgutachten

Die in diesem Abschnitt verzeichneten Anforderungen sind Gegenstand der Prüfung der Sicherheitseignung gemäß [gemRL_PruefSichEig]. Das entsprechende Sicherheitsgutachten ist der gematik vorzulegen.

Tabelle 9: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" spezifisch für den AdV-Server

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_2076-01	kDSM: Datenschutzmanagement nach BSI	gemSpec_DS_Anbieter
GS-A_2158-01	Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen	gemSpec_DS_Anbieter
GS-A_2214-01	kDSM: Anbieter müssen jährlich die Auftragsverarbeiter kontrollieren	gemSpec_DS_Anbieter
GS-A_2328-01	Pflege und Fortschreibung des Sicherheitskonzeptes und Notfallkonzeptes	gemSpec_DS_Anbieter
GS-A_2329-01	Umsetzung der Sicherheitskonzepte	gemSpec_DS_Anbieter
GS-A_2331-01	Sicherheitsvorfalls-Management	gemSpec_DS_Anbieter
GS-A_2332-01	Notfallmanagement	gemSpec_DS_Anbieter
GS-A_2345-01	regelmäßige Reviews	gemSpec_DS_Anbieter
GS-A_3737-01	Sicherheitskonzept	gemSpec_DS_Anbieter
GS-A_3753-01	Notfallkonzept	gemSpec_DS_Anbieter
GS-A_3772-01	Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen	gemSpec_DS_Anbieter
GS-A_4980-01	Umsetzung der Norm ISO/IEC 27001	gemSpec_DS_Anbieter

GS-A_4981-01	Erreichen der Ziele der Norm ISO/IEC 27001 Annex A	gemSpec_DS_Anbieter
GS-A_4982-01	Umsetzung der Maßnahmen der Norm ISO/IEC 27002	gemSpec_DS_Anbieter
GS-A_4983-01	Umsetzung der Maßnahmen aus dem BSI-Grundschutz	gemSpec_DS_Anbieter
GS-A_4984-01	Befolgen von herstellerspezifischen Vorgaben	gemSpec_DS_Anbieter
GS-A_5551	Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR	gemSpec_DS_Anbieter
GS-A_5557	Security Monitoring	gemSpec_DS_Anbieter
GS-A_5558	Aktive Schwachstellenscans	gemSpec_DS_Anbieter
GS-A_5626	kDSM: Auftragsverarbeitung	gemSpec_DS_Anbieter
VSDM-A_2637	Fachmodul VSDM: Zugriff nur für autorisierte Personen	gemSpec_FM_VSDM
VSDM-A_2789	Fachmodul VSDM: keine Protokollierung von Schlüsselmaterial	gemSpec_FM_VSDM
A_16395	Kein TLS Session-Resumption und Renegotiation	gemSpec_KTR-AdV
AdV-A_2407	Keine persistente Speicherung von Daten des Versicherten	gemSpec_KTR-AdV
AdV-A_2409	Löschen der Daten nach Abmeldung	gemSpec_KTR-AdV
AdV-A_2411	Keine Protokollierung medizinischer Daten	gemSpec_KTR-AdV
AdV-A_2412	Keine Protokollierung personenbezogener Daten	gemSpec_KTR-AdV
AdV-A_2416	TLS-Verbindung zwischen AdV-Server und AdV-App	gemSpec_KTR-AdV
AdV-A_2426	Löschen der ICCSN aus Fehlerprotokoll	gemSpec_KTR-AdV
AdV-A_2442	AdV-Server: Zugriff auf Protokolldateien	gemSpec_KTR-AdV
AdV-A_2513	Privates Schlüsselmaterial in HSM speichern	gemSpec_KTR-AdV
AdV-A_2575	Personalisierung des HSMs	gemSpec_KTR-AdV
GS-A_4359	X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt

GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_4379	Card-to-Card-Authentisierung G2	gemSpec_Krypt
GS-A_4384	TLS-Verbindungen	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	gemSpec_Krypt
GS-A_5339	TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität	gemSpec_Krypt
GS-A_4641	Initiale Einbringung TI-Vertrauensanker	gemSpec_PKI
GS-A_4748	Initiale Einbringung TSL-Datei	gemSpec_PKI
GS-A_4943	Alter der OCSP-Responses für eGK-Zertifikate	gemSpec_PKI

3.2.3 Herstellererklärung sicherheitstechnische Eignung

Sofern in diesem Abschnitt Anforderungen verzeichnet sind, muss der Hersteller bzw. der Anbieter deren Umsetzung und Beachtung zum Nachweis der sicherheitstechnischen Eignung durch eine Herstellererklärung bestätigen bzw. zusagen.

