

Telematikinfrastruktur 2.0

Spezifikation Proof of Patient Presence (PoPP)-Service

Version:	1.0.0_CC
Revision:	1106020
Stand:	20.01.2025
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_PoPP_Service

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_CC	20.01.2025		initiale Erstellung	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes.....	6
1.1 Zielsetzung.....	6
1.2 Zielgruppe.....	6
1.3 Geltungsbereich.....	6
1.4 Abgrenzungen.....	7
1.5 Methodik.....	7
2 Systemüberblick.....	9
2.1 Überblick zum Ablauf eGK und GesundheitsID.....	10
2.2 Überblick der Anwendungsfälle für die Ausstellung des PoPP-Token.....	11
2.3 Akteure und Rollen.....	14
2.3.1 Herstellung und Betrieb.....	14
2.3.1.1 Hersteller PoPP-Service.....	15
2.3.1.2 Anbieter PoPP-Service.....	15
2.3.1.3 gematik.....	15
2.3.1.4 Primärsystem-Hersteller.....	16
2.3.1.5 Hersteller PoPP-Modul.....	16
2.3.1.6 Hersteller App.....	16
2.3.1.7 Kostenträger (KTR).....	16
2.3.2 Nutzer.....	16
2.3.2.1 Leistungserbringerinstitution (LEI).....	16
2.3.2.2 Versicherte.....	16
3 Systemkontext PoPP-Service.....	18
3.1 Produkt-Zerlegung und Außenschnittstellen.....	18
3.2 Systemkontext.....	19
3.3 Nachbarsysteme.....	24
4 Funktionale Anwendungsfälle des PoPP-Service.....	25
4.1 Übersicht der Systemanwendungsfälle für die Ausstellung des PoPP-Token.....	25
4.2 Leistungserbringerinstitution (LEI) am PoPP-Service registrieren und anmelden.....	27
4.3 Mobiler Check-in und Ausgabe des PoPP-Token.....	28
4.3.1 Mobiler Check-in mit GesundheitsID.....	30
4.3.2 Mobiler Check-in mit eGK.....	34
4.3.3 PoPP-Token mittels TAN, lokal.....	41
4.3.4 PoPP-Token mittels TAN, mobil.....	43
4.4 Check-in in einer LEI mit eGK und Ausgabe des PoPP-Token.....	46
5 Übergreifende Festlegungen.....	52

5.1 PoPP-Token: Nachweis des Versorgungskontextes.....	52
5.1.1 PoPP-Token-Erstellung.....	52
5.1.2 PoPP-Token Prüfung.....	56
5.1.3 Ersatz-Prüfungsnachweis (VSDM-PN).....	57
5.1.3.1 Aufbau des VSDM-PN.....	58
5.1.3.2 Vorgaben zum VSDM-PN-HMAC-Sicherungsschlüssel.....	59
5.2 Datenschutz und Sicherheit.....	62
5.2.1 Vertrauenswürdige Ausführungsumgebung (VAU).....	64
5.2.1.1 Allgemein.....	64
5.2.1.2 Einbinden des ZETA Guard der gematik.....	65
5.2.1.3 Informative Erläuterung zu den Zielen der VAU und den konkreten Umsetzungshinweisen.....	67
5.2.1.4 Lifecycle eines Verarbeitungskontextes.....	68
5.2.1.5 Anforderungen an das HSM.....	70
5.2.1.6 Schlüsselnutzung direkt im Verarbeitungskontext.....	71
5.2.1.7 Speicherung von Daten.....	73
5.2.1.8 Transport von Daten und Authentisierung/Authentifizierung bei Kommunikation.....	73
5.2.1.9 Protokollierung und Monitoring.....	75
5.2.1.10 Konfigurierbarkeit.....	75
5.2.1.11 Anforderungen an den Hersteller.....	76
5.2.1.12 Anforderungen an den Anbieter.....	78
5.2.1.13 Bereitstellung durch die gematik.....	81
5.3 Identitäten und Zertifikate PoPP-Service.....	81
5.3.1 Überblick.....	81
5.3.2 Algorithmus für Schlüsselpaare.....	82
5.3.3 Entity Statement.....	82
5.3.4 Token-Signaturen.....	83
5.3.5 TLS.....	83
5.3.6 CV-Zertifikat.....	84
5.3.7 TSL-Handling.....	84
5.4 ZETA Guard im PoPP-Service.....	86
5.4.1 Bereitstellung, Konfiguration und Verwendung vom ZETA Guard.....	86
5.5 Vertrauenswürdige Uhrzeit im PoPP-Service.....	87
5.6 Federation Entity Statement.....	88
6 Funktionsmerkmale.....	92
6.1 PoPP-Service - Authorization Server.....	92
6.1.1 Standard Authorization Server mit Versicherten Authentisierung.....	92
6.1.2 Authorization Server Zusatzfunktion Authentifizierung eGK mobil.....	94
6.1.3 Anforderungen an den PoPP-Service Authorization Server in der Funktion OAuth Server.....	94
6.1.3.1.1 Service Discovery.....	94
6.1.3.1.2 Client Registrierung.....	95
6.1.3.2 Ausstellung eines "eHealth-ID-check" Access Token.....	95
6.1.3.3 Ausstellung eines "card-check" Access Token.....	97
6.1.4 Mobile Verfahren zur Bestätigung der Versicherten-Identität.....	97
6.1.5 Schnittstellen.....	107
6.2 PoPP-Service - Resource Server.....	107
6.2.1 eGK-Handling.....	108
6.2.1.1 eGK-Handling, Einführung.....	108

6.2.1.2 Szenario.....	111
6.2.1.3 eGK öffnen.....	112
6.2.1.4 eGK G2 kontaktbehaftet.....	113
6.2.1.5 eGK G2 kontaktlos.....	117
6.2.1.6 eGK G3 kontaktbehaftet und kontaktlos.....	120
6.2.1.7 Prüfung des X.509 Zertifikates einer eGK.....	121
6.2.1.8 eGK-Handling Fehlercodes.....	121
6.2.1.9 eGK-Hash-Datenbank.....	122
6.2.2 Zugriffsautorisierung und Business-Logik.....	126
6.2.2.1 Validierung der Access Token.....	128
6.2.2.2 TAN-Set, "lange" und "kurze" TAN.....	129
6.2.2.3 TANSet-Record.....	130
6.2.3 Schnittstelle für Token Abrufe.....	131
6.3 PoPP-Modul.....	133
6.4 PoPP-Client.....	133
6.5 Fehlerbehandlung.....	133
7 Testanforderungen.....	135
8 Betrieb.....	136
8.1 Schnittstellen und Anwendungsfälle.....	136
8.2 Leistungsanforderungen und Performance.....	136
9 Anhang A - Verzeichnisse.....	137
9.1 Abkürzungen.....	137
9.2 Glossar.....	139
9.3 Abbildungsverzeichnis.....	142
9.4 Tabellenverzeichnis.....	143
9.5 Referenzierte Dokumente.....	144
9.5.1 Dokumente der gematik.....	144
9.5.2 Weitere Dokumente.....	147
9.6 Allgemeine Erläuterungen.....	149
9.6.1 Entity Statement des PoPP-Service.....	149

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen an die Herstellung, den Test und den Betrieb des Produkttyps PoPP-Service. Diese Anforderungen basieren auf einem von der gematik erarbeiteten technischen Konzept einer PoPP-Lösung sowie auf fortlaufenden Abstimmungen mit den Gesellschaftern der gematik, insbesondere in Bezug auf die Nutzung der GesundheitsID.

Der PoPP-Service ist der Serveranteil der PoPP-Lösung, wobei PoPP für "Proof of Patient Presence" steht. Der PoPP-Service erzeugt die Bestätigung eines Versorgungskontextes in Form eines kryptographisch gesicherten PoPP-Token. Dieses Token bestätigt, dass ein bestimmter Versicherter mit einer bestimmten Leistungserbringerinstitution (LEI) zusammengekommen ist. Dieser Versorgungskontext wird beim Zugriff von Leistungserbringern (LE) auf TI-Fachdienste (FD), wie bspw. VSDM 2.0, "ePA für alle" oder E-Rezept, in Form eines PoPP-Token an diese übermittelt.

Neben dem PoPP-Service, der als Plattformdienst der Telematikinfrastruktur (TI) 2.0 betrieben wird, tragen weitere Komponenten zur PoPP-Lösung bei:

- PoPP-Clients, die als Teil der Primärsysteme (PS) implementiert werden,
- PoPP-Module, das als Teil von von Versicherten genutzte Anwendungen implementiert werden, welche bei der mobilen Nutzung der eGK oder bei Nutzung der GesundheitsID in die Kommunikation zur Erstellung von PoPP-Token eingebunden sind.

Die Spezifikation oder Beschreibung dieser weiteren Komponenten erfolgt in anderen Dokumenten.

1.2 Zielgruppe

Das Dokument richtet sich an:

- Hersteller und Anbieter des PoPP-Service,
- Hersteller von Produkttypen oder Komponenten, die eine Schnittstelle zum PoPP-Service besitzen,
- Hersteller und Anbieter von FD, die einen PoPP-Token nutzen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur TI des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (bspw. gemPTV_ATV_Festlegungen, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekanntgegeben.

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzungen

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang A – Verzeichnisse).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps PoPP-Service [gemProdT_PoPP_Service_PTV] verzeichnet. Für den Anbieter des PoPP-Service ist auch der Anbietertypsteckbrief für den PoPP-Service [gemAnbT_PoPP_Service_ATV] relevant.

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zum Themenbereich PoPP-Client, PoPP-Modul oder App-Anforderungen zur PoPP-Token Kommunikation.

1.5 Methodik

Anwendungsfälle und Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID, Anforderungen zusätzlich durch die dem [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Da in dem Beispielsatz "Eine leere Liste DARF NICHT ein Element besitzen." die Phrase "DARF NICHT" semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen "Eine leere Liste DARF KEIN Element besitzen." verwendet. Die Schlüsselworte werden außerdem um Pronomen in Großbuchstaben ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anwendungsfälle und Anforderungen werden im Dokument wie folgt dargestellt:

<AF-ID> - <Titel des Anwendungsfalles>

Text/Beschreibung

[<=]

bzw.

<AFO-ID> - <Titel der Afo>

Text/Beschreibung

[<=]

Dabei umfasst der Anwendungsfall bzw. die Anforderung sämtliche zwischen ID und Textmarke [≤] angeführten Inhalte.

Hinweis auf offene Punkte

Offener Punkt: Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.

2 Systemüberblick

In diesem Kapitel wird ein einführender Überblick über die PoPP-Lösung gegeben.

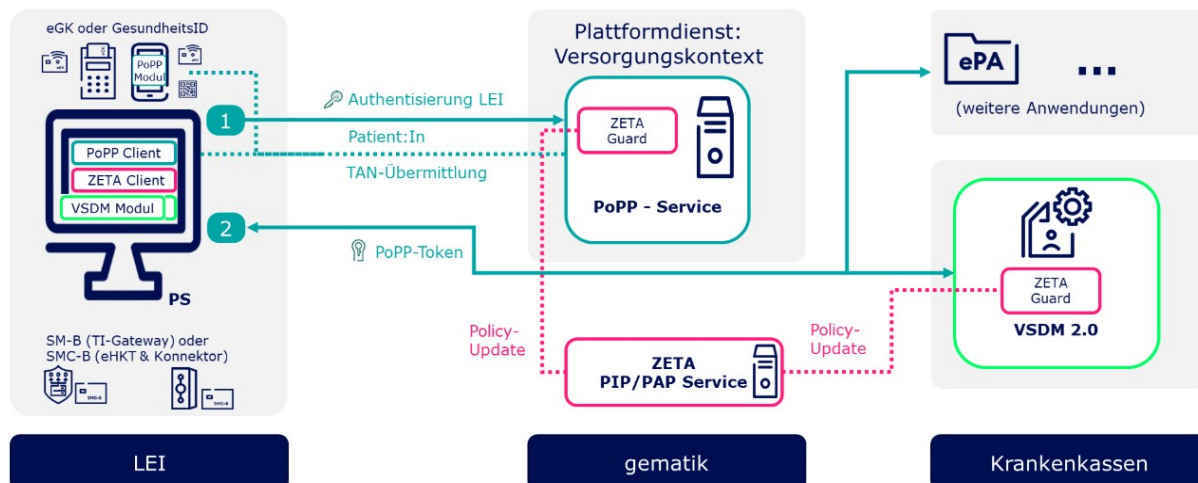


Abbildung 1: Einfacher Systemüberblick

Proof of Patient Presence (PoPP) ist ein Nachweis, der belegt, dass sich ein Versicherter zu einem bestimmten Zeitpunkt in einem Versorgungskontext mit einer bestimmten LEI befindet. Im kryptographisch gesicherten PoPP-Token sind somit Informationen über die LEI und über den Versicherten zusammengeführt. Dabei ist es die Aufgabe der PoPP-Lösung, die Authentifizierung der LEI durchzuführen und durch Authentifizierung des Versicherten per GesundheitsID oder Authentifizierung der elektronischen Gesundheitskarte (eGK) eines Versicherten den Versorgungskontext zu bestätigen. Das Ergebnis ist das PoPP-Token, das der LEI zur Autorisierung für den Zugriff auf die Daten des Versicherten in Diensten der TI dient.

Die Lösung besteht aus dem zentralen Server und verschiedenen Client Komponenten:

1. **PoPP-Service** - der als zentraler Dienst PoPP-Token für LEI erstellt. Ein Versicherter authentisiert sich dabei entweder mit seiner eGK oder seiner GesundheitsID.
2. **Primärsystem (PS) der LEI** - als Host der Client-Seite. Das PS besteht aus:
 - a. Basis-PS - enthält die bisherige Funktionalität inklusive der Verwaltung von Patientenstammdaten (PVS/KIS) , sowie eine neue Businesslogik, die für die Steuerung der Praxisabläufe bei der Erstellung eines PoPP-Token benötigt wird.
 - b. PoPP-Client - enthält die Funktionalität für die Kommunikation des Basis-PS mit dem PoPP-Service. Dazu gehören die Anfrage zur Erzeugung von PoPP-Token für den eGK- und den GesundheitsID-Pfad und die Bereitstellung des PoPP-Token durch den PoPP-Service.
Die Beschreibung und Anforderungen an den PoPP-Client finden sich in [gemILF_PoPP_Client],
 - c. ZETA Client - enthält die Funktionalität zur Erzeugung und Management der für den Zero Trust Ablauf notwendigen Identitäten und Abläufe gemäß [gemSpec_ZETA],
 - d. Anwendungs-Module zur Verwendung und Steuerung von TI-Anwendungen von (VSDM 2.0, ePA, E-Rezept).

