Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
KTR-AdV-Terminal

Version:	1.3.0
Revision:	241927
Stand:	30.06.2020
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_KTR-AdV-Terminal

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	05.10.17		initiale Erstellung des Dokuments	gematik
1.1.0	20.02.18		Einarbeitung P15.1	gematik
1.2.0	14.05.18		freigegeben	gematik
1.3.0	30.06.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes 4
1.1 Zielsetzung 4
1.2 Zielgruppe 4
1.3 Geltungsbereich 4
1.4 Abgrenzungen 4
1.5 Methodik 4
2 Systemüberblick 6
3 Systemkontext 8
3.1 Rollen 8
3.2 Nachbarsysteme 8
4 Zerlegung des Produkttyps 10
5 Funktionsmerkmale 11
6 Datenschutz- und Sicherheitsanforderungen 12
6.1 Datenschutz- und Sicherheitsanforderungen an die Hardware 12
6.2 Datenschutz- und Sicherheitsanforderungen an die Plattform 12
6.3 Sicherheitsanforderungen an Hersteller 15
6.4 ePA-spezifische Sicherheitsanforderungen 17
7 Informationsmodell 18
8 Verteilungssicht 19
9 Anhang A – Verzeichnisse 20
9.1 Abkürzungen 20
9.2 Glossar 20
9.3 Abbildungsverzeichnis 20
9.4 Tabellenverzeichnis 20
9.5 Referenzierte Dokumente 21
9.5.1 Dokumente der gematik 21
9.5.2 Weitere Dokumente 21

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert Anforderungen an den Produkttyp KTR-AdV-Terminal.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller eines KTR-AdV-Terminals.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens für den Online-Produktivbetrieb (Stufe 2.1). Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

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

1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:

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

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

2 Systemüberblick

Die **Anwendungen des Versicherten** (AdV) sind Anwendungsfälle, die Versicherte selbstständig ausführen können und mit denen sie ihre datenschutzrechtlichen Betroffenenrechte und ihre gesetzlich zustehenden Zugriffsrechte für die Anwendungen der TI wahrnehmen können. AdV-Anwendungsfälle können anwendungsunabhängig (z.B. PIN-Verwaltung auf der eGK) oder anwendungsspezifisch sein (z.B. Verwaltung der ePA).

Im Folgenden bezeichnen **AdV-Clients** Software-Clients, mit denen Versicherte über eine Benutzeroberfläche AdV-Anwendungsfälle bzgl. Anwendungen der TI nutzen können. AdV-Clients der TI werden von der gematik als eigener Produkttyp der TI oder als Teil eines Produkttyps der TI zugelassen. Beispiele von AdV-Clients der TI sind:

- **AdV-App**: Die AdV-App ist Teil des Produkttyps KTR-AdV [gemProdT_KTR-AdV_PTV]. Die Funktionen der AdV-App sind in [gemSpec_KTR-AdV] beschrieben.
- **ePA-FdV AdV**: Das ePA Frontend des Versicherten für das KTR-AdV-Terminal (ePA-FdV AdV) ist ein eigener Produkttyp [gemProdT_ePA_FdV_AdV_PTV]. Die Funktionen des ePA-FdV AdV sind in [gemSpec_Frontend_Vers_AdV] beschrieben.

Das **KTR-AdV-Terminal** ist Teil der AdV-Lösung für Versicherte in der TI und bietet eine Ablaufumgebung für AdV-Clients. Mit dem KTR-AdV-Terminal können insbesondere auch Versicherte AdV-Clients nutzen, die keine eigene IT für die Ausführung von AdV-Clients haben.

Der Produkttyp KTR-AdV-Terminal besteht aus

- der **Hardware** des KTR-AdV-Terminals. Hierzu gehört ein Kartenleser für die eGK.
- der **Firmware** des KTR-AdV-Terminals. Als Firmware wird die Gesamtheit aus **Software-Plattform** und **AdV-Clients** bezeichnet. Der Hersteller des KTR-AdV-Terminals stellt die Firmware des KTR-AdV-Terminals zur Verfügung.

