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

Änderungen in gemSpec_KTR-AdV

Tabelle 1: TAB_ADV_300 – Akteure und ihre Rollen

Akteur	Rolle	Beschreibung
Nutzer	Versicherter	Primärer Anwender, Nutzung von fachlichen Anwendungsfällen für Zugriff auf Daten der eGK Hinweis: Der Vertreter des Versicherten für AMTS ist kein Akteur in AdV. Ihm werden keine Anwendungsfälle bereitgestellt.
	Rollen für Administration und Betrieb ~~Administrator~~	Sekundäre Anwender, führt Administrations- und Betriebsaufgaben für die KTR-AdV durch, wie z. B. • Installation des Systems und von Updates, • Konfiguration des Systems, • Administration von Nutzern (jedoch nicht von Versicherten), • täglicher Betrieb, • Herstellen und Wahren der Betriebsbereitschaft (z. B. Freischaltung der SM-B(s)). ~~Nutzung von technischen Anwendungsfällen zum Herstellen und Wahren der Betriebsbereitschaft~~ Die Ausführung dieser Anwendungsfälle muss mit gesonderten Zugriffsrechten erfolgen.
Aus-führungs-umgebung	KTR-AdV-Terminal	Interaktives Gerät für Zugang zu mittels eGK gespeicherten Daten des Versicherten durch den Versicherten zur Wahrnehmung der Rechte auf informationelle Selbstbestimmung
	Gerät des Versicherten	Gerät des Versicherten, dass u.a. für Zugang zu mittels der eGK gespeicherten Daten zur Wahrnehmung der Rechte auf informationelle Selbstbestimmung ermöglicht
Anbieter	Organisatorische Rolle, kein Akteur in der Ausführung von Anwendungsfällen	Ein Hersteller bzw. Herausgeber eines Produkts des Produkttyps KTR-AdV (und ggfs. KTR-AdV-Terminals)
Betreiber		Der Betreiber eines konkreten Produkts, in dessen Betriebsumgebung die Teilkomponente KTR-AdV-Server (und ggfs. KTR-AdV-Terminals) betrieben werden

Der Nutzer kann in verschiedenen Rollen aktiv werden. Als Versicherter nimmt der Nutzer seine Datenschutzrechte auf informationelle Selbstbestimmung wahr, indem er fachliche

Anwendungsfälle zum Anzeigen und ggfs. Bearbeiten der mittels seiner eGK gespeicherten Daten startet. ~~Der Administrator ist derjenige Nutzer, der die technische Betriebsbereitschaft der KTR-AdV herstellt, d.h. das System für die Inbetriebnahme konfiguriert und während des Betriebs die Betriebsbereitschaft sicherstellt.~~ Die Nutzer mit den Rollen Administration und Betrieb stellen die technische Betriebsbereitschaft der KTR-AdV her, d. h. sie konfigurieren das System für die Inbetriebnahme und stellen während des Betriebs die Betriebsbereitschaft sicher.

⌦ AdV-A_2571 Rollen- und Berechtigungskonzept der KTR-AdV

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

⌦ AdV-A_2533 Kartenbezogene Benutzerrollen der KTR-AdV

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

- Versicherter, für den Zugriff auf Objekte einer eGK
- Berechtigte Nutzer ~~Administrator~~, für den Zugriff auf privates Schlüsselmaterial der SM-B-Identitäten

Andere, nicht zu diesen Rollen passende PIN-Objekte, DÜRFEN NICHT verwendet werden. ⌫

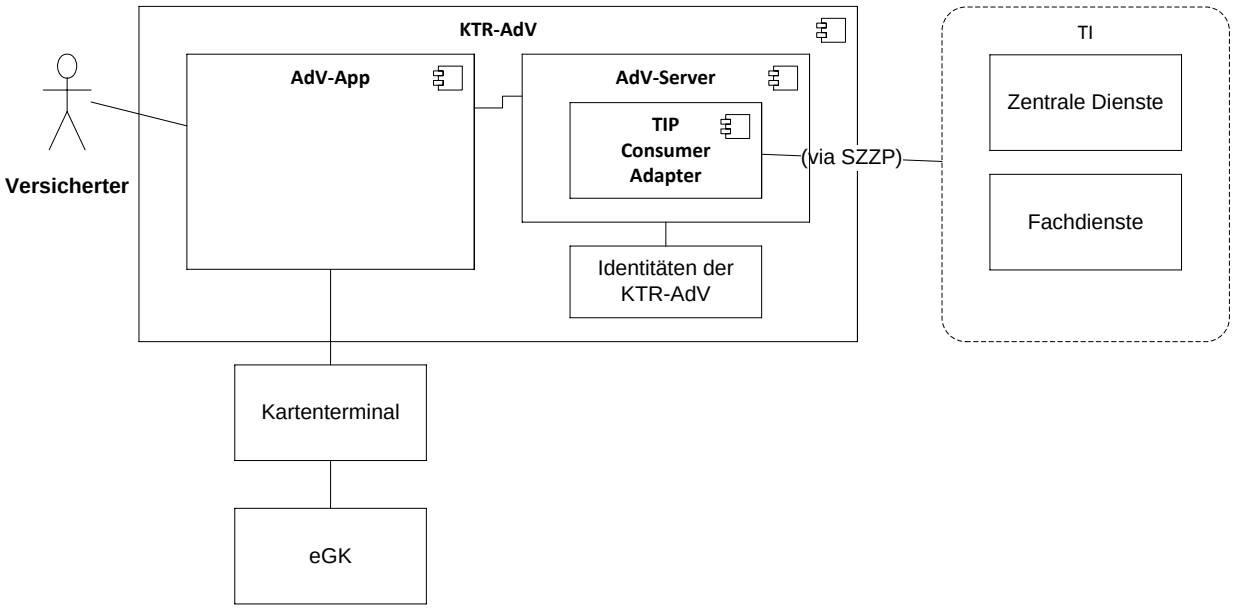

Abbildung 3: ABB_ADV_301 – Kontextdiagramm

⌦ AdV-A_2422 AdV-Server: Erzeugung von FehlerLog-Einträgen

Der AdV-Server MUSS bei lokal erkannten Fehlern und Remote-Fehlern ein Fehlerprotokoll schreiben, welches dem berechtigten Nutzer ~~Administrator~~ Rückschlüsse auf die aufgetretenen Fehler ermöglicht. ⌫

⌦ **AdV-A_2423 AdV-App: Erzeugung von FehlerLog-Einträgen**

Die AdV-App MUSS, wenn sie auf einem KTR-AdV-Terminal betrieben wird, bei lokal erkannten Fehlern und Remote-Fehlern ein Fehlerprotokoll schreiben, welches dem berechtigten Nutzer ~~Administrator~~ Rückschlüsse auf die aufgetretenen Fehler ermöglicht. ⌫

⌦ **AdV-A_2440 AdV-Server: Art der Protokollierung**

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

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

⌦ **AdV-A_2441 AdV-App: Art der Protokollierung**

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

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

⌦ **AdV-A_2442 AdV-Server: Zugriff auf Protokolldateien**

Der AdV-Server MUSS den Zugriff auf Protokolldateien mit einem Authentisierungsverfahren auf berechtigte Nutzer ~~Administrator~~ beschränken. ⌫

⌦ **AdV-A_2443 AdV-App: Zugriff auf Protokolldateien**

Die AdV-App MUSS, wenn sie auf einem KTR-AdV-Terminal betrieben wird, den Zugriff auf Protokolldateien mit einem Authentisierungsverfahren auf berechtigte Nutzer ~~Administrator~~ beschränken. ⌫