3. **PoPP-Modul für Versicherte** (PoPP-Modul) - ist ein integriertes Anwendungsmodul, mittels dessen ein Versicherter das Check-in bei einer LEI mit seiner GesundheitsID starten kann. Die Beschreibung und Anforderungen an das PoPP-Modul finden sich in [gemSpec_PoPP_Modul]. Es ist denkbar, dass so ein PoPP-Modul von einer Kasse oder von einem weiteren Anbieter (bspw. Apotheken-App oder Videosprechstunden-App) für das Smartphone/Endgerät eines Versicherten, als Browser-Anwendung oder als Desktop-Anwendung bereitgestellt wird.

2.1 Überblick zum Ablauf eGK und GesundheitsID

Der Nachweis des Versorgungskontextes (PoPP-Token) erfordert die Authentifizierung von LEI und Versicherten. Die LEI authentifiziert sich mit ihrer SMC-B. Der Versicherte hat die Wahl und authentifiziert sich entweder mittels GesundheitsID oder seine eGK wird authentifiziert. Dieser Authentifizierungsprozess wird als Check-in bezeichnet.

Der Versicherte hat zudem die Wahl den Check-in von einer LEI durchführen zu lassen (dazu übergibt er die eGK und alles weitere führt der PoPP-Client durch) oder er initiiert den Check-in selbst mittels eines Smartphones, Laptops oder PCs (mobiler Check-in). Beim mobilen Check-in kommt auf dem Gerät des Versicherten das PoPP-Modul zum Einsatz. Der mobile Check-in ist für alle Versorgungskontexte verfügbar. Beispielsweise für Videosprechstunden-Anwendungen ist der mobile Check-in die einzig Möglichkeit, die den Versicherten für einen Check-in zur Verfügung steht.

Führt der Versicherte einen mobilen Check-in durch, dann werden dabei TAN erzeugt. Die TAN werden später in der LEI zur Herstellung des Versorgungskontextes verwendet. Dabei wird zwischen folgenden Typen von TAN unterschieden:

1. Die "lange" TAN (mit viel Entropie) ist dazu gedacht, mittels QR-Code Scanner von einem Primärsystem entgegengenommen zu werden. Eine "lange" TAN ist niemals an eine bestimmte LEI gebunden. Deshalb ist es möglich eine "lange" TAN in jeder LEI zur Erzeugung eines PoPP-Token zu verwenden
2. Die "kurze" TAN (kurze numerische Zeichenkette) ist dazu gedacht, manuell ins System eingegeben zu werden. Eine kurze TAN ist stets an eine bestimmte LEI gebunden und es ist nur in dieser LEI möglich die "kurze" TAN erfolgreich zur Erzeugung eines PoPP-Token zu verwenden.

Technologieoffenheit

In diesem Dokument wird als kleinster gemeinsamer Nenner und zur Sicherstellung der Interoperabilität für die Übermittlung "langer" TAN mittels QR-Code beschrieben. Weil die gematik Technologieoffenheit unterstützt, steht die gematik weiteren Übertragungsverfahren offen gegenüber, bspw. NFC.

2.2 Überblick der Anwendungsfälle für die Ausstellung des PoPP-Token

Die in diesem Kapitel aufgeführten Anwendungsfälle schildern die Absichten des Nutzers in Verbindung mit dem Primärsystem und dienen als Lesehilfe zu den fachlichen Anwendungsfällen. Die Anwendungsfälle erheben keinen Anspruch auf Vollständigkeit.

Bei den Anwendungsfällen wird seitens der Versicherten die Verwendung der eGK oder der GesundheitsID unterschieden. Seitens der LEI wird unterschieden, ob der Versorgungskontext entsteht während Versicherter und LEI physisch gemeinsam anwesend sind (Praxisbesuch, Hausbesuch), oder ob die LEI virtuell anwesend ist, wie bspw. bei einer Videosprechstunde.

Tabelle 1: PoPP-Use Cases (Business Sicht)

ID	Anwendungsfälle
UC_PoPP_1a	<p>PoPP-Token bei physischer Anwesenheit in der LEI - GesundheitsID - Scanner vorhanden</p> <p>Ein Versicherter möchte eine Versorgung in einer LEI in Anspruch nehmen. Die LEI benötigt für den Zugriff auf die Daten des physisch anwesenden Versicherten den Nachweis des Versorgungskontextes. Dazu startet der Versicherte zuvor den Check-in-Vorgang in einer App mit integriertem PoPP-Modul, indem er sich zunächst mittels GesundheitsID authentisiert. Anschließend erhält er ein TAN-Set mit "lange" TAN. Die TAN sind als QR-Code im PoPP-Modul dargestellt. Nachdem das Personal der LEI den QR-Code einer TAN eingescannt hat, ist der Check-in-Vorgang abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontextes.</p>
UC_PoPP_1b	<p>PoPP-Token bei physischer Anwesenheit in der LEI - GesundheitsID - Scanner nicht vorhanden</p> <p>Ein Versicherter möchte eine Versorgung in einer LEI in Anspruch nehmen. Die LEI benötigt für den Zugriff auf die Daten des physisch anwesenden Versicherten den Nachweis des Versorgungskontextes. Dazu startet der Versicherte den Check-in-Prozess in einer App mit integriertem PoPP-Modul, indem er sich zunächst mittels GesundheitsID authentisiert, dann die LEI aus dem Verzeichnis auswählt oder einen von der LEI für den Check-in bereitgestellten QR-Code scannt und anschließend eine "kurze" TAN erhält. Nach der mündlichen Übermittlung der TAN durch den Versicherten und anschließender Eingabe durch das LEI-Personal im PS, ist der Check-in-Vorgang abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontextes.</p>
UC_PoPP_1c	<p>PoPP-Token bei physischer Anwesenheit in der LEI - eGK</p> <p>Ein Versicherter möchte eine Versorgung in einer LEI in Anspruch nehmen. Die LEI benötigt für den Zugriff auf die Daten des physisch anwesenden Versicherten den Nachweis des Versorgungskontextes. Dazu wird die eGK des Versicherten an einem geeigneten Lesegerät der LEI präsentiert. Nachdem der Versicherte den Check-in-Prozess mit der eGK durchgeführt hat, ist dieser abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontextes.</p>
UC_PoPP_2a	<p>PoPP-Token bei physischer Anwesenheit außerhalb der LEI - GesundheitsID - Scanner vorhanden</p> <p>Ein Versicherter möchte eine Versorgung außerhalb einer LEI in Anspruch nehmen. Dazu kommt das Personal der LEI zum Versicherten. Das Personal verwendet ein mobiles Endgerät, auf dem ein PS installiert (mobiles PS) und an das über einen QR-Code Scanner verfügt (als Anwendung im Gerät oder als angeschlossenes externes Gerät). Die LEI benötigt für den Zugriff auf die Daten des physisch anwesenden</p>

	<p>Versicherten den Nachweis des Versorgungskontextes. Dazu startet der Versicherte zuvor den Check-in-Vorgang in einer App mit integriertem PoPP-Modul, indem er sich zunächst mittels GesundheitsID authentisiert. Anschließend erhält er eine "lange" TAN, welche als QR-Code dargestellt ist. Nachdem das Personal der LEI den QR-Code mit dem am mobilen PS angeschlossenen Scanner eingescannt hat, ist der Check-in-Vorgang abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontextes.</p>
UC_PoPP_2b	<p>PoPP-Token bei physischer Anwesenheit außerhalb der LEI - GesundheitsID - Scanner nicht vorhanden</p> <p>Ein Versicherter möchte eine Versorgung außerhalb einer LEI in Anspruch nehmen. Dazu kommt das Personal der LEI zum Versicherten. Die LEI benötigt für den Zugriff auf die Daten des physisch anwesenden Versicherten den Nachweis des Versorgungskontextes. Dazu startet der Versicherte den Check-in-Prozess in einer App mit integriertem PoPP-Modul, indem er sich zunächst mittels GesundheitsID authentisiert, dann die LEI aus dem Verzeichnis auswählt oder einen von der LEI für den Check-in bereitgestellten QR-Code scannt und anschließend eine "kurze" TAN erhält. Nach der mündlichen Übermittlung der TAN durch den Versicherten und anschließender Eingabe durch das Personal der LEI im mobilen PS, ist der Check-in-Vorgang abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontextes.</p>
UC_PoPP_2c	<p>PoPP-Token bei physischer Anwesenheit außerhalb der LEI - eGK</p> <p>Ein Versicherter möchte eine Versorgung außerhalb einer LEI in Anspruch nehmen. Dazu kommt das Personal der LEI zum Versicherten. Die LEI benötigt für den Zugriff auf die Daten des physisch anwesenden Versicherten den Nachweis des Versorgungskontextes. Dazu wird die eGK des Versicherten an einem geeigneten mobilen Lesegerät der LEI präsentiert. Nachdem das LEI-Personal die eGK eingelesen hat, ist der Check-in-Vorgang abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontextes.</p>
UC_PoPP_3a	<p>PoPP-Token ohne physische Anwesenheit in der LEI - GesundheitsID - digitaler Kommunikationsweg ins PS vorhanden</p> <p>Ein Versicherter möchte virtuell eine Versorgung einer LEI in Anspruch nehmen. Die LEI benötigt für den Zugriff auf die Daten des virtuell anwesenden Versicherten den Nachweis des Versorgungskontextes. Dazu startet der Versicherte zuvor den Check-in-Vorgang in einer App mit integriertem PoPP-Modul, indem er sich zunächst mit seiner GesundheitsID authentisiert und anschließend eine "lange" TAN erhält. Der Versicherte übermittelt elektronisch die TAN über einen von der LEI angebotenen Kommunikationsweg. Nachdem das LEI-Personal den übermittelten Inhalt im PS verarbeitet hat, ist der Check-in-Vorgang abgeschlossen und die LEI erhält im PS den benötigten Nachweis des Versorgungskontextes.</p>

UC_PoPP_3b	<p>PoPP-Token ohne physische Anwesenheit in der LEI - GesundheitsID - digitaler Kommunikationsweg ins PS nicht vorhanden</p> <p>Ein Versicherter möchte virtuell eine Versorgung einer LEI in Anspruch nehmen. Die LEI benötigt für den Zugriff auf die Daten des virtuell anwesenden Versicherten den Nachweis des Versorgungskontextes. Dazu startet der Versicherte den Check-in-Prozess in einer App mit integriertem PoPP-Modul. Er authentisiert sich zunächst mittels GesundheitsID und wählt dann die LEI aus dem Verzeichnis aus oder scannt einen von der LEI für den Check-in bereitgestellten QR-Code. (falls diese nicht durch die App bereits vorausgewählt ist). Anschließend erhält er eine "kurze" TAN. Nach der mündlichen Übermittlung der TAN durch den Versicherten und anschließender Eingabe durch das LEI-Personal im PS, ist der Check-in-Vorgang abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontextes.</p>
UC_PoPP_3c	<p>PoPP-Token ohne physische Anwesenheit in der LEI - eGK (mobil) - digitaler Kommunikationsweg ins PS vorhanden</p> <p>Ein Versicherter möchte virtuell eine Versorgung einer LEI in Anspruch nehmen. Die LEI benötigt für den Zugriff auf die Daten des virtuell anwesenden Versicherten den Nachweis des Versorgungskontextes. Dazu startet der Versicherte oder ein Vertreter den Check-in-Prozess im PoPP-Modul einer App, indem die eGK des Versicherten an einem geeigneten mobilen Lesegerät präsentiert wird und er anschließend eine "lange" TAN erhält. Der Versicherte oder Vertreter übermittelt elektronisch die TAN aus der App an die LEI. Nachdem das LEI-Personal den übermittelten Inhalt im PS verarbeitet hat, ist der Check-in-Vorgang abgeschlossen, und die LEI erhält im PS den benötigten Nachweis des Versorgungskontextes.</p>
UC_PoPP_3d	<p>PoPP-Token ohne physische Anwesenheit in der LEI - eGK (mobil) - digitaler Kommunikationsweg ins PS nicht vorhanden</p> <p>Ein Versicherter möchte virtuell eine Versorgung einer LEI in Anspruch nehmen. Die LEI benötigt für den Zugriff auf die Daten des virtuell anwesenden Versicherten den Nachweis des Versorgungskontextes. Dazu startet der Versicherte oder ein Vertreter den Check-in-Prozess im PoPP-Modul der App, indem er die LEI aus dem entsprechenden Verzeichnis auswählt (falls diese nicht durch die App bereits vorausgewählt ist). Dann wird die eGK des Versicherten an einem geeigneten mobilen Lesegerät präsentiert und dieser erhält anschließend eine "kurze" TAN. Nach der mündlichen Übermittlung der TAN durch den Versicherten resp. Vertreter und anschließender Eingabe durch das LEI-Personal im PS, ist der Check-in-Vorgang abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontextes.</p>

***Hinweis:** Das vom PoPP-Service erstellte PoPP-Token enthält die Information, mit welcher Methode (siehe proofMethod im [Kapitel PoPP-Token-Erstellung]) der Versorgungskontext nachgewiesen wurde. Somit ist es den PoPP-Token nutzenden Anwendungen und Diensten möglich, in ihrem Anwendungs- oder Dienstkontext Autorisierungsentscheidungen aufgrund der Prüfmethode zu treffen. So kann beispielsweise aufgrund der Prüfmethode "healthid" eine Anwendung nur einen Teil, während aufgrund der Prüfmethode "ehc-practitioner" die Anwendungen alle Anwendungsfälle autorisiert.*

2.3 Akteure und Rollen

Der PoPP-Service wird vom Anbieter PoPP-Service im Internet betrieben. Es müssen für die verschiedenen Betriebsumgebungen (Produktivumgebung (PU), Referenzumgebung(RU) und nach Bedarf die gemäß [gemKPT_Test] geforderten Test- und Referenzumgebungen (TU und RU DEV) jeweils voneinander unabhängige Instanzen betrieben werden. Für die Absicherung gegenüber dem Internet wird der von der gematik bereitgestellte ZETA Guard verwendet.

2.3.1 Herstellung und Betrieb

Folgende Rollen und Akteure kommen bei Herstellung und Betrieb des PoPP-Service vor.