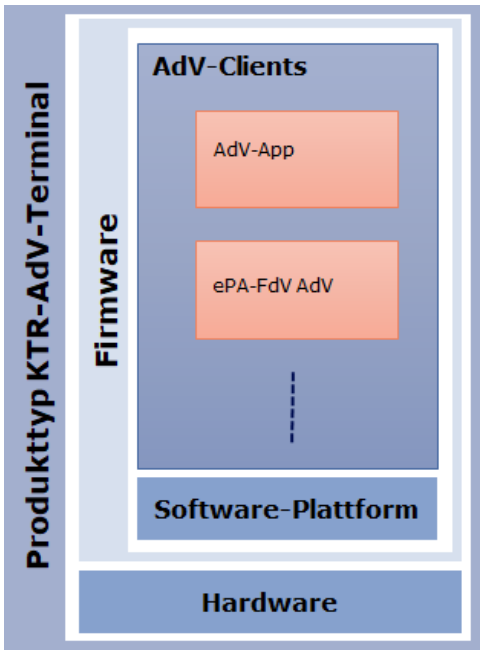


Abbildung 1 ABB_ADV_600 Aufbau des KTR-AdV-Terminals

Die **Software-Plattform** des KTR-AdV-Terminals (im Folgenden kurz *Plattform*) dient den AdV-Clients als Ablaufumgebung und beinhaltet alle Softwareanteile des KTR-AdV-Terminals, außer den AdV-Clients. Zur Plattform gehören BIOS/UEFI, Treiber (u.a. für den Kartenleser), Betriebssystem und Bibliotheken. Die Firmware des KTR-AdV-Terminals integriert mindestens einen zugelassenen AdV-Client.

Es ist keine Aufgabe des Herstellers des KTR-AdV-Terminals, die AdV-Clients zu entwickeln oder zuzulassen. Unbenommen davon steht es Herstellern eines KTR-AdV-Terminals natürlich frei, auch AdV-Clients in der Rolle eines AdV-Client-Herstellers zu entwickeln und zuzulassen.

Das KTR-AdV-Terminal wird im Auftrag der Krankenkassen und deren Verantwortung betrieben (z.B. in Geschäftsstellen der Krankenkassen). Der Betrieb ist nicht ins ITSM der TI eingebunden.

3 Systemkontext

Im Folgenden werden die Rollen und die Nachbarsysteme bzgl. des KTR-AdV-Terminals beschrieben.

3.1 Rollen

Im Kontext des KTR-AdV-Terminals treten folgende Rollen auf:

- **Hersteller KTR-AdV-Terminal**: Stellt ein KTR-AdV-Terminal her. Der Hersteller ist verantwortlich dafür, dass sein Produkt alle Anforderungen des Produkttypsteckbriefs [gemProdT_KTR-AdV-Terminal_PTV] erfüllt. Er integriert zugelassene AdV-Clients von AdV-Client-Herstellern in seine Firmware.
- **Hersteller AdV-Client**: Ist ein Hersteller eines AdV-Clients (z.B. Hersteller eines ePA-FdV AdV) und verantwortlich für die Umsetzung aller Anforderungen aus dem Produkttypsteckbrief des AdV-Clients.
- **Betriebsverantwortlicher KTR-AdV-Terminal**: Betreibt ein zugelassenes KTR-AdV-Terminal. Der Betriebsverantwortliche ist für die Umsetzung aller Anforderungen aus dem Handbuch des Herstellers des KTR-AdV-Terminals verantwortlich, die sich auf den sicheren Betrieb des KTR-AdV-Terminals beziehen. KTR-AdV-Terminals werden in der Regel in Geschäftsstellen der Krankenkassen betrieben. Der Betrieb ist nicht in das ITSM der TI eingebunden.
  - **Administrator des KTR-AdV-Terminals**: Der Administrator eines KTR-AdV-Terminals sorgt für die technische Betriebsbereitschaft des KTR-AdV-Terminals (z.B. Konfiguration bei Inbetriebnahme, Einbringen in das Netzwerk des Betriebsverantwortlichen).
- **Versicherte**: Versicherte nutzen die AdV-Clients des KTR-AdV-Terminals unter Nutzung ihrer eGK.

3.2 Nachbarsysteme

Die folgende Abbildung zeigt die Beziehung des KTR-AdV-Terminals zu benachbarten Systemen.