Tabelle 10: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung" spezifisch für die AdV-App

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_17178	Produktentwicklung: Basisschutz gegen OWASP Top 10 Risiken	gemSpec_DS_Hersteller
A_17179	Auslieferung aktueller zusätzlicher Softwarekomponenten	gemSpec_DS_Hersteller
GS-A_2330-02	Hersteller: Schwachstellen-Management	gemSpec_DS_Hersteller
GS-A_2350-01	Produktunterstützung der Hersteller	gemSpec_DS_Hersteller
GS-A_2354-01	Produktunterstützung mit geeigneten Sicherheitstechnologien	gemSpec_DS_Hersteller
GS-A_2524-01	Produktunterstützung: Nutzung des Problem-Management-Prozesses	gemSpec_DS_Hersteller
GS-A_2525-01	Hersteller: Schließen von Schwachstellen	gemSpec_DS_Hersteller

GS-A_4944-01	Produktentwicklung: Behebung von Sicherheitsmängeln	gemSpec_DS_Hersteller
GS-A_4945-01	Produktentwicklung: Qualitätssicherung	gemSpec_DS_Hersteller
GS-A_4946-01	Produktentwicklung: sichere Programmierung	gemSpec_DS_Hersteller
GS-A_4947-01	Produktentwicklung: Schutz der Vertraulichkeit und Integrität	gemSpec_DS_Hersteller
AdV-A_2405	AdV-App: Betrieb in KTR-AdV-Terminal	gemSpec_KTR-AdV
AdV-A_2414	AdV-App: Bereitstellen von Softwareaktualisierungen	gemSpec_KTR-AdV
AdV-A_2499	PIN-Eingabe nicht speichern	gemSpec_KTR-AdV
AdV-A_2511	Separierung der AdV-App von Diensten der TI	gemSpec_KTR-AdV
AdV-A_2562	PIN-Geheimnis ausschließlich an Karte übermitteln	gemSpec_KTR-AdV

Tabelle 11: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung" spezifisch für den AdV-Server

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_2355-01	Meldung von erheblichen Schwachstellen und Bedrohungen	gemSpec_DS_Anbieter
GS-A_4473-01	kDSM: Unverzügliche Benachrichtigung bei Verstößen gemäß Art. 34 DSGVO	gemSpec_DS_Anbieter
GS-A_4478-01	kDSM: Nachweis der Umsetzung von Maßnahmen in Folge eines gravierenden Datenschutzverstoßes	gemSpec_DS_Anbieter
GS-A_4479-01	kDSM: Meldung von Änderungen der Kontaktinformationen zum Datenschutzmanagement	gemSpec_DS_Anbieter
GS-A_4523-01	Bereitstellung Kontaktinformationen für Informationssicherheit	gemSpec_DS_Anbieter
GS-A_4524-01	Meldung von Änderungen der Kontaktinformationen für Informationssicherheit	gemSpec_DS_Anbieter
GS-A_4526-01	Aufbewahrungsvorgaben an die Nachweise zu Sicherheitsmeldungen	gemSpec_DS_Anbieter

GS-A_4530-01	Maßnahmen zur Behebung von erheblichen Sicherheitsvorfällen und Notfällen	gemSpec_DS_Anbieter
GS-A_4532-01	Nachweis der Umsetzung von Maßnahmen in Folge eines erheblichen Sicherheitsvorfalls oder Notfalls	gemSpec_DS_Anbieter
GS-A_5017-01	Meldung und Behandlung von Schwachstellen	gemSpec_DS_Anbieter
GS-A_5324-01	Teilnahme des Anbieters an Sitzungen des kISMS	gemSpec_DS_Anbieter
GS-A_5324-02	kDSM: Teilnahme des Anbieters an Sitzungen des kDSM	gemSpec_DS_Anbieter
GS-A_5555	Unverzögliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_5556	Unverzögliche Behebung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_5559	Bereitstellung Ergebnisse von Schwachstellenscans	gemSpec_DS_Anbieter
GS-A_5560	Entgegennahme und Prüfung von Meldungen der gematik	gemSpec_DS_Anbieter
GS-A_5561	Bereitstellung 24/7-Kontaktpunkt	gemSpec_DS_Anbieter
GS-A_5562	Bereitstellung Produktinformationen	gemSpec_DS_Anbieter
GS-A_5563	Jahressicherheitsbericht	gemSpec_DS_Anbieter
GS-A_5564	kDSM: Ansprechpartner für Datenschutz	gemSpec_DS_Anbieter
GS-A_5565	kDSM: Unverzögliche Behebung von Verstößen gemäß Art. 34 DSGVO	gemSpec_DS_Anbieter
GS-A_5566	kDSM: Sicherstellung der Datenschutzanforderungen in Unterbeauftragungsverhältnissen	gemSpec_DS_Anbieter
GS-A_5624	Auditrechte der gematik zur Informationssicherheit	gemSpec_DS_Anbieter
GS-A_5625	kDSM: Auditrechte der gematik zum Datenschutz	gemSpec_DS_Anbieter
AdV-A_2413	AdV-Server: Keine unberechtigten Zugriffe	gemSpec_KTR-AdV

3.2.4 Zertifizierung nach Technischer Richtlinie

In diesem Abschnitt sind Anforderungen verzeichnet, deren Umsetzung im Zuge einer Prüfung gemäß Technischer Richtlinie [TR-03158] nachgewiesen werden muss. Der Nachweis erfolgt durch die Vorlage des Zertifikates nach [TR-03158].