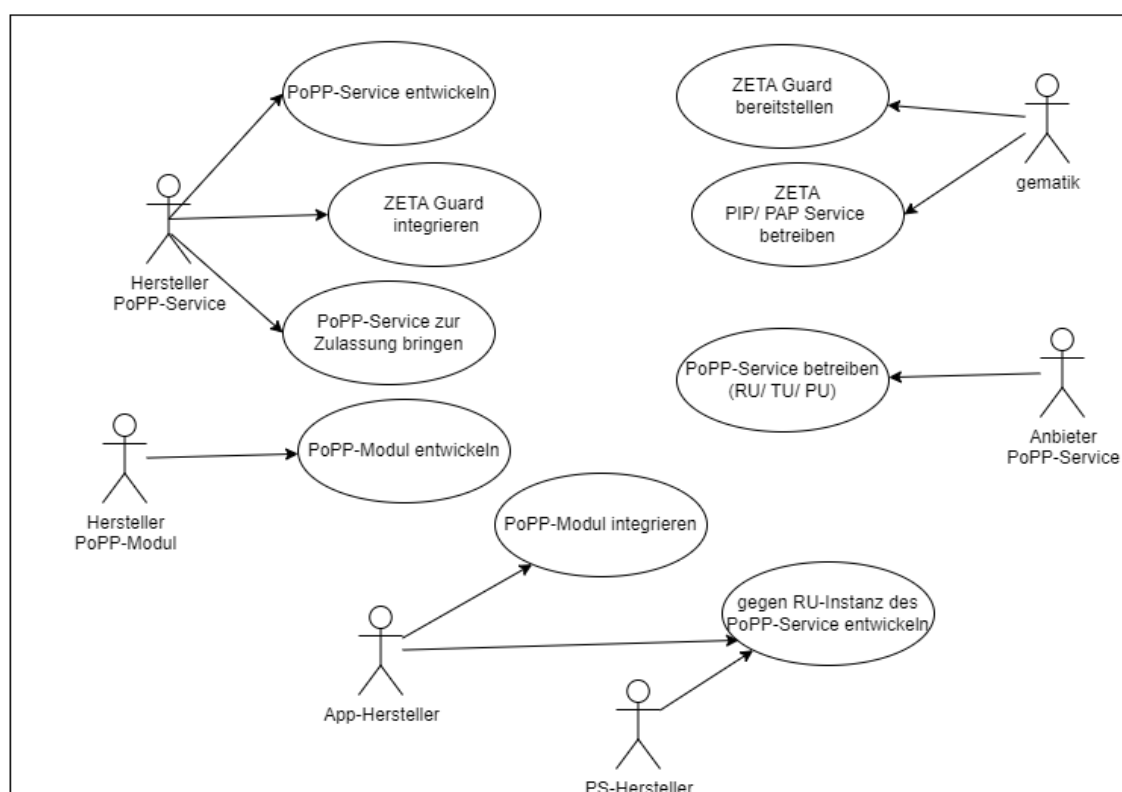


Abbildung 2: Rollen und Akteure bei Herstellung und Betrieb des PoPP-Service

2.3.1.1 Hersteller PoPP-Service

Der Hersteller des PoPP-Service implementiert und entwickelt den PoPP-Service gemäß den Vorgaben der gematik. Er erwirkt eine Produktzulassung für den PoPP-Service.

2.3.1.2 Anbieter PoPP-Service

Der Anbieter PoPP-Service verantwortet und betreibt den zugelassenen PoPP-Service gemäß den Vorgaben der gematik. Dabei muss er für die Verbindungen ins Internet, den

von der gematik beigestellten ZETA Guard verwenden.

Neben dem Betrieb von Instanzen für den Produktivbetrieb müssen weitere Instanzen für den Testbetrieb gemäß gemKPT_Test betrieben werden.

2.3.1.3 gematik

Die gematik spezifiziert den PoPP-Service und schreibt die Entwicklung und den Produktivbetrieb des PoPP-Service aus.

Die gematik unterstützt den Hersteller PoPP-Service durch die Beistellung des ZETA Guard.

Darüber hinaus betreibt die gematik die Zero Trust Komponenten Policy Information Point (PIP) und Policy Administration Point (PAP): ZETA PIP und PAP Service.

2.3.1.4 Primärsystem-Hersteller

PS-Hersteller setzen die PoPP-Client- und Trust Client-Funktionalität um. Sie nutzen den vom Anbieter in der RU bereitgestellten PoPP-Service, um ihre jeweilige Umsetzung zu testen.

2.3.1.5 Hersteller PoPP-Modul

Das PoPP-Modul ist eine Frontend-Komponente, über die Versicherte mit dem PoPP-Service interagieren und das für den mobilen Check-in verwendet wird. Das PoPP-Modul kann als Modul in einer Kassen-App oder in einer Drittanbieter-App integriert sein. Je nach Ausprägung sind Anforderungen an das PoPP-Modul zu erfüllen [gemSpec_PoPP_Modul].

2.3.1.6 Hersteller App

App Hersteller integrieren das PoPP-Modul eines PoPP-Modul Hersteller für einen mobilen Check-in Prozess. Sie entwickeln Funktionalität für die Präsentation und Übertragung von TAN aus dem Check-in Prozess an eine LEI. Sie nutzen den PoPP-Service in der RU, um die Funktionalität zu testen. Apps, welche ein PoPP-Modul integrieren, müssen sich die korrekte Implementierung durch die gematik bestätigen lassen (Bestätigungsverfahren).

2.3.1.7 Kostenträger (KTR)

Kostenträger übermitteln (oder beauftragen die Übermittlung von) Informationen zum Befüllen einer Datenbank an den PoPP-Service (siehe [Kapitel eGK-Hash-Datenbank]). Diese Informationen vereinfachen die kontaktlose Verwendung einer eGK im PoPP-Kontext.

2.3.2 Nutzer

Folgende Rollen und Akteure kommen im Betrieb der Anwendung des PoPP-Service vor.

2.3.2.1 Leistungserbringerinstitution (LEI)

Die LEI nutzen den PoPP-Service, um eine Zugriffsberechtigung (PoPP-Token) bspw. für den Abruf von Daten eines Versicherten aus seiner ePA erzeugen zu lassen. Dabei benutzt die LEI ein für die PoPP-Lösung angepasstes PS, in dem PoPP-Client-Funktionalität, Trust Client-Funktionalität und Funktionalität für eine Fachanwendung, die das PoPP-Token verwendet, implementiert ist.

2.3.2.2 Versicherte

Versicherte nutzen den PoPP-Service indirekt, wenn sie sich bei einer LEI einchecken oder auf andere Art und Weise bei der Erstellung des Versorgungskontext zwischen LEI und Versicherten mitwirken. Die Versicherten steuern ihre Krankenversicherungsnummer (KVNR) bei, indem sie sich:

1. über ihre GesundheitsID authentisieren,
2. oder sich mit ihrer eGK in der LEI vorstellen (Nutzung der Praxis Hardware für die Prüfung der eGK auf Authentizität),
3. oder sich per eGK mobil bei der LEI anmelden.
4. oder sich ein Vertreter per eGK mobil bei der LEI anmeldet.

3 Systemkontext PoPP-Service

In diesem Kapitel findet sich die logische Zerlegung des Produkttyps Proof of Patient Presence (PoPP)-Service anhand eines Komponenten-Diagramms, die Beschreibung des Systemkontexts mit allen bereitstellenden Außenschnittstellen des PoPP-Service sowie die Auflistung und kurze Beschreibung der Nachbarsysteme.

3.1 Produkt-Zerlegung und Außenschnittstellen

Der Produkttyp PoPP-Service besteht aus mehreren Komponenten. Die Komponenten für die Erstellung des PoPP-Token sind in PoPP-Service Resource Server zusammengefasst. Die Kommunikation zwischen LEI und PoPP-Service wird durch ein Zero Trust Access (ZETA) Guard abgesichert. Für die Kommunikationswege zwischen einem Versicherten und dem PoPP-Service wird ein weiterer Autorisierungsdienst, der PoPP-Service Authorization Server, benötigt, solange ein ZETA Guard diese Funktionalität noch nicht übernimmt.

Der PoPP-Service Resource Server besteht aus mehreren Komponenten für die Bearbeitung von Token Requests, bei denen die elektronische Gesundheitskarte (eGK) verwendet wird (eGK-Kommunikation, eGK-Hash-Datenbank, für den Support von kontaktlos angebunden eGK) und solchen, bei denen Versicherte die GesundheitsID verwenden (GesundheitsID-Flow, GesundheitsID-Session).

Die Komponenten für die abschließende Token-Erstellung und Versichertenstammdatenmanagement-Prüfungsnachweis (VSDM-PN Erstellung) sowie der sichere Schlüsselspeicher gehören ebenfalls zum Produkttyp. Ferner gehören betriebliche Komponenten für die Erfassung und Aufbereitung von Monitoring Daten für die gematik Betriebsdatenerfassung (BDE) und ein Security Monitoring dazu.

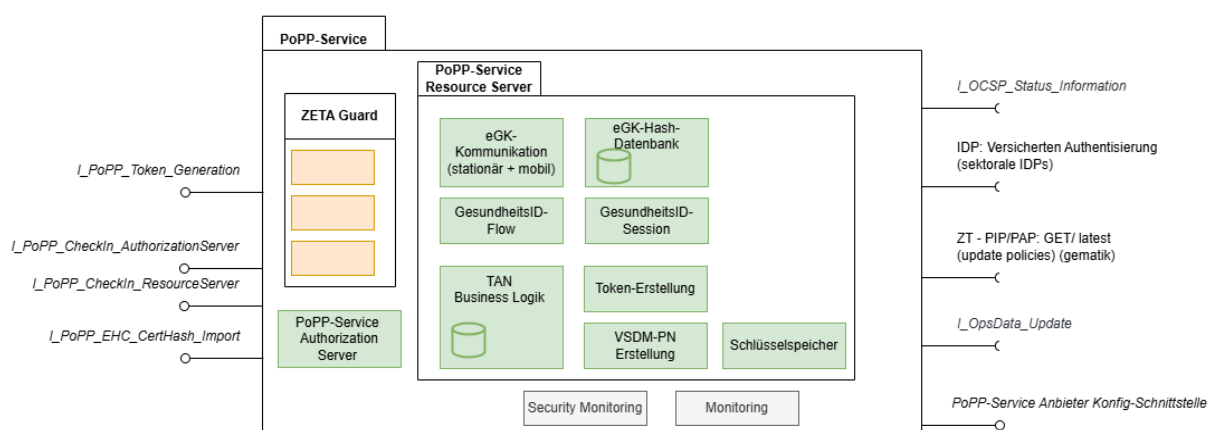


Abbildung 3: Produkttypzerlegung

Der PoPP-Service stellt folgende Außenschnittstellen bereit:

- **I_PoPP_Token_Generation** wird vom Primärsystem einer LEI verwendet um vom PoPP-Service ein PoPP-Token und ein VSDM-PN zu erlangen.
- **I_PoPP_CheckIn_AuthorizationServer** wird vom Versicherten für ein mobilen Check-in verwendet um vom PoPP-Service ein Access Token zu erlangen. Das Access Token wird benötigt um den Resource Server des PoPP-Service nutzen zu können.

- **I_PoPP_CheckIn_ResourceServer** wird vom Versicherten verwendet. Der PoPP-Service Resource Server verlangt ein Access Token und liefert ein TAN-Set.
- **I_PoPP_EHC_CertHash_Import** wird von den TSPs der Kassen aufgerufen und dient der Befüllung der CertHash-Datenbank, mittels derer das Mapping von CV-Zertifikaten zu X.509-Zertifikaten von eGKs erreicht wird. Dies dient der Unterstützung von Anwendungsfällen bei denen der Versicherte die eGK mit einem kontaktlosen Kartenlesegerät der LEI verwendet.

Der PoPP-Service benutzt die folgenden Schnittstellen:

- **IDP:** Versicherten Authentisierung (sektorale IDPs)
Wird im Anwendungsfall GesundheitsID für die Authentisierung der Versicherten vom PoPP-Service Authorization Server genutzt. Details siehe [gemSpec_IDP_Sek].
- **ZETA PIP/PAP:** GET/latest (update policies) (gematik)
Wird vom ZETA Guard für die Versorgung mit den stets aktuellen Zugriffs-Policies und weiteren Konfigurationsdaten genutzt (Details siehe [gemSpec_ZETA]).
- **I_OCSP_Status Information:**
Wird vom PoPP-Service für die Statusabfragen für eGK (PoPP-Service Resource), für SM(C)-B (ZETA Guard), für die eigenen TI 1.0 PoPP-Token-Signatur-Identität und das eigene Internet-TLS-Server-Zertifikat verwendet.
- **I_OpsData_Update:**
Wird vom PoPP-Service für die Lieferung von Betriebsdaten verwendet.

Für den PoPP-Service Anbieter wird eine interne Schnittstelle angeboten:

- **PoPP-Service Anbieter Konfig-Schnittstelle**
Interne Schnittstellen, die vom PoPP-Service Anbieter genutzt wird um den PoPP-Service zu konfigurieren

3.2 Systemkontext

Ein Systemkontext beschreibt die Umgebung, in der ein System operiert, und die Interaktionen zwischen dem System und externen Entitäten.

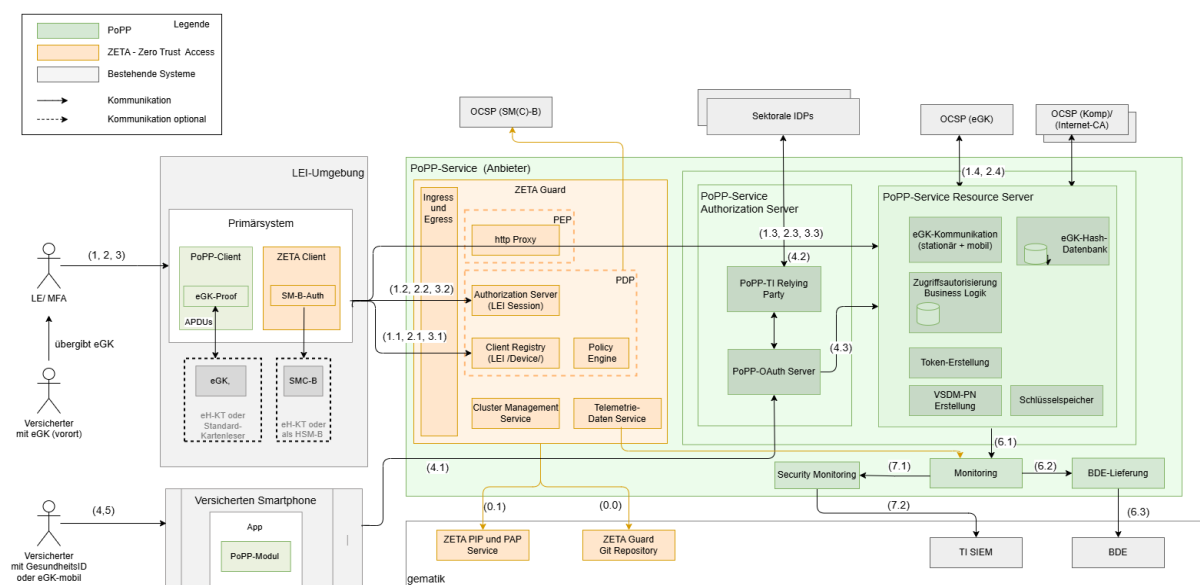


Abbildung 4: Systemkontext PoPP-Lösung

Die obige Abbildung zeigt die vom PoPP-Service Anbieter verantworteten Komponenten und Interaktionen. Die zum ZETA Guard gehörenden Komponenten sind in orange dargestellt, die Komponenten, welche die PoPP Businesslogik implementieren sind in grün dargestellt. Dargestellt sind zusätzlich heute bereits vorhandene und genutzte Komponenten und Dienste, die für die Nutzerauthentisierung (bspw. eGK und IDP) bzw. die Betriebsüberwachung (bspw. mittels Betriebsdatenerfassung - kurz BDE) in Anwendungsfällen der TI 2.0 weitergenutzt werden können (grau).