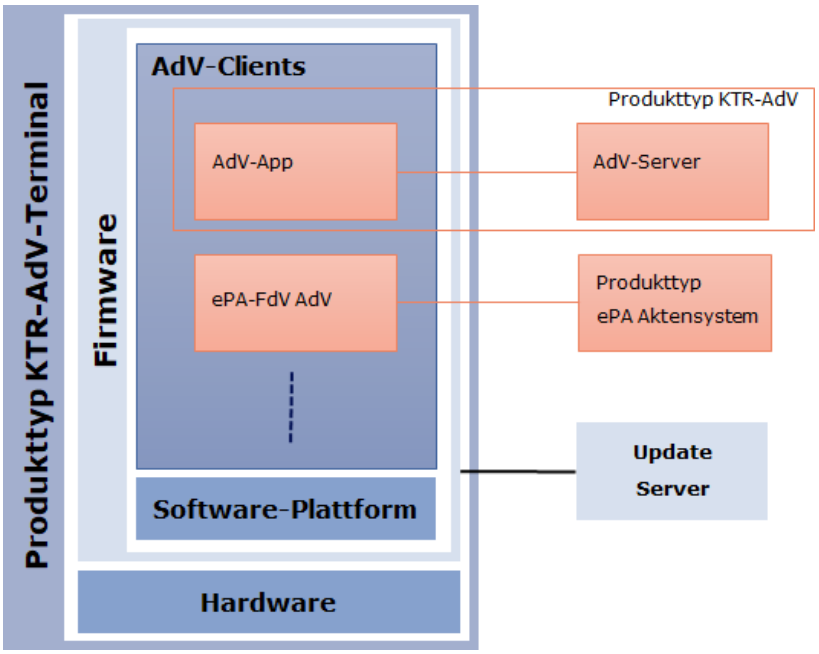


Abbildung 2 - benachbarte Systeme

Eine Interaktion des KTR-AdV-Terminals mit benachbarten Systemen erfolgt über die in der Firmware des KTR-AdV-Terminals enthaltenen AdV-Clients:

- die AdV-App des Produkttyps KTR-AdV nutzt die Schnittstellen des AdV-Servers [gemSpec_KTR-AdV],
- das ePA-FdV AdV nutzt die Schnittstellen des Produkttyps ePA-Aktensystem [gemSpec_Aktensystem].

Das KTR-AdV-Terminal aktualisiert seine Firmware mittels eines Update Servers.Hierbei ist es auch möglich, dass unterschiedliche Anteile der Firmware von unterschiedlichen Update-Servern bezogen werden.

4 Zerlegung des Produkttyps

Eine weitere Untergliederung des Produkttyps ist nicht erforderlich.

5 Funktionsmerkmale

Die Anforderungen dieses Abschnitts beschreiben Funktionsmerkmale des KTR-AdV-Terminals.

AdV-A_2537 - KTR-AdV-Terminal: Hardwareumfang
Das KTR-AdV-Terminal MUSS einen Kartenleser, eine Anzeigeeinheit und Bedienelemente (z. B. mit Möglichkeit zur Texteingabe) umfassen, die für Versicherte zugänglich sind.**[**<=**]**

Hinweis: Es kann auch ein mobiles Endgerät (z.B. Tablet) als Kartenleser genutzt werden, um NFC-fähige eGKs direkt auszulesen.

A_19785 - KTR-AdV-Terminal: Firmware enthält mindestens einen zugelassenen AdV-Client
Das KTR-AdV-Terminal MUSS in seiner Firmware mindestens einen AdV-Client enthalten.**[**<=**]**

Die Firmware eines KTR-AdV-Terminals kann z.B. eine AdV-App gemäß [gemSpec_KTR-AdV] und/oder ein ePA-FdV AdV gemäß [gemSpec_Frontend_Vers_AdV] enthalten. Die Auswahl an möglichen AdV-Clients erhöht sich bei Vorhandensein entsprechender Zulassungsverfahren (z.B. AdV-Client für elektronische Verordnungen).

A_19621 - KTR-AdV-Terminal: Update-Server
Der Hersteller des KTR-AdV-Terminals MUSS sicherstellen, dass Updates der Firmware des KTR-AdV-Terminals von einem bzw. ggf. mehreren Update-Servern bezogen werden können, der über das Internet erreichbar sind. **[**<=**]**

Um auch Versicherten mit körperlichen Einschränkungen sowie Aktivitätseinschränkungen den uneingeschränkten Zugang zum KTR-AdV-Terminal zu ermöglichen, sollen die Anforderungen aus der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz umgesetzt werden. Die Privatsphäre der Versicherten muss dabei gewahrt werden.