Tabelle 12: Anforderungen zur sicherheitstechnischen Eignung "Zertifizierung nach Technischer Richtlinie" spezifisch für die AdV-App

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
NFDM-A_2393	Verbot Protokollierung medizinischer Daten	gemSpec_FLA_NFDM
NFDM-A_2394	Verbot Protokollierung Schlüsselmaterial	gemSpec_FLA_NFDM
NFDM-A_2395	Verbot Protokollierung personenbezogener Daten	gemSpec_FLA_NFDM
NFDM-A_2396	Zugriffsprotokollierung auf der eGK	gemSpec_FLA_NFDM
NFDM-A_2397	Verbot der persistenten Speicherung medizinischer Daten	gemSpec_FLA_NFDM
NFDM-A_2399	Terminalanzeigen für PIN-Eingabe	gemSpec_FLA_NFDM
VSDM-A_2586	ReadVSD: Protokollierung VSD-Aktualisierung	gemSpec_FM_VSDM
VSDM-A_2789	Fachmodul VSDM: keine Protokollierung von Schlüsselmaterial	gemSpec_FM_VSDM
A_15110	AdV-App: TLS-Verbindung zum AdV-Server initiieren	gemSpec_KTR-AdV
A_15113	AdV-App: Flaglist prüfen	gemSpec_KTR-AdV
A_15116	AdV-App: Abbruch bei Fehler im Verbindungsaufbau und Freischaltung eGK	gemSpec_KTR-AdV
A_15117	AdV-App: Ablehnen von Kartenkommandos	gemSpec_KTR-AdV
AdV-A_2407	Keine persistente Speicherung von Daten des Versicherten	gemSpec_KTR-AdV
AdV-A_2409	Löschen der Daten nach Abmeldung	gemSpec_KTR-AdV
AdV-A_2411	Keine Protokollierung medizinischer Daten	gemSpec_KTR-AdV
AdV-A_2412	Keine Protokollierung personenbezogener Daten	gemSpec_KTR-AdV
AdV-A_2415	AdV-App: Vertrauliche PIN-Eingabe erlauben	gemSpec_KTR-AdV
AdV-A_2416	TLS-Verbindung zwischen AdV-Server und AdV-App	gemSpec_KTR-AdV
AdV-A_2417	AdV-App: lokaler Truststore	gemSpec_KTR-AdV

AdV-A_2418	AdV-App: unzulässige TLS-Verbindungen ablehnen	gemSpec_KTR-AdV
AdV-A_2426	Löschen der ICCSN aus Fehlerprotokoll	gemSpec_KTR-AdV
AdV-A_2443	AdV-App: Zugriff auf Protokolldateien	gemSpec_KTR-AdV
AdV-A_2499	PIN-Eingabe nicht speichern	gemSpec_KTR-AdV
AdV-A_2562	PIN-Geheimnis ausschließlich an Karte übermitteln	gemSpec_KTR-AdV
AdV-A_2573	AdV-App: Initialisierung und Aktualisierung des TLS-Vertrauensankers	gemSpec_KTR-AdV
GS-A_4357	X.509-Identitäten für die Erstellung und Prüfung digitaler nicht-qualifizierter elektronischer Signaturen	gemSpec_Krypt
GS-A_4359	X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	gemSpec_Krypt
GS-A_4361	X.509-Identitäten für die Erstellung und Prüfung digitaler Signaturen	gemSpec_Krypt
GS-A_4362	X.509-Identitäten für Verschlüsselungszertifikate	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_4370	Kryptographische Algorithmen für XML-Dokumente	gemSpec_Krypt
GS-A_4371	XML-Signaturen für nicht-qualifizierte Signaturen	gemSpec_Krypt
GS-A_4374	XML-Verschlüsselung - Hybrid	gemSpec_Krypt
GS-A_4376-02	XML-Verschlüsselung - Hybrid, Schlüsseltransport RSAES-OAEP	gemSpec_Krypt
GS-A_4384	TLS-Verbindungen	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_4388	DNSSEC-Kontext	gemSpec_Krypt
GS-A_4389	Symmetrischer Anteil der hybriden Verschlüsselung binärer Daten	gemSpec_Krypt