Das PS mit den beiden integrierten Modulen PoPP-Client und Trust Client triggert über verschiedene Aufrufwege die Anwendungsfälle (1), (2) und (3), nachdem bspw. eine LEI einen Check-in-Vorgang für einen Patienten initiiert hat. Die PoPP-Client Funktionalität verantwortet die fachlichen Abläufe zur PoPP-Token-Erstellung.

Die ZETA Client Funktionalität verantwortet die für Zero Trust relevante Kommunikation mit dem PoPP-Service. Dabei greift sie auf eine freigeschaltete SM(C)-B zu und benutzt diese zur Authentifizierung für die Registrierung (x.1) und Anmeldung (x.2) im Policy Decision Point (PDP) des ZETA Guard. Dabei wird ein PoPP-Client Access Token erzeugt, das für die weiteren Business-Logik Aufrufe (PoPP-Client Funktionalität) verwendet wird. Diese erfolgen dann über den Policy Enforcement Point (PEP) des ZETA Guard.

Tabelle 2: Kurzbeschreibung der Komponenten in der PoPP-Lösung

Komponente	Kurzbeschreibung	Anforderungen
PoPP-Service	Der PoPP-Service umfasst folgende Komponenten der PoPP-Lösung: <ul style="list-style-type: none"> • ZETA Guard • PoPP-Service Authorization Server • PoPP-Service Resource Server. 	
ZETA Guard	Der Zero Trust Cluster ZETA Guard schützt die Kommunikation zwischen dem PoPP-Service Resource Server und den LEI.	[gemSpec_ZETA] [Kapitel <u>ZETA Guard im PoPP-Service</u>]
PoPP-Service Authorization Server	Der PoPP-Service Authorization Server ist eine Komponente, welche nur temporär bis zur Umsetzung von ZETA für Versicherte benötigt und von ZETA später abgelöst wird. Der PoPP-Service Authorization Server umfasst folgende Komponenten: <ul style="list-style-type: none"> • PoPP-OAuth Server • PoPP-TI Relying Party 	[Kapitel <u>PoPP-Service - Authorization Server</u>]
PoPP-OAuth Server	Der PoPP Open Authorization	

	<p>(OAuth) Server ist die Komponente des PoPP-Service Authorization Server, welche anfragenden Clients (App mit integriertem PoPP-Modul) Access Token für den Zugriff auf den PoPP-Service Resource Server ausstellt.</p> <p>Je nachdem, ob sich der Versicherte mit seiner GesundheitsID oder eGK authentifiziert, wird ein "eHealth-ID-check" Access Token oder "card-check" Access Token ausgestellt.</p>	
PoPP-TI Relying Party	<p>PoPP-TI Relying Party ist die Komponente des PoPP-Service Authorization Server, welche die Kommunikation mit den sektoralen IDP bei der Authentifizierung des Versicherten mit seiner GesundheitsID übernimmt.</p>	
PoPP-Service Resource Server	<p>PoPP-Service Resource Server enthält die eigentliche Businesslogik des PoPP-Service für das Ausstellen von TAN an Versicherte und PoPP-Token an LEI-Systeme.</p>	
eGK-Kartenkommunikation	<p>In der Komponente eGK-Kartenkommunikation sind die Funktionalitäten für die Token-Erstellung in den Fällen, wenn ein Versicherter mittels seiner eGK beteiligt ist.</p>	[Kapitel <u>eGK-Handling</u>]
eGK-Hash-DB	<p>Die Komponente eGK-Hash-DB enthält die Datenbank und steuernde Funktionalität für den Abgleich von anonymisierten eGK-Metadaten für die Unterstützung der kontaktlosen Nutzung von eGK.</p>	[Kapitel <u>eGK-Hash-Datenbank</u>]
Zugriffsautorisierung (Business Logik und DB)	<p>Die Komponente Zugriffsautorisierung enthält die Datenbank für die TAN-Set-Datensätze und die steuernde Funktionalität, wenn ein Versicherter einen mobilen</p>	[Kapitel <u>Zugriffsautorisierung und Business-Logik</u>]

	Check-in durchführt.	
Token-Erstellung	Die Komponente Token-Erstellung enthält die Funktionalität zum Erstellen des PoPP-Token; hier werden die Daten von der LEI und dem Versicherten im PoPP-Token zusammengefügt.	[Kapitel <u>PoPP-Token: Nachweis des Versorgungskontextes</u>]
VSDM-PN-Erstellung	Die Komponente 'VSDM-PN Erstellung' bietet die Funktionalität, während einer Übergangszeit zusätzlich zum PoPP-Token einen Prüfnachweis nach dem alten VSDM 1.0 - Muster zu erstellen. Dieser Nachweis wird dem Token-Response hinzugefügt.	[Kapitel <u>PoPP-Token: Nachweis des Versorgungskontextes</u>]
Schlüsselspeicher	Die Komponente Schlüsselspeicher enthält die Funktionalität zur sicheren Ablage der verwendeten Schlüssel und zur Speicherung von Daten.	[Kapitel <u>Speicherung von Daten</u>] [Kapitel <u>5.2.1.6-Schlüsselnutzung direkt im Verarbeitungskontext</u>]
Monitoring	Die Komponente Monitoring sammelt Funktionalitäten für das Eigen-Monitoring der verwendeten Systeme zur Überwachung und Analyse des Betriebszustandes.	(bis zur Veröffentlichung in C_11939)
BDE-Lieferung	Die Komponente BDE-Lieferung fasst die Daten des PoPP-Service für die Betriebsdatenerfassung (BDE) der gematik zusammen und versendet sie.	(bis zur Veröffentlichung in C_11939)
Security Monitoring	Die Komponente Security Monitoring enthält Funktionen für das Sicherheits- und Event-Monitoring im PoPP-Service.	(bis zur Veröffentlichung in C_11939)
Primärsystem (PS)	Bestehende Primärsysteme werden für PoPP erweitert.	
ZETA Client	Der Trust Client (ZETA Client)	[gemSpec_ZETA]
PoPP-Client	Der PoPP-Client ist der direkte Kommunikationspartner des	[gemILF_PoPP_Client]

	PoPP-Service im PS einer LEI.	
App	App ist eine Kassen-App oder Drittanbieter-App (Smartphone-App, Desktop-Anwendung, Browser-Anwendung), die von einem Versicherten mit GesundheitsID oder einem Versicherten mit eGK mobil genutzt wird.	
PoPP-Modul	Das PoPP-Modul übernimmt beim mobilen Check-in die Kommunikation mit dem PoPP-Service . Das PoPP-Modul verwaltet TAN-Sets, die es vom PoPP-Service im Rahmen eines mobilen Check-ins erhält und hilft bei der Übertagung einer TAN an das Primärsystem.	[gemSpec_PoPP_Modul]

3.3 Nachbarsysteme

In der Abbildung "Systemkontext PoPP-Lösung" sind die Nachbarsysteme des PoPP-Service dargestellt:

- Sektoraler IDP:
verantwortlich für die Authentisierung eines Versicherten mit GesundheitsID,
- OCSP-Responder des TSP für SM-B:
im Internet verfügbar für die OCSP-Prüfung von SM-B durch den ZETA Guard,
- OCSP-Responder des TSP für eGK:
im Internet verfügbar für die OCSP-Prüfung von eGK durch den PoPP-Service,
- OCSP-Responder des TSP für Komponenten PKI:
im Internet verfügbar für die OCSP-Prüfung des TI 1.0 Komponenten Zertifikats der PoPP-Service Identität, verwendet bei der Signatur der Application Protocol Data Units (APDU) im eGK-Ablauf,
- OCSP-Responder Internet-CA:
im Internet verfügbar für die OCSP-Prüfung des TLS-Internet-Zertifikats des PoPP-Service (für die Client-Schnittstelle)
- die gematik stellt folgende Dienste bereit:
PIP und PAP Service für Zero Trust, git-Repository für die ZETA Guard Images, Überwachung und Betriebsdatenerfassung: BDE und Telematikinfrastruktur Security Information and Event Management (TI-SIEM).

In der Abbildung "Systemkontext PoPP-Lösung" sind folgende nutzende Systeme nicht dargestellt:

- Fachanwendungen und FD im Internet, sowie Dienste und Komponenten, die noch in der TI 1.0 verortet sind, wie E-Rezept-FD, ePA < 3.x:
 - VSDM 2.0,

- "ePA für alle": Kann PoPP-Token oder VSDM-PN nutzen, abhängig von der ePA-Entwicklungsstufe,
- E-Rezept: Kann ebenfalls PoPP-Token oder VSDM-PN nutzen, abhängig von der eRp-FD- Entwicklungsstufe.

Außerdem sind die App-Backend-Systeme der nicht abgebildet.

4 Funktionale Anwendungsfälle des PoPP-Service

In diesem Kapitel werden die Anwendungsfälle beschrieben, die von der Proof of Patient Presence (PoPP)-Lösung abgedeckt werden. Die Anwendungsfälle zum mobilen Check-in mit elektronischer Gesundheitskarte (eGK) oder GesundheitsID resultieren in einer Transaktionsnummer (TAN), welche in einem weiteren Anwendungsfall in ein PoPP-Token eingetauscht werden kann. Der Anwendungsfall eines Check-in mit eGK direkt bei der Leistungserbringerinstitution (LEI) führt hingegen direkt zur Ausstellung eines PoPP-Token für die LEI.

Neben der Erstellung eines PoPP-Token wird auch die Registrierung und Anmeldung der LEI betrachtet. Ausgangspunkt sind die PoPP-Use Cases aus Tabelle "PoPP-Use Cases (Business Sicht)".

4.1 Übersicht der Systemanwendungsfälle für die Ausstellung des PoPP-Token

Die Anwendungsfälle für die Ausstellung eines PoPP-Token lassen sich in drei Gruppen einteilen:

- Anwendungsfälle zur Authentisierung einer LEI,
- Anwendungsfälle, wie sich ein Versicherter für die Ausstellung des PoPP-Token authentisiert,
- Anwendungsfälle, die beschreiben, wie die Ausgabe des PoPP-Token an das PS einer LEI erfolgt.

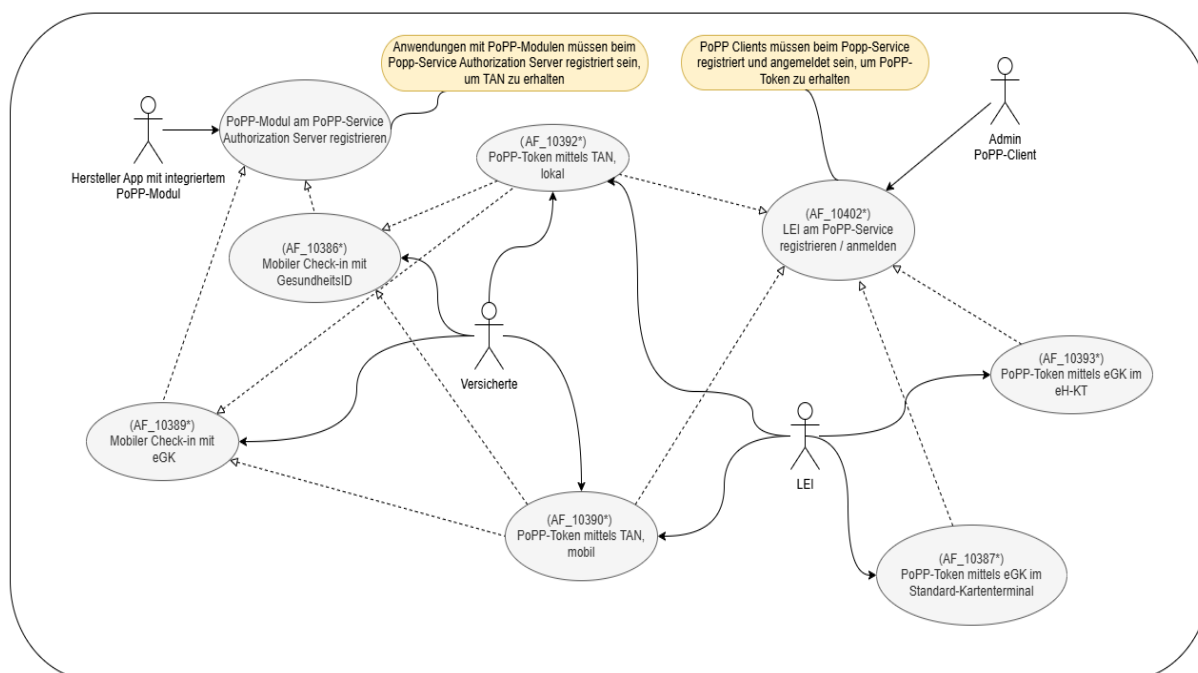


Abbildung 5: Anwendungsfälle zur Attestierung des Versorgungskontextes

Zur Umsetzung der in der Tabelle "PoPP-Use Cases (Business Sicht)" dargestellten Use Cases ist der Ablauf folgender Anwendungsfall-Ketten erforderlich:

Tabelle 3: Zuordnung der Anwendungsfälle zu den Use Cases

Anwendungs-fall	Kurzbeschreibung	technische Anwendungsfälle
UC_PoPP_1a	PoPP-Token bei physischer Anwesenheit in der LEI - GesundheitsID - Scanner vorhanden	<ol style="list-style-type: none"> erst AF_10386* - Mobiler Check-in mit GesundheitsID dann AF_10392* - PoPP-Token mittels TAN, lokal; "lange" TAN
UC_PoPP_1b	PoPP-Token bei physischer Anwesenheit in der LEI - GesundheitsID - Scanner nicht vorhanden	Identisch zu UC_PoPP_1a, aber "kurze" TAN statt "lange" TAN
UC_PoPP_1c	PoPP-Token bei physischer Anwesenheit in der LEI - eGK	<ol style="list-style-type: none"> entweder AF_10393* - PoPP-Token mittels eGK im eH-KT oder AF_10387* - PoPP-Token mittels eGK im Standard-Kartenterminal
UC_PoPP_2a	PoPP-Token bei physischer Anwesenheit außerhalb der LEI - GesundheitsID - Scanner vorhanden	Identisch zu UC_PoPP_1a
UC_PoPP_2b	PoPP-Token bei physischer Anwesenheit außerhalb der LEI - GesundheitsID - Scanner nicht vorhanden	Identisch zu UC_PoPP_1b
UC_PoPP_2c	PoPP-Token bei physischer Anwesenheit außerhalb der LEI - eGK	Identisch zu UC_PoPP_1c
UC_PoPP_3a	PoPP-Token ohne physische Anwesenheit in der LEI - GesundheitsID - digitaler Kommunikationsweg ins PS vorhanden	<ol style="list-style-type: none"> erst AF_10386* - Mobiler Check-in mit GesundheitsID dann AF_10390* - PoPP-Token mittels TAN, mobil; "lange" TAN
UC_PoPP_3b	PoPP-Token ohne physische Anwesenheit in der LEI - GesundheitsID - digitaler Kommunikationsweg ins PS nicht vorhanden	Identisch zu UC_PoPP_3a, aber "kurze" TAN statt "lange" TAN
UC_PoPP_3c	PoPP-Token ohne physische Anwesenheit in der LEI - eGK	<ol style="list-style-type: none"> erst AF_10389* - Mobiler Check-in mit eGK

	(mobil) - digitaler Kommunikationsweg ins PS vorhanden	2. dann AF_10390* - PoPP-Token mittels TAN, mobil; "lange" TAN
UC_PoPP_3d	PoPP-Token ohne physische Anwesenheit in der LEI - eGK (mobil) - digitaler Kommunikationsweg ins PS nicht vorhanden	Identisch zu UC_PoPP_3c, aber "kurze" TAN statt "lange" TAN

Nach dem mobilen Check-in stehen den Versicherten im PoPP-Modul seiner App TANs zur Verfügung.

Bei den Use-Cases UC_PoPP_1a, UC_PoPP_2a, UC_PoPP_3a und UC_PoPP_3c sind im PoPP-Modul mehrere "lange" TAN in einem TAN-Set verfügbar.

Bei den Use-Cases UC_PoPP_1b, UC_PoPP_2b, UC_PoPP_3b und UC_PoPP_3d ist im PoPP-Modul nur eine einzelne "kurze" TAN verfügbar, die ist stets nur von genau einer LEI gegen ein PoPP-Token einlösbar ist.

Der Use-Case UC_PoPP_1a deckt auch den Sachverhalt ab, wenn ein Versicherter bspw. in einem Ärztehaus mehrere LEI aufsucht.

Der Use-Case UC_PoPP_2a deckt auch den Sachverhalt ab, dass beispielsweise ein Versicherter nacheinander von mehreren Leistungserbringern zu Hause besucht wird.

Der Use-Case UC_PoPP_3a deckt auch den Sachverhalt ab, dass beispielsweise ein Versicherter nacheinander bei mehreren LEIs in einer Videosprechstunde vorspricht.

Die benannten Anwendungsfälle werden in den nachfolgenden Kapiteln beschrieben. Anwendungsfälle werden wie Anforderungen behandelt, das heißt, die beschriebenen Sequenzen und Abläufe sind normativ.

4.2 Leistungserbringerinstitution (LEI) am PoPP-Service registrieren und anmelden

Um mit dem PoPP-Service arbeiten zu können, muss sich das PS einer LEI am PoPP-Service registrieren und anmelden. Die Registrierung erfolgt einmalig mit dem ZETA Client im PS unter Verwendung des Zero Trust Access (ZETA) Guard des PoPP-Service. Die Anmeldung für registrierte PS erfolgt über seine Authentifizierung gemäß [gemSpec_ZETA] mindestens einmal täglich.

Die Registrierung und die Anmeldung der LEI erfolgen implizit bei der Verwendung des PoPP-Service zur Erstellung eines PoPP-Token. Seitens der LEI ist eine freigeschaltete SM(C)-B erforderlich. Sind diese Voraussetzungen gegeben, kann beim Check-in von Versicherten in der LEI dann der Versorgungskontext mit einem PoPP-Token attestiert werden.

Die Anforderungen und Abläufe für die Registrierung der LEI sind in [gemSpec_ZETA#Kap. Ablauf der SM-B Authentifizierung mit DPoP] beschrieben. Im Ergebnis der LEI-Registrierung und -Anmeldung liegt im PS ein Access Token mit Demonstrating Proof of Possession (DPoP) Bindung vor, mit welchem der funktionale Zugriff des PS auf den PoPP-Service erlaubt wird.

Sobald ein PS am PoPP-Service erfolgreich registriert wurde und angemeldet ist, kann es PoPP-Token erzeugen lassen bzw. abrufen.

AF_10402 - LEI am PoPP-Service registrieren / anmelden

Attribute	Bemerkung
Beschreibung	Die LEI registriert sich am PoPP-Service und meldet sich am PoPP-Service an, indem sie sich gegenüber diesem authentifiziert. Nach erfolgreicher Anmeldung kann die LEI über das PS PoPP-Token für einen Versicherten beim PoPP-Service abrufen.
Vorbedingung	<ul style="list-style-type: none"> • SM(C)-B ist freigeschaltet. • Einboxkonnektor mit eHealth-Kartenterminal (eH-KT) und SMC-B oder TI-Gateway mit Highspeed-Konnektor und SMC-B als Karte im eH-KT oder als SM-B im Hardware-Sicherheitsmodul (HSM) des HSK, • PS implementiert einen PoPP-Client. • PS implementiert einen Trust Client.
Ablauf	Technische Beschreibung siehe in [gemSpec_ZETA#Kapitel Ablauf der SM-B Authentifizierung mit DPoP A_26091*]
Nachbedingung	<ul style="list-style-type: none"> • Die LEI ist am PoPP-Service registriert und angemeldet. • Im PS liegt ein Access Token mit DPoP Bindung vor. Es wird verwendet, um PoPP-Token Anforderungen der LEI im Resource Server des PoPP-Service zu bearbeiten.
Akzeptanzkriterien	<ul style="list-style-type: none"> • <u>Bearbeitung von Anfragen nach Authentifizierung eines PoPP-Clients</u>
Alternativen	keine

[<=]

ML-164206 - Bearbeitung von Anfragen nach Authentifizierung eines PoPP-Clients

Nach erfolgreicher Registrierung und Authentifizierung mit DPoP gemäß [gemSpec_ZETA] ist der PoPP-Client dem PoPP-Service bekannt. Eingehende Anfragen des PoPP-Clients MUSS der PoPP-Service Resource Server entgegennehmen und verarbeiten.

[<=]

4.3 Mobiler Check-in und Ausgabe des PoPP-Token

Versicherte haben die Möglichkeit, sich unabhängig vom Ort für eine Leistungserbringung anzumelden (mobiler Check-in). Der mobile Check-in erfolgt dabei unter Verwendung einer Anwendung, die ein PoPP-Modul integriert (siehe [gemSpec_PoPP_Modul]). Als Ergebnis einer Autorisierungsanfrage des PoPP-Moduls an den PoPP-Service Authorization Server kann das PoPP-Modul die Ausstellung einer TAN beim PoPP-Service selbst beantragen. Die Konstellation für die Ausstellung einer TAN unterscheiden sich in den Punkten:

- Hat die App mit integrierte PoPP-Modul das Bestätigungsverfahren erfolgreich durchlaufen?

- Handelt es sich um ein virtuelles Anwendungsszenario wie Videosprechstunde oder Online-Apotheke oder ist der mobile Check-in die Vorbereitung einer Vorstellung am Ort der Leistungserbringung (Praxis, Klinik)?
- Ist die LEI zum Zeitpunkt des Check-in bekannt?
- Welche Übertragungskanäle bietet die LEI für eine Übertragung einer TAN an?

Starten die Versicherten den Check-in-Prozess über das in eine App integrierte PoPP-Modul, so ist sowohl eine Authentisierung mit GesundheitsID als auch mit eGK (mobil) über direktes Auslesen durch den PoPP-Service Resource Server möglich.

Nach erfolgreicher Authentisierung mit GesundheitsID oder eGK (mobil) werden vom PoPP-Service Authorization Server Access Token erstellt, mit denen autorisierte Zugriffe auf die Schnittstellen des PoPP-Service Resource Server durch das PoPP-Modul durchgeführt werden.

Reicht das PoPP-Modul ein Access Token für eine Authentifizierung der eGK (mobil) beim PoPP-Service Resource Server ein ("card-check" Access Token), so führt dieser eine Kartenprüfung durch Ansprechen der eGK-Schnittstellen durch und entnimmt die notwendigen Daten des Versicherten aus der eGK.

Reicht das PoPP-Modul ein Access Token nach erfolgreicher Authentisierung mit GesundheitsID beim PoPP-Service Resource Server ein ("eHealth-ID-check" Access Token), so enthält das Access Token bereits die Daten zum Versicherten aus dem vom sektoralen Identity Provider (sektoralen IDP) ausgestellten ID Token (siehe [gemSpec_IDP_Sek]).

Über das in eine App integrierte PoPP-Modul ist es möglich ein TAN-Set mit "langen" TAN vom PoPP-Service ohne Kenntnis der LEI zu beziehen, bei der die TAN später eingesetzt werden sollen. Ebenso ist eine Auswahl einer LEI direkt beim Check-in möglich. Das PoPP-Modul erhält dann einen "kurze" TAN vom PoPP-Service Resource Server, welche nur bei dieser LEI einlösbar ist.

Die folgende Abbildung zeigt die Abläufe je nach Konstellation des PoPP-Modul.

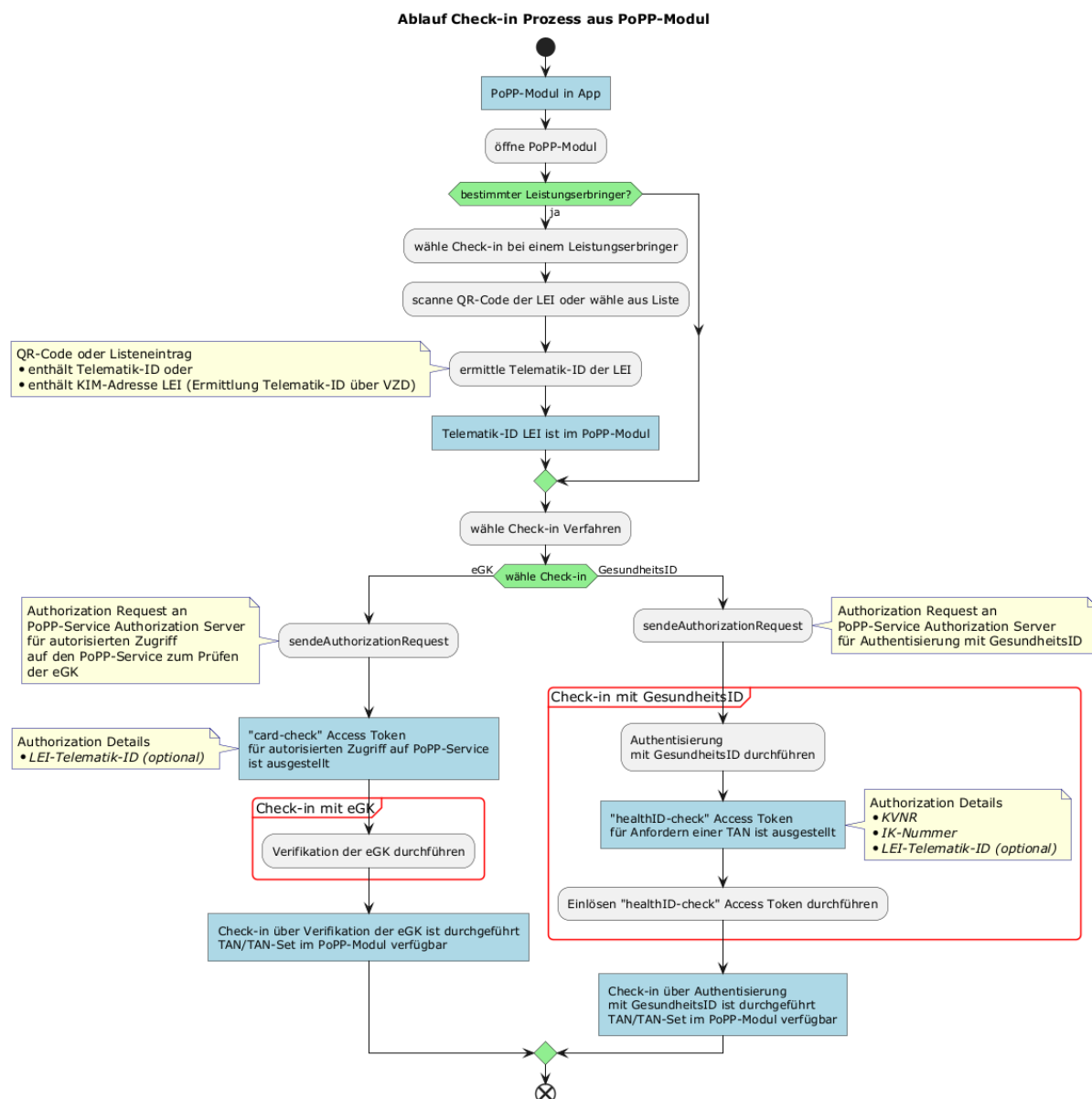


Abbildung 6: Abläufe Check-in für unterschiedliche Konstellationen

In den folgenden Abschnitten werden die Anwendungsfälle und detaillierten Abläufe beschrieben.