AdV-A_2577-01 - Barrierefreiheit
Das KTR-AdV-Terminal SOLL die von der Überwachungsstelle nach § 13 Abs. 3 des Behindertengleichstellungsgesetzes gemäß § 3 Abs. 5 BITV 2.0 veröffentlichten Informationen zu Barrierefreiheitsanforderungen umsetzen.**[**<=**]**

6 Datenschutz- und Sicherheitsanforderungen

In diesem Kapitel werdendie Datenschutz- und Sicherheitsanforderungen an die Hardware und die Plattform des KTR-AdV-Terminals sowie den Hersteller des KTR-AdV-Terminals beschrieben.

Die Datenschutz- und Sicherheitsanforderungen an die in die Firmware integrierten AdV-Clients sind in den Produkttypsteckbriefen der AdV-Clients beschrieben.

6.1 Datenschutz- und Sicherheitsanforderungen an die Hardware

Die Datenschutz- und Sicherheitsanforderungen geben keine konkrete Bauform des KTR-AdV-Terminals vor. Der Hersteller des KTR-AdV-Terminals hat hier Spielraum bei der konkreten Umsetzung des KTR-AdV-Terminals. Mobile Umsetzungsvarianten sollen explizit möglich sein.

Es sind bzgl. der Hardware des KTR-AdV-Terminals folgende Anforderungen zu erfüllen:

AdV-A_2527 - KTR_AdV-Terminal: Physischer Schutz der nicht benötigten HW-Schnittstellen
Das KTR-AdV-Terminal MUSS nicht benötigte Hardwareschnittstellendurch Sicherheitsmechanismen vor einem physischen Zugriff schützen.**[**<=**]**

A_19557 - KTR-AdV-Terminal: Sicherheitsmaßnahmen für benötigte HW-Schnittstellen
Das KTR-AdV-Terminal MUSS benötigte Hardwareschnittstellen (z. B. Netzwerkanschluss) durch Sicherheitsmechanismen schützen, um Angriffe über diese Schnittstellen abzuwehren.**[**<=**]**

AdV-A_2528 - Schutz Schnittstellen Kartenleser
Das KTR-AdV-Terminal MUSS die Schnittstellen des Kartenlesers zum Anschluss an das KTR-AdV-Terminal gegen unbefugten Zugriff sichern.**[**<=**]**

Eine mögliche Umsetzung dieser Anforderung ist, den physischen Zugang zur Schnittstelle zu verhindern.

6.2 Datenschutz- und Sicherheitsanforderungen an die Plattform

Dieser Abschnitt beschreibt die Anforderungen an die Plattform des KTR-AdV-Terminals.

Die Plattform des KTR-AdV-Terminals muss den Zugriff des Betriebsverantwortlichen auf die verarbeiteten sensiblen Daten des Versicherten unterbinden und sich selbst vor Angriffen von Nutzern des KTR-AdV-Terminals (Außentäter) schützen. Angriffe von Außentätern können hierbei beispielsweise über die Nutzerschnittstelle des KTR-AdV-Terminals stattfinden oder über manipulierte Dokumente, die der Angreifer aus seiner eigenen elektronischen Patientenakte herunterlädt und im KTR-AdV-Terminal verarbeiten lässt.

A_19592 - KTR-AdV-Terminal: Integrität der Firmware
Das KTR-AdV-Terminal MUSS technisch sicherstellen, dass die Firmware im KTR-AdV-Terminal nur genau dann ausgeführt wird, wenn die Firmware integer ist. **[**<=**]**

A_19595 - KTR-AdV-Terminal: Regelmäßige Updates
Das KTR-AdV-Terminal MUSS

- einmal täglich nach Firmware-Updates fragen,
- die Integrität und Authentizität des Update-Paketes prüfen und
- bei erfolgreicher Prüfung der Integrität und Authentizität das vorliegende Update automatisch installieren.

[<=]

A_19596 - KTR-AdV-Terminal: TLS Verbindung
Das KTR-AdV-Terminal MUSS eine TLS-Verbindung mit Serverauthentifizierung zum Update-Serveraufbauen.**[<=]**

Hinweis: Die für die TLS-Verbindung genutzten Schlüssel sind kein Teil der PKI der TI.