GS-A_4390	Asymmetrischer Anteil der hybriden Verschlüsselung binärer Daten	gemSpec_Krypt
GS-A_4393	Algorithmus bei der Erstellung von Hashwerten von Zertifikaten oder öffentlichen Schlüsseln	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_5131	Hash-Algorithmus bei OCSP/CertID	gemSpec_Krypt
GS-A_5339	TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität	gemSpec_Krypt
GS-A_4943	Alter der OCSP-Responses für eGK-Zertifikate	gemSpec_PKI

3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

Der Produkttyp erfordert den Nachweis der elektrischen, mechanischen und physikalischen Eignung. Sofern dabei spezifische Anforderungen der gematik zu beachten sind, werden diese nachfolgend aufgeführt. Der Nachweis erfolgt durch die Vorlage des Prüfberichts.

Tabelle 13: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Es liegen keine Anforderungen vor	

4 Produkttypspezifische Merkmale

4.1 Optionale Ausprägungen

In diesem Kapitel werden die optional zu erfüllenden Anforderungen in Tabelle 14 aufgeführt.

Tabelle 14: Optionale Anforderungen („KANN-Anforderungen“)

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
VSDM-A_2944	Fachmodul VSDM: Debugprotokoll schreiben	gemSpec_FM_VSDM
A_18467	TLS-Verbindungen, Version 1.3	gemSpec_Krypt
AdV-A_2432	AdV-Server: DebugLog	gemSpec_KTR-AdV
AdV-A_2433	AdV-App: DebugLog	gemSpec_KTR-AdV
AdV-A_2434	AdV-Server: SecurityLog	gemSpec_KTR-AdV
AdV-A_2435	AdV-App: SecurityLog	gemSpec_KTR-AdV
AdV-A_2487	AdV-App: AdV-UC_25: „Mit eGK verschlüsseln“	gemSpec_KTR-AdV
AdV-A_2488	AdV-App: AdV-UC_26: „Mit eGK entschlüsseln“	gemSpec_KTR-AdV
AdV-A_2489	AdV-App: AdV-UC_27: „Authentisierungsrequest mit eGK signieren“	gemSpec_KTR-AdV
AdV-A_2490	AdV-App: AdV-UC_24: „Zertifikat von eGK lesen“	gemSpec_KTR-AdV
AdV-A_2493	Ergänzende Standards für Transportschnittstelle	gemSpec_KTR-AdV
AdV-A_2553	AdV-App: Datenübertragung bei Kartentausch durchführen	gemSpec_KTR-AdV
AdV-A_2568	Warnung des Nutzers vor Abmeldung nach Inaktivität	gemSpec_KTR-AdV

GS-A_4036	Möglichkeit des Einsatzes von Hochverfügbarkeitsprotokollen	gemSpec_Net
GS-A_5040	Änderung der Produktversion bei Produktänderungen außerhalb von Produkttypänderungen	gemSpec_OM
GS-A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM
A_17689	Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach ECC-RSA (ECC-Migration)	gemSpec_PKI
A_17690	Nutzung der Hash-Datei für TSL (ECC-Migration)	gemSpec_PKI
A_17820	Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach RSA (ECC-Migration)	gemSpec_PKI

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

5.2 Tabellenverzeichnis

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion	6
Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"	8
Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test" spezifisch für die AdV-App	10
Tabelle 4: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test" spezifisch für den AdV-Server	17
Tabelle 5: Anforderungen zur funktionalen Eignung "Herstellererklärung"	21
Tabelle 6: Anforderungen zur funktionalen Eignung "Herstellererklärung" spezifisch für die AdV-App	29
Tabelle 7: Anforderungen zur funktionalen Eignung "Herstellererklärung" spezifisch für den AdV-Server.....	30
Tabelle 8: Anforderungen zur sicherheitstechnischen Eignung "CC-Evaluierung"	31
Tabelle 9: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" spezifisch für den AdV-Server	31
Tabelle 10: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung" spezifisch für die AdV-App	33
Tabelle 11: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung" spezifisch für den AdV-Server	34
Tabelle 12: Anforderungen zur sicherheitstechnischen Eignung "Zertifizierung nach Technischer Richtlinie" spezifisch für die AdV-App.....	36
Tabelle 13: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung	38
Tabelle 14: Optionale Anforderungen („KANN-Anforderungen“)	39

5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[CC]	Internationaler Standard: Common Criteria for Information Technology Security Evaluation https://www.commoncriteriaportal.org/cc/
[gemRL_PruefSichEig]	gematik: Richtlinie zur Prüfung der Sicherheitseignung
[TR-03158]	Technische Richtlinie BSI TR-03158 Anwendungen des Versicherten - AdV-App