4.3.1 Mobiler Check-in mit GesundheitsID

Ein Versicherter kann die Authentisierung mit seiner GesundheitsID nutzen, um sich in einer LEI oder außerhalb einer LEI (bspw. für eine Videosprechstunde) anzumelden. Zum Zeitpunkt der Anmeldung muss der Versicherte nicht notwendigerweise Informationen über die LEI zur Verfügung haben. Vielmehr wird ihm im Zuge der Anmeldung eine TAN oder ein TAN-Set bestehend aus mehreren TAN (TAN Repräsentation in Form eines QR-Code oder einer Zeichenkette) übermittelt, welches er anschließend bei einer LEI vor Ort oder virtuell -bspw. für eine Videosprechstunde- einlösen kann.

PoPP-Modul	PoPP-Service Authorization Server	sektoraler IDP Kasse	PoPP-Service Resource Server
<p>Check in mit eID</p> <p>Authentifizierung Details</p> <ul style="list-style-type: none"> Client-ID Authentifizierender Bsp (optional, wenn notwendig) TeleMarkt-ID LEI (optional, wenn zuvor ausgestellt) <p>HealthID-check' Access Token in PoPP-Modul</p> <p>Request Header "HealthID-check" Access Token ist Authentifizierung Details</p> <ul style="list-style-type: none"> ja/nein ID-Nummer LEI-TeleMarkt-ID (optional) <p>Token-Valid</p> <ul style="list-style-type: none"> als virtueller Short als QR-Code im PoPP-Modul darstellbar <p>Token-Invalid</p> <p>Token-Valid sind in QR-Code im PoPP-Modul darstellbar</p> <p>Check in über Authentifizierung des GesundheitsID zu beschleunigten Token-Set in PoPP-Modul verfügbar?</p> <p>Wurde im PoPP-Modul zuvor eine LEI ausgestellt, so gibt es genau eines "kurze" TAN. Wurde im PoPP-Modul zuvor keine LEI ausgestellt, so gibt es ein TAN-Set mit konfigurierter Anzahl "langer" TANs.</p>	<p>sende PoPP-Auth Request</p> <p>erzeuge "HealthID-check" Access Token</p> <p>Authentifizierung Details</p> <ul style="list-style-type: none"> KVVH aus ID-Token QR-Nummer aus ID-Token TeleMarkt-ID LEI (optional) <p>speichere "HealthID-check" Access Token</p> <p>sende "HealthID-check" Access Token an PoPP-Modul</p> <p>erzeuge ID-Token mit KVVH und ID-Nummer</p>	<p>Gibne Authentifizierungsantrag durch</p> <p>hole Einwilligung des Versicherungs ein</p> <p>erzeuge ID-Token mit KVVH und ID-Nummer</p>	<p>validiere "HealthID-check" Access Token</p> <p>entferntes "HealthID-check" Access Token</p> <p>entferntes KVVH/ID-Nummer aus "HealthID-check" Access Token</p> <p>erzeuge TeleMarkt-ID aus "HealthID-check" Access Token</p> <p>TeleMarkt-ID-Set?</p> <p>erzeuge "kurze" TAN zu TeleMarkt-ID</p> <p>erzeuge TAN-Set mit konfigurierter Anzahl "langer" TANs</p> <p>erzeuge TAN-Set-Record</p> <p>TAN-Set-Record?</p> <p>speichere TAN-Set-Record</p> <p>sende TAN/TAN-Set</p> <p>speichere TAN-Set-Record</p> <p>TAN/TAN-Set?</p> <p>sende TAN/TAN-Set</p> <p>Anzahl der TANs im PoPP-Service konfiguriert</p> <p>Authentifizierung Details</p> <ul style="list-style-type: none"> KVVH ID-Nummer TAN-TAN-Set Zusätzlicher Eintrag (ID) Zusätzlicher Ablauf (exp) <p>Authentifizierung Details</p> <ul style="list-style-type: none"> TAN/TAN-Set Zusätzlicher Ablauf (exp)

AF 10386 - Mobiler Check-in mit GesundheitsID

Attribute	Bemerkung
Beschreibung	<p>Der Versicherte startet den Prozess zur Attestierung eines Versorgungskontextes, indem er über das in einer App integrierte PoPP-Modul eine Authentisierung mit seiner GesundheitsID anstößt. Aus Sicht des Versicherten unterscheidet sich der Ablauf der Authentisierung nicht von den Abläufen zur Anmeldung an anderen TI-Anwendungen wie elektronische Patientenakte (ePA) oder Elektronisches Rezept (E-Rezept). Der Versicherte muss zu diesem Zeitpunkt nicht unbedingt wissen/entscheiden, bei welcher LEI er sich anmeldet.</p> <p>Nach erfolgreicher Authentifizierung wird dem Versicherten eine TAN oder ein TAN-Set mit einer konfigurierbaren Anzahl an TAN ausgestellt. Jede TAN lässt sich in Form eines QR-Code einer LEI präsentieren.</p>

Vorbedingungen	<p>Vorbedingungen:</p> <ol style="list-style-type: none"> 1. Zum Zeitpunkt der Authentisierung des Versicherten muss dieser einen Internetzugang haben. Der Authentisierungsprozess muss nicht zwingend am Ort der LEI erfolgen. Ein Internetzugang für die Versicherten am Ort der Leistungserbringung ist nicht zwingend notwendig. 2. Der Versicherte verwendet die eine App mit integrierten PoPP-Modul. Die App ist beim PoPP-Service Authorization Server registriert. 3. Die GesundheitsID ist für den Versicherten im sektoralen IDP seiner Krankenkasse eingerichtet. 4. Der Versicherte kann sich über sein Smartphone gegenüber des sektoralen IDP seiner Krankenkasse authentifizieren.
Ablauf	<p>Authentisierung des Versicherten mit seiner GesundheitsID:</p> <ol style="list-style-type: none"> 1. Der Versicherte öffnet in das in die App integrierte PoPP-Modul. Je nach Implementierung könnte sich das PoPP-Modul in der User Experience (UX) bspw. als "online Check-in", "Arztbesuch vorbereiten" oder "Videosprechstunde beitreten" o.ä. darstellen. 2. Der Versicherte wählt eine LEI (bspw. über eine Liste oder durch das Scannen eines QR-Code) aus. Dieser Schritt ist optional. 3. Der Versicherte wählt aus der Liste der registrierten sektoralen IDP seine Kasse aus. Dieser Schritt ist nur notwendig, wenn die Information in der App nicht vorliegt (in den Kassen-Apps liegen die Informationen vor, hier wird der Schritt nicht benötigt). 4. Das PoPP-Modul sendet einen Authorization Request an den PoPP-Service Authorization Server unter folgenden Angabe: <ol style="list-style-type: none"> a. der Client-ID des PoPP-Modul, welche im Registrierungsprozess vergeben wurde, b. der Telematik-ID der ausgewählten LEI (optional, wenn durch Nutzer eine Auswahl erfolgt ist) und c. den Identifier des sektoralen IDP (optional, wenn durch Nutzer eine Auswahl erfolgt ist). 5. Der PoPP-Service Authorization Server prüft, ob ein Client mit der angegebenen Client-ID registriert ist. 6. Über den PoPP-Service Authorization Server wird die Authentisierung des Versicherten am sektoralen IDP der Kasse initiiert. 7. Beim Versicherten öffnet sich das Authenticator-Modul des sektoralen IDP, je nach Implementierung, in der Kassen-App oder als eigene Authenticator-App. 8. Dem Versicherten wird ein Consent-Dialog mit der Information angezeigt, dass der PoPP-Service die KVNR des Versicherten abfragen möchte. (Der Consent Dialog ist Bestandteil des Authenticator-Moduls des sektoralen IDP [gemSpec_IDP_Sek]. Er ist so gestaltet, dass der Versicherte den Zweck der Information erkennt und sich klar für eine Zustimmung oder Ablehnung

	<p>entscheiden kann. Die Abfrage des Consents erfolgt einmalig und wird dann seitens sektoraler IDP gespeichert. Der Anwender hat die Möglichkeit die Zustimmung jederzeit über die Nutzerpräferenzen im Authenticator-Modul zu widerrufen).</p> <ol style="list-style-type: none">9. Lehnt der Versicherte die Anfrage ab, so wird der Prozess abgebrochen. Der Versicherte wird über einen entsprechend gestalteten Dialog darüber informiert.10. Stimmt der Versicherte zu, so präsentiert ihm das Authenticator-Modul als Nächstes die Auswahl der möglichen Authentisierungsmittel.11. Der Versicherte authentisiert sich mit einem der Authentisierungsmittel.12. Nach erfolgreicher Authentifizierung wird vom PoPP-Service Authorization Server für das PoPP-Modul ein "eHealth-ID-check" Access Token mit folgenden Informationen ausgestellt:<ol style="list-style-type: none">a. KVNR des Versicherten,b. IK-Nummer der Krankenkasse,c. Anzahl der angeforderten TAN (optional),d. Telematik-ID einer LEI (optional).13. Das PoPP-Modul erhält das "eHealth-ID-check" Access Token vom PoPP-Service Authorization Server. <p>Erstellung der TAN und des TAN-Sets</p> <ol style="list-style-type: none">1. Das PoPP-Modul fordert mit Übergabe des "eHealth-ID-check" Access Token ein TAN-Set beim PoPP-Service Resource Server an.2. Der PoPP-Service Resource Server entnimmt nach Validierung und Entschlüsselung des "eHealth-ID-check" Access Token aus diesem die Informationen:<ol style="list-style-type: none">a. KVNR des Versicherten,b. IK-Nummer der Krankenkasse erstellt.c. Anzahl der angeforderten TAN (optional),d. Telematik-ID einer LEI (optional).3. Der PoPP-Service Resource Server erstellt mit KVNR und IK-Nummer den Versichertenanteil der Attestierung in Form eines Datensatzes (TANSet-Record) für die Erstellung eines PoPP-Token.4. Auf Basis der ermittelten Informationen generiert der PoPP-Service:<ol style="list-style-type: none">a. eine "kurze" TAN, wenn die Telematik-ID der LEI bekannt ist.b. ein TAN-Set mit der angeforderten Anzahl an "langen" TAN, wenn keine Telematik-ID einer LEI zum Zeitpunkt des Check-in bekannt ist.5. Der PoPP-Service Resource Server speichert die generierte TAN bzw. das generierte TAN-Set und einen Zeitstempel im TANSet-
--	--

	<p>Record.</p> <p>6. Der PoPP-Service Resource Server speichert im TANSet-Record die proofMethod gemäß [I_PoPP_Token_Generation.yaml].</p> <p>7. Der PoPP-Service Resource Server übermittelt dem PoPP-Modul die generierte TAN bzw. das generierte TAN-Set und den Zeitstempel zu dem die Gültigkeit von TAN/TAN-Set abläuft.</p>
Nachbedingung	TAN bzw. TAN-Set werden bei Nichtverwendung nach Ablauf des übermittelten Zeitstempels vom Gerät des Versicherten gelöscht.
Akzeptanzkriterien	<ul style="list-style-type: none"> • <u>AF_10386 - TAN ist erstellt und als QR-Code im PoPP-Modul darstellbar</u> • <u>AF_10386 - Vorbereitung zur Attestierung des Versorgungskontextes mit TANSet-Record</u> • <u>AF_10386 - Löschen einer TAN</u>
Alternativen	Alternativ zur GesundheitsID kann der Versicherte den Versorgungskontext mit seiner eGK attestieren.

Hinweis 1: Der Gültigkeitszeitraum einer TAN bzw. eines TAN-Sets wird durch den Gültigkeitszeitraum des TANSet-Record (A_27328) festgelegt.*

Hinweis 2: In den Fällen, wo ein TAN-Set mit mehreren TAN generiert wird, ist die Anzahl der zu generierenden TAN konfigurierbar (A_26567).【<=】*

4.3.2 Mobiler Check-in mit eGK

Ein Versicherter mit eGK befindet sich außerhalb einer LEI (bspw. für eine Videosprechstunde) und nutzt die eGK mit seinem Smartphone, um sich anzumelden. Zum Zeitpunkt der Anmeldung muss der Versicherte nicht notwendigerweise Informationen über die LEI zur Verfügung haben. Vielmehr wird ihm im Zuge der Anmeldung je nach Anfrageinhalten des PoPP-Modul eine "kurze" TAN oder ein TAN-Set bestehend aus mehreren "langen" TAN übermittelt. Die TAN können in Form eines QR-Code oder einer Zeichenkette im PoPP-Modul präsentiert werden.

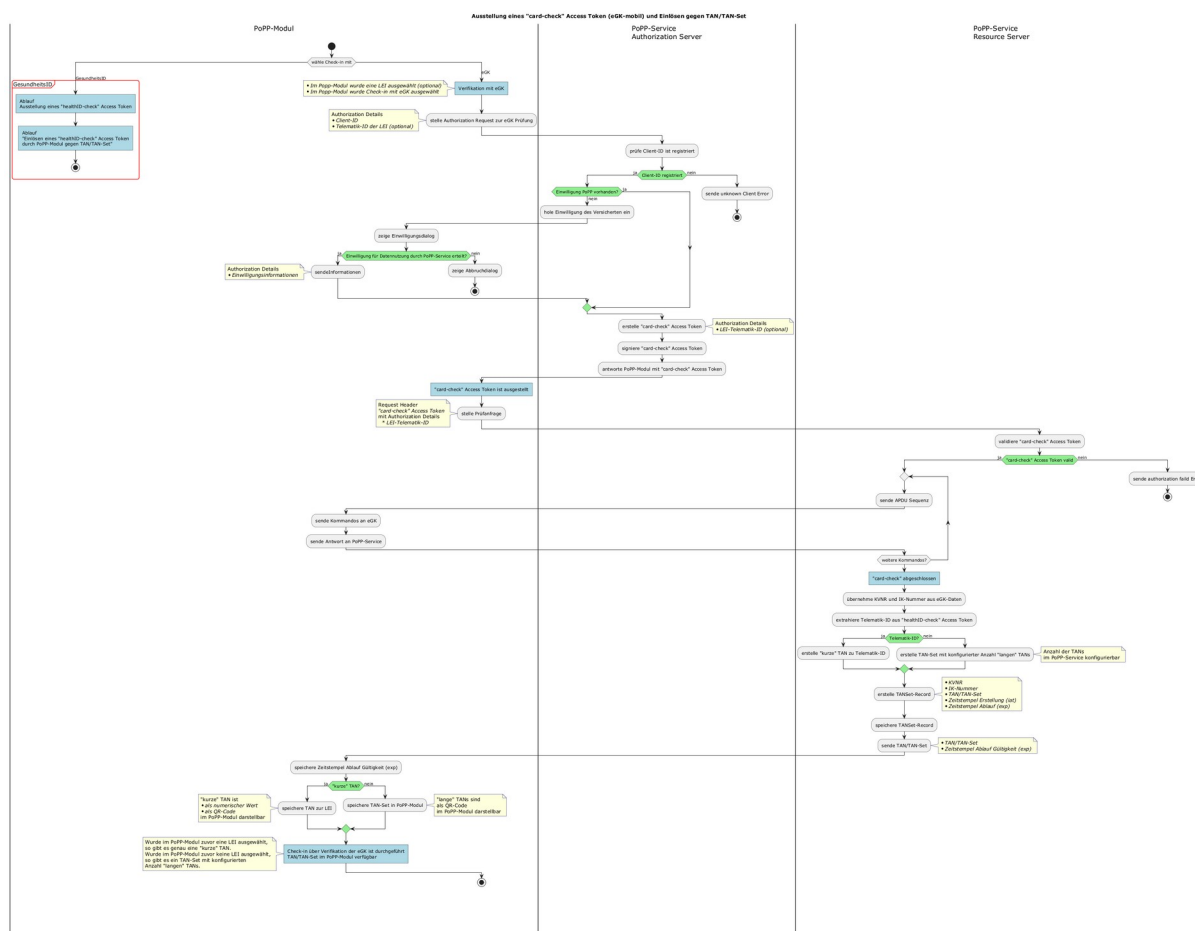


Abbildung 8: Ausstellen und Einlösen eines "card-check" Access Token
AF 10389 - Mobiler Check-in mit eGK