A_19597 - KTR-AdV-Terminal: TLS nach Vorgaben der TR-02102-2
Das KTR-AdV-Terminal MUSS für die TLS-Verbindung zum Update-Serverdie Vorgaben der Technischen Richtlinie BSI TR-02102-2 einhalten.**[<=]**

A_19598 - KTR-AdV-Terminal: Sichere TLS-Implementierung
Das KTR-AdV-Terminal SOLL eine bekannte und vertrauenswürdige sichere TLS-Implementierung nutzen. **[<=]**

Hinweis: Der Hersteller sollte eine existierende TLS-Implementierung verwenden, deren Sicherheit anerkannt ist, und TLS nicht neu implementieren. Dies reduziert den Aufwand beim Sicherheitsnachweis. Die Beurteilung, was eine vertrauenswürdige und bekannte TLS-Implementierung ist, erfolgt durch den Produktgutachter.

A_19988 - KTR-AdV-Terminal: Keine Zusatzfunktionen in den selbstentwickelten Anteilen der Plattform
DasKTR-AdV-Terminal MUSS sicherstellen, dass die Anteile der Plattform, die vom Hersteller des KTR-AdV-Terminals selbst entwickelt werden, keine Anwendungsfunktionalitäten außerhalb des von der gematik normierten Funktionsumfangs enthalten.**[<=]**

Hinweis:Zusätzliche kassenspezifische Funktionalitäten können nur als Teil der AdV-Clients implementiert werden.

A_19599 - KTR-AdV-Terminal: Härtung der Plattform-Komponenten anderer Hersteller
Das KTR-AdV-Terminal MUSS sicherstellen, dass Softwarekomponenten der Plattform, die nicht vom Hersteller des KTR-AdV-Terminals selbst entwickelt oder zur Entwicklung beauftragt werden (z.B. Betriebssystem),

- aus bekannten und vertrauenswürdigen Quellen bezogen werden und
- für diese Softwarekomponenten ausschließlich die für den Betrieb des KTR-AdV-Terminals erforderlichen Funktionen genutzt werden.

[<=]

A_19600 - KTR-AdV-Terminal: Beschränkung der Verbindungen
DasKTR-AdV-Terminal MUSS sicherstellen, dass die von Systemen zum KTR-AdV-Terminal eingehenden Verbindungen sowie die von der Plattform des KTR-AdV-Terminals ausgehenden Verbindungen auf das notwendige Minimum beschränkt sind. **[<=]**

Hinweis: Für die ausgehenden Verbindungen der AdV-Clients sind die AdV-Clients verantwortlich.Zulässige Verbindungen zum KTR-AdV-Terminal sind bspw. solche, die für

die Verwaltung des KTR-AdV-Terminals im Rahmen eines Mobile Device Managements notwendig sind (z.B. Sperren von entwendeten Geräten).

A_19601 - KTR-AdV-Terminal: Minimale Nutzerschnittstelle
Das KTR-AdV-Terminal MUSS sicherstellen, dass Nutzern keine Möglichkeit zum Zugriff auf die Plattform angeboten wird (d.h. keine Kommandozeile, kein Login auf der Plattform, kein Zugriff auf Konfigurationen des Gerätes, Betriebssystems, keine Zugriffe auf App-Stores etc.) und sie ausschließlich die für Versicherten am KTR-AdV-Terminal explizit vorgesehenen Anwendungsfälle nutzen können. **[**<=**]**

Hinweis: Die für den Versicherten am KTR-AdV-Terminal explizit vorgesehenen Anwendungsfälle ergeben sich aus den Anwendungsfällen der AdV-Clients.

A_19602 - KTR-AdV-Terminal: Minimale Admin-Funktionalität
Das KTR-AdV-Terminal MUSS sicherstellen, dass sich die Administrations-Funktionen der Firmware auf genau die Funktionen beschränken, die minimal zur Administration des KTR-AdV-Terminals benötigt werden und dass diese Funktionen nur nach erfolgreicher Authentifizierung genutzt werden können. **[**<=**]**

A_19603 - KTR-AdV-Terminal: Keine Administration bei laufenden AdV-Clients
Das KTR-AdV-Terminal MUSS sicherstellen, dass die Administrations-Funktionen der Firmware nur nutzbar sind, wenn nicht gleichzeitig AdV-Clients aktiv sind. **[**<=**]**

AdV-A_2524 - KTR-AdV-Terminal: Lesebestätigung der Sicherheitshinweise
Das KTR-AdV-Terminal MUSS vor dem Abschluss einer Konfiguration über die Admin-GUI eine Bestätigung anfordern, dass die Sicherheitshinweise im Handbuch des Herstellers des KTR-AdV-Terminals beachtet wurden.**[**<=**]**

A_19604 - KTR-AdV-Terminal: Keine persistente Speicherung von Versichertendaten
Das KTR-AdV-Terminal DARF die in der Plattform verarbeiteten Daten von Versicherten (u.a. personenbezogene Daten, Schlüssel, PINs) NICHT persistent speichern.**[**<=**]**

AdV-A_2517 - KTR-AdV-Terminal: Löschen von Protokolldaten
DasKTR-AdV-Terminal MUSS Protokolldaten, die älter als 14 Tage sind, löschen. **[**<=**]**

A_19605 - KTR-AdV-Terminal: Sicheres Löschen nach Ende einer Session
Das KTR-AdV-Terminal MUSS die im KTR-AdV-Terminal verarbeiteten Daten von Versicherten (u.a. personenbezogene Daten, Schlüssel, PINs) am Ende der Session des Nutzers aktiv sicher aus dem Arbeitsspeicher des KTR-AdV-Terminals löschen.**[**<=**]**

A_19607 - KTR-AdV-Terminal: Starten einer Session nur bei integrem System
Das KTR-AdV-Terminal MUSS sicherstellen, dass Sessions nur gestartet werden, wenn das laufende System integer ist und nicht manipuliert wurde. **[**<=**]**

Hinweis: Die Anforderung soll insbesondere vor Angriffen von Außentätern schützen, die über ihr eigenes ePA-Aktenkonto Dokumente mit Schwachstellen oder ausführbaren Code ins KTR-AdV-Terminal laden. Beim Start einer Session dürfen diese schadhaften Dokumente bzw. die durch sie am System ggf. entstandenen schadhaften Änderungen nicht mehr im System sein.

A_19609 - KTR-AdV-Terminal: Sichere PIN-Eingabe
Das KTR-AdV-Terminal MUSS sicherstellen, dass auf die vom Versicherten eingegebene PIN nicht unautorisiert zugegriffen werden kann. **[**<=**]**

AdV-A_2529 - KTR-AdV-Terminal: Sichere PIN-Eingabe berücksichtigen und unterstützen
Das KTR-AdV-Terminal MUSS die unbeobachtete PIN-Eingabe durch den Versicherten in der Gerätekonzeption berücksichtigen und unterstützen.**[**<=**]**

AdV-A_2518 - KTR-AdV-Terminal: Unbeobachtetes Einsehen von Daten berücksichtigen und unterstützen
Das KTR-AdV-Terminal MUSS die unbeobachtete Darstellung von Daten des Versicherten in der Gerätekonzeption berücksichtigen und unterstützen.**[<=]**

A_19610 - KTR-AdV-Terminal: Nutzung zugelassener AdV-Clients
Das KTR-AdV-Terminal MUSS sicherstellen, dass in der Firmware des KTR-AdV-Terminals nur von der gematik zugelassene AdV-Clients genutzt werden und dass diese von der Plattform wie spezifiziert genutzt werden. **[<=]**

Hinweis: Dass die Firmware nur zugelassene AdV-Clients beinhaltet wird vom Produktgutachter im Rahmen der Produktzulassung geprüft.

6.3 Sicherheitsanforderungen an Hersteller

Der Hersteller des KTR-AdV-Terminals hat die Anforderungen aus [gemSpec_DS_Hersteller] zu erfüllen, insbesondere an den sicheren Softwareentwicklungsprozess.

Zusätzlich sind folgende Anforderungen vom Hersteller eines KTR-AdV-Terminals umzusetzen.