Attribute	Bemerkung
Beschreibung	<p>Versicherter und LEI kommunizieren virtuell, sie sind nicht physisch am gleichen Ort.</p> <p>Der Versicherte startet den Prozess zur Attestierung eines Versorgungskontextes, indem er über das PoPP-Modul in der App den Check-in durch die Authentisierung seiner eGK am PoPP-Service anstößt.</p> <p>Die eGK des Versicherten wird über ein geeignetes Medium ausgelesen (bspw. Auslesen über NFC bei Verwendung einer App auf dem Smartphone oder Kartenlesegerät bei einer Desktop-Anwendung).</p> <p>Der Versicherte muss zu diesem Zeitpunkt nicht unbedingt wissen/entscheiden, bei welcher LEI er sich anmeldet.</p> <p>Nach erfolgreicher Authentisierung der eGK wird dem Versicherten eine TAN oder ein TAN-Set mit einer konfigurierbaren Anzahl an TAN ausgestellt. Jede TAN lässt sich in Form eines QR-Code einer LEI präsentieren.</p>

Vorbedingung	<ol style="list-style-type: none">1. Zum Zeitpunkt der Authentisierung des Versicherten muss dieser einen Internetzugang haben. Der Authentisierungsprozess muss nicht zwingend am Ort der LEI erfolgen. Ein Internetzugang für die Versicherten am Ort der Leistungserbringung ist nicht zwingend notwendig.2. Der Versicherte verwendet die eine App mit integriertem PoPP-Modul.3. Die App ist beim PoPP-Service Authorization Server registriert4. Das Endgerät des Versicherten verfügt über ein Lesegerät für kontaktlose oder kontaktbehaftete Kartenkommunikation.
--------------	---

Ablauf	<p>Authentisierung einer eGK:</p> <ol style="list-style-type: none"> 1. Der Versicherte öffnet in der App das PoPP-Modul. Je nach Implementierung könnte sich das PoPP-Modul in der UX bspw. als "online Check-in", "Arztbesuch vorbereiten" oder "Videosprechstunde beitreten" o.ä. darstellen. 2. Der Versicherter wählt eine LEI (bspw. über eine Liste oder durch das Scannen eines QR-Code) aus. Dieser Schritt ist optional. 3. Das PoPP-Modul sendet einen Authorization Request an den PoPP-Service Authorization Server unter folgenden Angabe <ol style="list-style-type: none"> a. der Client-ID des PoPP-Modul, welche im Registrierungsprozess vergeben wurde, b. der Telematik-ID der ausgewählten LEI (optional, wenn durch Nutzer eine Auswahl erfolgt ist) 4. Der PoPP-Service Authorization Server prüft, ob ein PoPP-Modul mit der angegebenen Client-ID am PoPP-Service Authorization Server registriert ist. 5. Der PoPP-Service Authorization Server antwortet mit Abfrage der Einwilligung zum Datenzugriff auf die Versichertendaten durch den PoPP-Service, wenn diese Einwilligung noch nicht vorliegt. <ol style="list-style-type: none"> a. Im PoPP-Modul wird dem Versicherten ein Einwilligungsdialo g angezeigt, der ihn darüber informiert, dass der PoPP-Service die KVNR des Versicherten abfragen möchte. Der Dialog muss so gestaltet sein, dass der Versicherte den Zweck der Datenanfrage erkennt und sich klar für eine Zustimmung oder Ablehnung entscheiden kann. Der Versicherte wählt, ob die Zustimmung nur für den aktuellen Vorgang gilt oder auch für alle zukünftigen Vorgänge. Der Versicherte muss in der Lage sein eine erteilte Zustimmung jederzeit zu widerrufen. Die Zustimmung kann einmalig erfolgen, muss aber durch den Versicherten jederzeit widerrufbar sein. b. Lehnt der Versicherte die Anfrage ab, wird der Prozess abgebrochen. Der Versicherte wird über einen entsprechend gestalteten Dialog im PoPP-Modul darüber informiert. 6. Das Anwendungsfrontend überträgt die Einwilligungsinformationen an den PoPP-Service Authorization Server. 7. Der PoPP-Service Authorization Server stellt ein von ihm signiertes "card-check" Access Token aus und sendet es an das Anwendungsfrontend zurück. Dieses "card-check" Access Token legitimiert den Zugriff auf die Schnittstelle des PoPP-Service Resource Server zum Datentransfer zwischen eGK und PoPP-Service. Das "card-check" Access Token enthält Informationen: <ol style="list-style-type: none"> a. Anzahl der angeforderten TAN (optional), b. Telematik-ID einer LEI (optional). 8. Über das PoPP-Modul wird der Versicherte aufgefordert, seine eGK zum Auslesen an sein Endgerät zu halten oder in eine
--------	---

	<p>Vorrichtung am Endgerät zu stecken.</p> <ol style="list-style-type: none"> 9. Das PoPP-Modul sendet einen cardCommunication Request mit dem "card-check" Access Token an den PoPP-Service Resource Server. 10. Der PoPP-Service Resource Server validiert das "card-check" Access Token. 11. Nach positiver Prüfung liest der PoPP-Service Resource Server die Informationen aus dem "card-check" Access Token Information: <ol style="list-style-type: none"> a. Anzahl der angeforderten TAN (optional), b. Telematik-ID einer LEI (optional). 12. Der PoPP-Service Resource Server beginnt mit der Prüfung der eGK. Dazu sendet er Application Protocol Data Units (APDU) Kommandos an das PoPP-Modul mit dem Zweck die eGK zu authentisieren und KVNR sowie IK-Nummer Zaus der eGK auszulesen. 13. Das PoPP-Modul delegiert die die ADPU Kommandos an die eGK und nimmt die Antworten auf die Kommandos entgegen. 14. Das PoPP-Modul sendet die Antworten der ADPU Kommandos an den PoPP-Service Resource Server. 15. Die Schritte 10-14 werden durchlaufen, bis alle notwendigen Kommandos abgearbeitet sind. 16. Der PoPP-Service Resource Server erstellt einen TANSet-Record mit den ausgelesenen Daten - KVNR und IK-Nummer - und speichert diesen. 17. Auf Basis der ermittelten Informationen aus dem "card-check" Access Token generiert der PoPP-Service: <ol style="list-style-type: none"> a. eine "kurze" TAN, wenn die Telematik-ID der LEI bekannt ist. b. ein TAN-Set mit der angeforderten Anzahl an "langen" TAN, wenn keine Telematik-ID einer LEI zum Zeitpunkt des Check-in bekannt ist. 18. Der PoPP-Service Resource Server speichert die generierte TAN bzw. das TAN-Set und einen Zeitstempel zum TANSet-Record. 19. Der PoPP-Service Resource Server speichert im TANSet-Record die proofMethod gemäß [I_PoPP_Token_Generation.yaml] 20. Der PoPP-Service Resource Server antwortet dem PoPP-Modul auf dessen cardCommunication Request mit der generierten TAN und dem Zeitstempel, zu dem die Gültigkeit der TAN abläuft.
Nachbedingung	Die TAN wird bei Nichtverwendung nach Ablauf des übermittelten Zeitstempels vom Gerät des Versicherten gelöscht.
Akzeptanzkriterien	<ul style="list-style-type: none"> • <u>AF_10386 - TAN ist erstellt und als QR-Code im PoPP-Modul darstellbar</u> • <u>AF_10386 - Vorbereitung zur Attestierung des Versorgungskontextes mit TANSet-Record</u>

	<ul style="list-style-type: none"> • AF_10386 - Löschen einer TAN
Alternativen	Alternativ zur eGK kann der Versicherte den Versorgungskontext mit seiner GesundheitsID attestieren.

Hinweis: Der Gültigkeitszeitraum einer TAN bzw. eines TAN-Sets wird durch den Gültigkeitszeitraum des TANSet-Record (A_27328) festgelegt[<=]*

ML-161890 - AF_10386 - TAN ist erstellt und als QR-Code im PoPP-Modul darstellbar

Nach erfolgreicher Authentisierung der eGK des Versicherten MUSS eine TAN gemäß den Vorgaben in [gemSpec_PoPP_Service] erstellt worden sein. Die TAN MUSS im PoPP-Modul vom Versicherten abgerufen und als QR-Code dargestellt werden können.[<=]

ML-161891 - AF_10386 - Vorbereitung zur Attestierung des Versorgungskontextes mit TANSet-Record

Nach erfolgreicher Authentisierung der eGK des Versicherten MUSS der PoPP-Service für die Attestierung des Versorgungskontextes die KVN-Nummer des Versicherten, die IK-Nummer der Kasse, die proofMethod und einen Zeitstempel in einem TANSet-Record angelegt und abgespeichert haben. Der TANSet-Record MUSS eindeutig der ausgegebenen TAN bzw. des ausgegebenen TAN-Sets zugeordnet sein.
[<=]

4.3.3 PoPP-Token mittels TAN, lokal

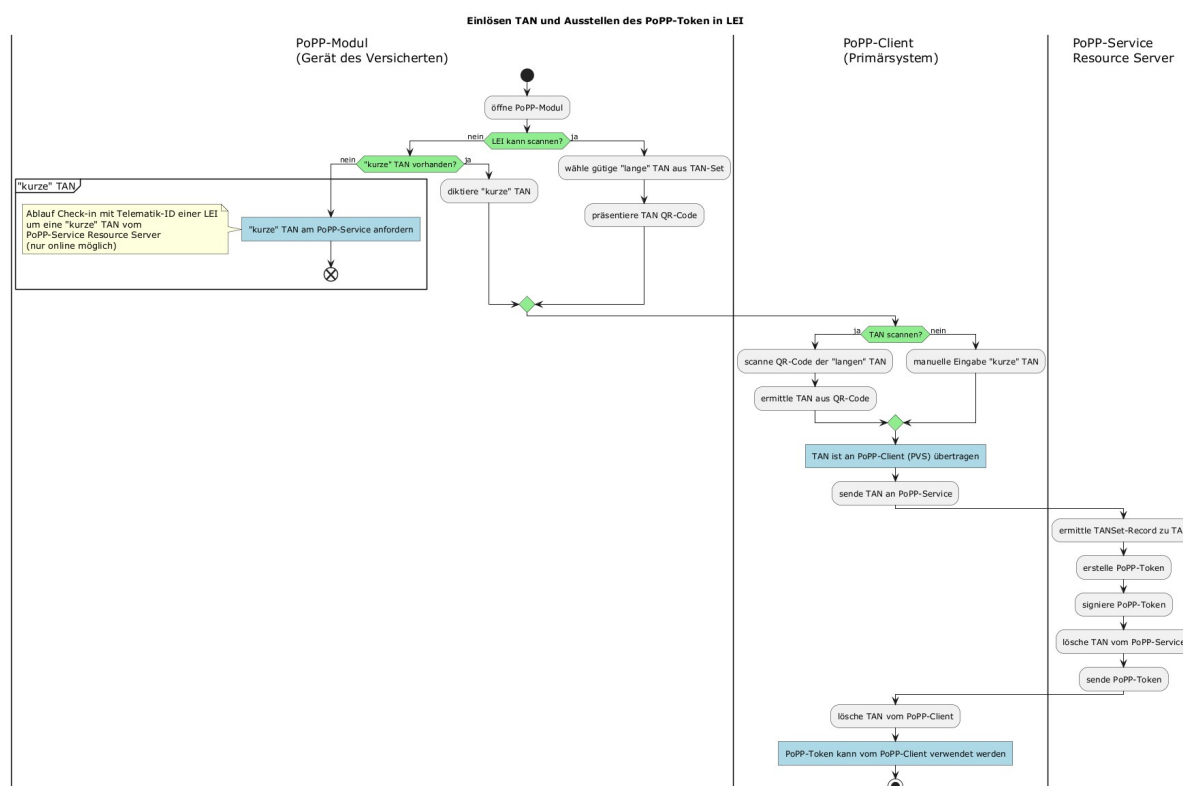


Abbildung 9: Ausstellung PoPP-Token durch LEI über Einlösen einer TAN durch Versicherten am Ort der Leistungserbringung

AF_10392 - PoPP-Token mittels TAN, lokal

Attribute	Bemerkung
Beschreibung	<p>Ein Versicherter präsentiert im PoPP-Modul der App eine TAN (Ergebnis der Authentisierung des Versicherten "mobil") als QR-Code oder als Zeichenkette.</p> <p>Die Authentisierung des Versicherten und die Präsentation der TAN bei einer LEI kann zeitlich und räumlich entkoppelt stattfinden.</p> <p>In der Umgebung der LEI wird der QR-Code von Mitarbeitern des LEI gescannt oder, im Fall einer "kurzen" TAN manuell übermittelt.</p> <p>Die aus dem QR-Code extrahierte oder manuell übermittelte TAN wird über das PS des LEI beim PoPP-Service Resource Server gegen ein PoPP-Token getauscht. Der PoPP-Service Resource Server erstellt aus den Daten der zur TAN gehörenden TANSet-Record und den Daten des LEI ein PoPP-Token und sendet dieses zurück an den in das PS integrierten PoPP-Client.</p> <p>Durch das Übermitteln der TAN in der LEI und den Abruf des PoPP-Token durch die LEI wird die Attestierung des Versorgungskontextes erst wirksam.</p> <p>Nach Auslieferung des PoPP-Token wird die TAN sowohl im PoPP-Client als auch im PoPP-Service gelöscht.</p>
Vorbedingung	<ol style="list-style-type: none"> 1. Der Versicherte hat über das PoPP-Modul in der App eine Authentisierung durchgeführt. Der Versicherte kann in seinem PoPP-Modul eine gültige TAN als QR-Code oder, im Falle einer "kurzen" TAN, als numerischen Wert präsentieren. 2. Im PoPP-Service Resource Server ist ein Datensatz (TANSet-Record) mit den Attestierungsinformationen des Versicherten und einer Zuordnung zur TAN angelegt. <p>Vorbedingungen Leistungserbringer:</p> <ol style="list-style-type: none"> 1. Das PS der LEI ist über Einboxkonnektor und SMC-B oder TI-Gateway mit Highspeed-Konnektor und SMC-B als Karte oder als SM-B im HSM des HSK an die TI angeschlossen. 2. Das PS ist in der Rolle des PoPP-Clients am PoPP-Service registriert und angemeldet.
Ablauf	<p>Präsentation des QR-Code und Abschluss der Attestierung (kann zeitlich und räumlich entkoppelt ablaufen):</p> <ol style="list-style-type: none"> 1. Der Versicherte befindet sich in der LEI (bspw. in die Praxis eines Arztes). 2. Der Versicherte präsentiert eine gültige TAN. <ol style="list-style-type: none"> a. Verfügt die LEI nicht über die Möglichkeit zum Scannen, wählt er die zuvor für die LEI generierte "kurze" TAN. Ist diese nicht vorhanden, so muss der Versicherte über das PoPP-Modul der App eine "kurze" TAN beim PoPP-Service generieren lassen (siehe AF_10386*, AF_10389*). b. Verfügt die LEI über die Möglichkeit zum Scannen öffnet der Versicherte den QR-Code einer TAN zum Check-in im PoPP-Modul in der App. 3. Der Versicherte präsentiert den QR-Code am Empfang der LEI oder diktiert die "kurze" TAN.