A_19611 - KTR-AdV-Terminal: Produktspezifische Umgebungsanforderungen im Handbuch
Der Hersteller des KTR-AdV-Terminals MUSS im Handbuch beschreiben, welche produktspezifischen Anforderungen an die Einsatzumgebung des KTR-AdV-Terminals für den sicheren Betrieb notwendig und vom Betriebsverantwortlichen umzusetzen sind. **[<=]**

A_19612 - KTR-AdV-Terminal: Produktübergreifende Umgebungsanforderungen im Handbuch
Der Hersteller des KTR-AdV-Terminals MUSS den Betriebsverantwortlichen im Handbuch darüber informieren,

- welche Maßnahmen geeignet sind, um das KTR-AdV-Terminal im Betrieb vor Diebstahl- bzw. Austausch zu schützen,
- dass Maßnahmen gegen den unberechtigten Zugang zu den Schnittstellen des KTR-AdV-Terminals getroffen werden müssen (ausgenommen sind die Nutzerschnittstelle und der Kartenleser),
- dass Maßnahmen getroffen werden müssen, um Manipulationen am Kartenleser (z.B. Skimming-/Folien-Angriffe) des KTR-AdV-Terminals zu verhindern,
- dass im LAN des Betriebsverantwortlichen, in dem sich das KTR-AdV-Terminal befindet, Maßnahmen auf Netzebene zum Schutz gegen unautorisierte Zugriffe aus dem Internet umzusetzen sind (Paketfilter) und
- wie Versicherte das KTR-AdV-Terminal so nutzen können, dass Dritte das Display des KTR-AdV-Terminals, und damit die Daten des Versicherten, sowie die PIN-Eingabe und Dateneingaben nicht unbefugt einsehen können.

[<=]

A_20210 - KTR-AdV-Terminal: Prozess zur Sicherstellung der Integrität der Firmware
DerHersteller des KTR-AdV-Terminals MUSS einen Prozess etablieren und dokumentieren, um die Integrität der Firmware während des gesamten Lebenszyklus sicherzustellen und Manipulationen auszuschließen. Dies gilt insbesondere für Innentäter beim Hersteller des

KTR-AdV-Terminals und umfasst auch ein ggf. genutztes Mobile Device Management.**[<=]**

A_19613 - KTR-AdV-Terminal: Herstellerprozess gewährleistet nur zugelassene Firmware
DerHersteller des KTR-AdV-Terminals MUSS sicherstellen, dass Firmware bzw. Anteile der Firmware und Update-Pakte nur auf einem KTR-AdV-Terminal installiert werden, falls diese durch die gematik zugelassen wurden oder deren Änderung nach Vorgaben der gematik durch den Hersteller des KTR-AdV-Terminals als nicht zulassungsrelevant bewertet wurden. **[<=]**

Hinweis: ImZulassungsverfahren für das KTR-AdV-Terminal ist festgelegt, wann Änderungen durch die gematik als zulassungsrelevant betrachtet werden. Zulassungsrelevante Änderungen sind z.B. Änderungen von Sicherheitsfunktionen oder deren Implementierung (z. B. Wechsel der TLS-Implementierung). Nicht-zulassungsrelevante Änderungen sind z.B. Sicherheitsupdates für von anderen Herstellern bezogenen Software-Komponenten der Plattform (z.B. Betriebssystem, Bibliotheken),die aus einer vertrauenswürdigen Quelle bezogen werden.

A_19614 - KTR-AdV-Terminal: Beschränkung auf zugelassene AdV-Clients
Der Hersteller des KTR-AdV-Terminals MUSS sicherstellen, dass nur von der gematik zugelassene AdV-Clients Teil der Firmware sind. **[<=]**

A_19622 - KTR-AdV-Terminal: Sichere Ausführung der Apps nach Handbuch
Der Hersteller des KTR-AdV-Terminals MUSS für die in der Firmware enthaltenen AdV-Clients sicherstellen, dass die in den jeweiligen Handbüchern der AdV-Clients beschriebenen Voraussetzungen an die Ausführungsumgebung vom KTR-AdV-Terminal umgesetzt werden. **[<=]**

A_19617 - KTR-AdV-Terminal: Maßnahmen gegen Innentäter
DerHersteller des KTR-AdV-Terminals MUSS sicherstellen, dass Mitarbeiter des Herstellers nicht eigenständig schadhafte Firmware bzw. Firmware-Updates in Umlauf bringen können und die auf einem KTR-AdV-Terminal installierte Firmware nicht unautorisiert ändern oder konfigurieren können.**[<=]**

A_19618 - KTR-AdV-Terminal: Nachvollziehbarkeit von Änderungen installierter Firmware
Falls Mitarbeiter des Herstellers des KTR-AdV-Terminals die auf einem KTR-AdV-Terminal installlierte Firmware konfigurieren können (z.B. mittels Mobile Device Managements), MUSS der Hersteller des KTR-AdV-Terminals sicherstellen, dass eine Konfiguration nur im Vier-Augen-Prinzip erfolgt und im Nachhinien nachvollzogen und überprüft werden kann, wer, welche Änderung wann durchgeführt hat.**[<=]**

AdV-A_2526 - Bereitstellen von Softwareaktualisierungen
Der Hersteller des KTR-AdV-Terminals MUSS Schwachstellen in seiner Firmware unverzüglich schließen und die resultierenden Updates auf dem Update-Server bereitstellen. **[<=]**

Hinweis: Setzt der Hersteller des KTR-AdV-Terminals Softwareanteile anderer Hersteller in seiner Firmware ein, die Schwachstellen aufweisen, so hat der Hersteller des KTR-AdV-Terminals diese unverzüglich mit einer sicheren Version (d.h. einer Version ohne Schwachstelle) zu aktualisieren. Dies gilt insbesondere auch für die in der Firmware enthaltenen AdV-Clients.

6.4 ePA-spezifische Sicherheitsanforderungen

Für die Anwendung ePA erzeugt das ePA-Aktensystem für ein KTR-AdV-Terminal eine Geräteidentität (DeviceID) entsprechend [gemSpec_Aurorisierung]. Zum Schutz dieser ePA-spezifischen Geräteidentität (DeviceID) im KTR-AdV-Terminal hat das KTR-AdV-Terminal folgende Anforderungen umzusetzen.

A_19625 - KTR-AdV-Terminal: Sichere Speicherung der Geräteidentität
Das KTR-AdV-Terminal MUSS die im Registrierungsprozess vom Aktensystem erhaltene ePA-spezifische Geräteidentität des KTR-AdV-Terminals in einem TPM oder SE speichern, bzw. durch alternative Maßnahmen im KTR-AdV-Terminal einen Schutz gleicher Stärke erreichen.**[<=]**

A_19626 - KTR-AdV-Terminal: Kein Zugriff auf Geräteidentität
Das KTR-AdV-Terminal MUSS technisch sicherstellen, dass Nutzer, Administratoren oder Hersteller des KTR-AdV-Terminals keinen Zugriff auf die im KTR-AdV-Terminal verarbeitete ePA-spezifische Geräteidentität haben. **[<=]**

A_19627 - KTR-AdV-Terminal: Zugriff auf Geräteidentität nur durch ePA-FdV-App
Das KTR-AdV-Terminal MUSS technisch sicherstellen, dass nur die ePA-FdV-App auf die ePA-spezifische Geräteidentität im KTR-AdV-Terminal zugreifen kann. **[<=]**

7 Informationsmodell

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

8 Verteilungssicht

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

9 Anhang A – Verzeichnisse

9.1 Abkürzungen

Kürzel	Erläuterung
AdV	Anwendungen des Versicherten
eGK	elektronische Gesundheitskarte
ePA	elektronische Patientenakte
FIPS	Federal Information Processing Standard
KTR	Kostenträger
PIN	Personal Identification Number
TI	Telematikinfrastruktur
TLS	Transport Layer Security, Transportschichtsicherheit

9.2 Glossar

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

9.3 Abbildungsverzeichnis

Abbildung 1 ABB_ADV_600 Aufbau des KTR-AdV-Terminals 6
Abbildung 2 - benachbarte Systeme 9

9.4 Tabellenverzeichnis

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

9.5 Referenzierte Dokumente

9.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemProdT_ePA_FdV_AdV_PTV]	gematik: Produkttypsteckbrief ePA-Frontend des Versicherten im KTR-AdV-Terminal
[gemProdT_KTR-AdV_PTV]	gematik: Produkttypsteckbrief KTR-AdV
[gemProdT_KTR-AdV-Terminal_PTV]	gematik: Produkttypsteckbrief KTR-AdV-Terminal
[gemSpec_Aktensystem]	gematik: Spezifikation ePA-Aktensystem
[gemSpec_Autorisierung]	gematik: Spezifikation Autorisierung ePA
[gemSpec_DS_Hersteller]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller
[gemSpec_Frontend_Vers_AdV]	gematik: Spezifikation ePA-Frontend des Versicherten im KTR-AdV-Terminal
[gemSpec_KTR-AdV]	gematik: Spezifikation KTR-AdV

9.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
BITV 2.0	Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0)