	<ol style="list-style-type: none"> 4. Mitarbeiter der LEI scannen den QR-Code oder erfassen die "kurze" TAN über eine manuelle Eingabe. 5. Der PoPP-Client im PS der LEI übernimmt die TAN aus dem QR-Code oder über die Eingabe. 6. Der PoPP-Client im PS der LEI sendet die TAN an den PoPP-Service Resource Server. 7. Der PoPP-Service Resource Server liest den TANSet-Record zur TAN aus der Datenbank. 8. Der PoPP-Service Resource Server erstellt ein PoPP-Token, welches die Versichertendaten aus dem TANSet-Record und die LEI-Daten aus der SMC-B (registrierter PoPP-Client) enthält. 9. Der PoPP-Service Resource Server signiert das PoPP-Token. 10. Der PoPP-Service Resource Server liefert das signierte PoPP-Token an den PoPP-Client im PS der LEI. 11. Das PS der LEI verwendet das PoPP-Token zur Abfrage weiterer TI-Dienste wie Versichertenstammdatenmanagement (VSDM).
Nachbedingung	<ol style="list-style-type: none"> 1. Die TAN ist nach Verwendung im PoPP-Service gelöscht. 2. Die TAN und TANSet-Record sind bei Nichtverwendung nach Ablauf der Gültigkeit im PoPP-Service gelöscht. 3. Die TAN ist nach Verwendung im PS gelöscht. 4. Die TAN ist nach Verwendung vom Gerät des Versicherten gelöscht
Akzeptanzkriterien	<ul style="list-style-type: none"> • <u>AF_10386 - Löschen einer TAN</u> • <u>AF_10386 - PoPP-Client - Einlösen einer TAN gegen ein PoPP-Token</u> • <u>AF_10386 - PoPP-Client - Einlösen oder Verfall einer TAN</u>

[<=]

4.3.4 PoPP-Token mittels TAN, mobil

Der Anwendungsfall zum Einlösen einer TAN und Ausstellen eines PoPP-Token für eine Videosprechstunde ist exemplarisch für den Fall, dass der LE, bzw. die LEI nicht physisch mit dem Versicherten in Kontakt ist, sondern die Kommunikation virtuell erfolgt. Hier wird der Ablauf beschrieben, wenn eine App (z.B. Videosprechstunde) ein PoPP-Modul für den Check-in für die Versicherten anbietet und die TAN über angebotene Kommunikationskanäle an einen PoPP-Client überträgt.

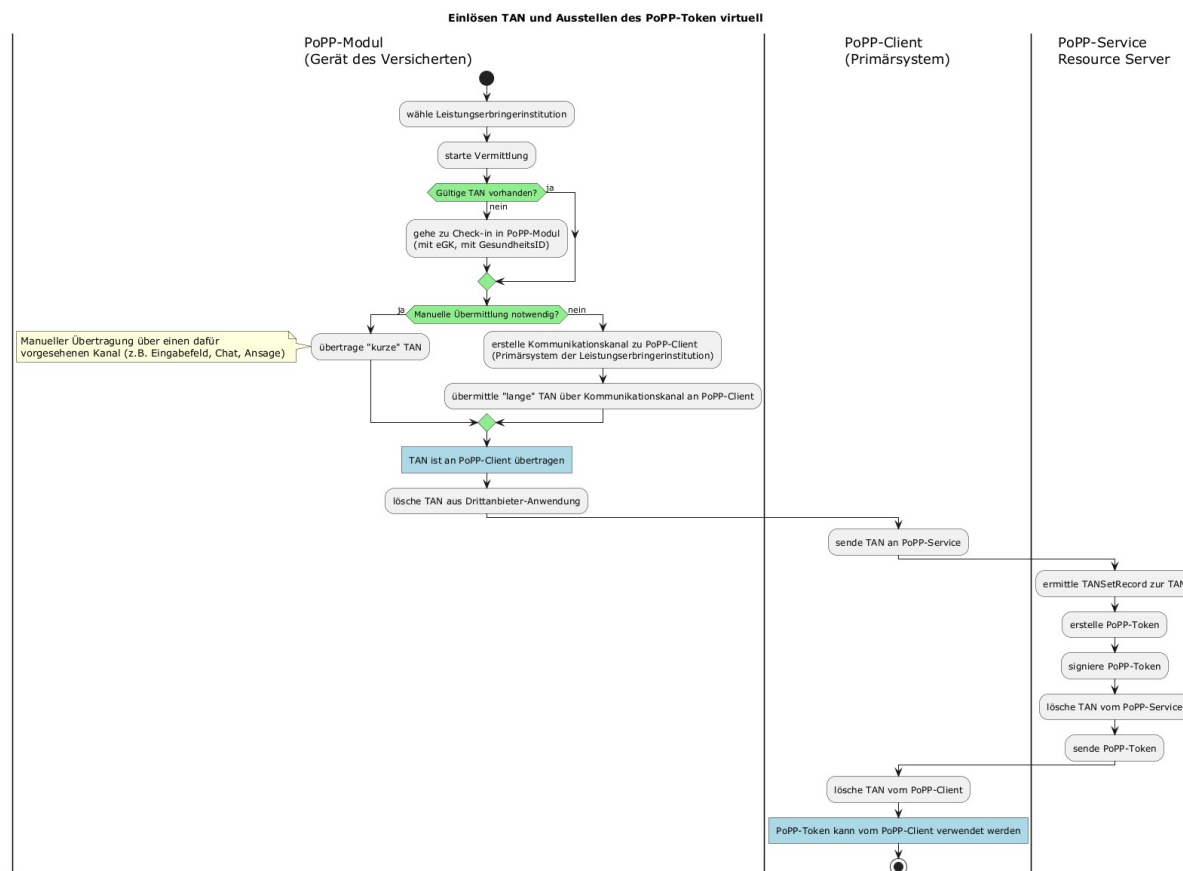


Abbildung 10: Ausstellung PoPP-Token durch LEI über Einlösen einer TAN durch Versicherten mobil (Videosprechstunde, Apotheken)

AF_10390 - PoPP-Token mittels TAN, mobil

Attribute	Bemerkung
Beschreibung	<p>Ein Versicherter öffnet die App mit integriertem PoPP-Modul (bspw. Videosprechstunden-Anbieter). Wurde vorher als Ergebnis einer Authentifizierung des Versicherten mit GesundheitsID oder eGK eine TAN erstellt, so wird dieses dem Versicherten im PoPP-Modul der Anwendung dargestellt. Ist aktuell keine gültige TAN im PoPP-Modul hinterlegt, wird der Versicherte aufgefordert ein Check-in in seinem PoPP-Modul durchzuführen.</p> <p>Der Versicherte startet die Übertragung der TAN (bspw. nach Aufforderung durch die LEI) im PoPP-Modul der Anwendung. Die gültige TAN wird von der App an den PoPP-Client des PS der LEI übermittelt.</p> <p>Je nach Art und Möglichkeit der App kann die TAN über einen digitalen Kanal ("lange" TAN) oder manuell ("kurze" TAN) übertragen werden.</p> <p>Die TAN wird über den PoPP-Client im PS der LEI beim PoPP-Service Resource Server gegen ein PoPP-Token getauscht. Der PoPP-Service Resource Server erstellt aus den Daten des zur TAN gehörenden TANSet-Record und den Daten der LEI ein PoPP-Token und sendet dieses zurück an den in das PS integrierten PoPP-Client.</p> <p>Durch Einlösen der TAN und den Abruf des PoPP-Token durch das PS</p>

	<p>der LEI wird die Attestierung des Versorgungskontextes erst wirksam. Nach Auslieferung des PoPP-Token wird die TAN sowohl im PoPP-Client als auch im PoPP-Service Resource Server gelöscht.</p>
Vorbedingung	<ol style="list-style-type: none"> 1. Die App hat eine gültige TAN nach erfolgreicher Authentisierung des Nutzers mit der GesundheitsID. 2. Im PoPP-Service Resource Server ist ein TANSet-Record mit den Informationen zum Versicherten und einer Zuordnung zur TAN angelegt. <p>Vorbedingungen Leistungserbringer:</p> <ol style="list-style-type: none"> 1. DieApp hat einen sicheren Übertragungskanal zum PoPP-Client im PS der LEI. Die TAN kann über diesen Weg an das PS übertragen werden. 2. Alternativ bietet die App die Möglichkeit der Übertragung einer "kurzen" TAN (bspw. durch manuelle Eingabe). 3. Das PS der LEI ist über Einboxkonnektor und SMC-B oder TI-Gateway mit Highspeed-Konnektor und SMC-B als Karte oder als SM-B im HSM des HSK an die TI angeschlossen. 4. Das PS ist in der Rolle des PoPP-Clients am PoPP-Service registriert und angemeldet.
Ablauf	<ol style="list-style-type: none"> 1. Der Versicherte öffnet die App (bspw. Videosprechstunden-App). 2. Der Versicherte wählt in der App den Partner (LE) (bspw. für die Videosprechstunde) aus. 3. Der Versicherte bestätigt die Verbindungsaufnahme zum LE. 4. Die App öffnet einen sicheren Übertragungskanal zum PoPP-Client im PS der LEI oder bietet die Eingabe einer "kurzen" TAN an. 5. Die App überträgt die "lange" TAN oder die eingegebene "kurze" TAN über den sicheren Kanal an den PoPP-Client im PS in der LEI. 6. Der PoPP-Client im PS der LEI sendet die TAN an den PoPP-Service Resource Server. 7. Der PoPP-Service Resource Server liest den TANSet-Record zur TAN aus der Datenbank. 8. Der PoPP-Service Resource Server erstellt ein PoPP-Token, welches die Versichertendaten aus dem TANSet-Record und den Daten des registrierter PoPP-Client (Telematik-ID der LEI) enthält. 9. Der PoPP-Service Resource Server signiert das PoPP-Token. 10. Der PoPP-Service Resource Server liefert das signierte PoPP-Token an den PoPP-Client im PS der LEI. 11. Das PS der LEI verwendet das PoPP-Token zur Abfrage weiterer TI-Dienste.
Nachbedingung	<ol style="list-style-type: none"> 1. Die TAN ist nach Verwendung im PoPP-Service gelöscht.

	<ol style="list-style-type: none"> 2. Die TAN und TANSet-Record sind bei Nichtverwendung nach Ablauf der Gültigkeit im PoPP-Service gelöscht. 3. Die TAN ist nach Verwendung im PS gelöscht. 4. Die TAN ist nach Verwendung vom Gerät des Versicherten gelöscht. 5. Die TAN ist nach Verwendung aus der App gelöscht.
Akzeptanzkriterien	<ul style="list-style-type: none"> • <u>AF_10386 - Löschen einer TAN</u> • <u>AF_10386 - PoPP-Client - Einlösen einer TAN gegen ein PoPP-Token</u> • <u>AF_10386 - PoPP-Client - Einlösen oder Verfall einer TAN</u>

[<=]

ML-161895 - AF_10386 - PoPP-Client - Einlösen einer TAN gegen ein PoPP-Token

Löst ein registrierter und angemeldeter PoPP-Client eine TAN beim PoPP-Service Resource Server ein, so MUSS dieser ein PoPP-Token mit den Daten des Versicherten aus dem TANSet-Record erstellen, welcher der TAN zugeordnet ist. Das PoPP-Token MUSS mit den Daten des PoPP-Clients ergänzt und signiert an den PoPP-Client zurückgegeben werden.

[<=]

ML-161897 - AF_10386 - PoPP-Client - Einlösen oder Verfall einer TAN

Der PoPP-Service DARF eine TAN NICHT öfter als einmal einlösen. Der PoPP-Service DARF eine TAN NICHT mehr einlösen, wenn deren Gültigkeitszeitraum überschritten ist.[<=]

ML-161896 - AF_10386 - Löschen einer TAN

Eine Komponente, die eine TAN oder einen TANSet-Record speichert, MUSS diese Information unwiderruflich löschen, sobald die Information als ungültig verfällt oder die TAN eingelöst wurde.

[<=]

4.4 Check-in in einer LEI mit eGK und Ausgabe des PoPP-Token

Bevor der PoPP-Service für eine LEI ein PoPP-Token erstellt, ist es erforderlich, dass sich die LEI mit Hilfe der SM-B beim PoPP-Service authentisiert. Des Weiteren ist es erforderlich die Anwesenheit einer eGK nachzuweisen. Der dazu verwendete PoPP-Client ist Bestandteil des PS.

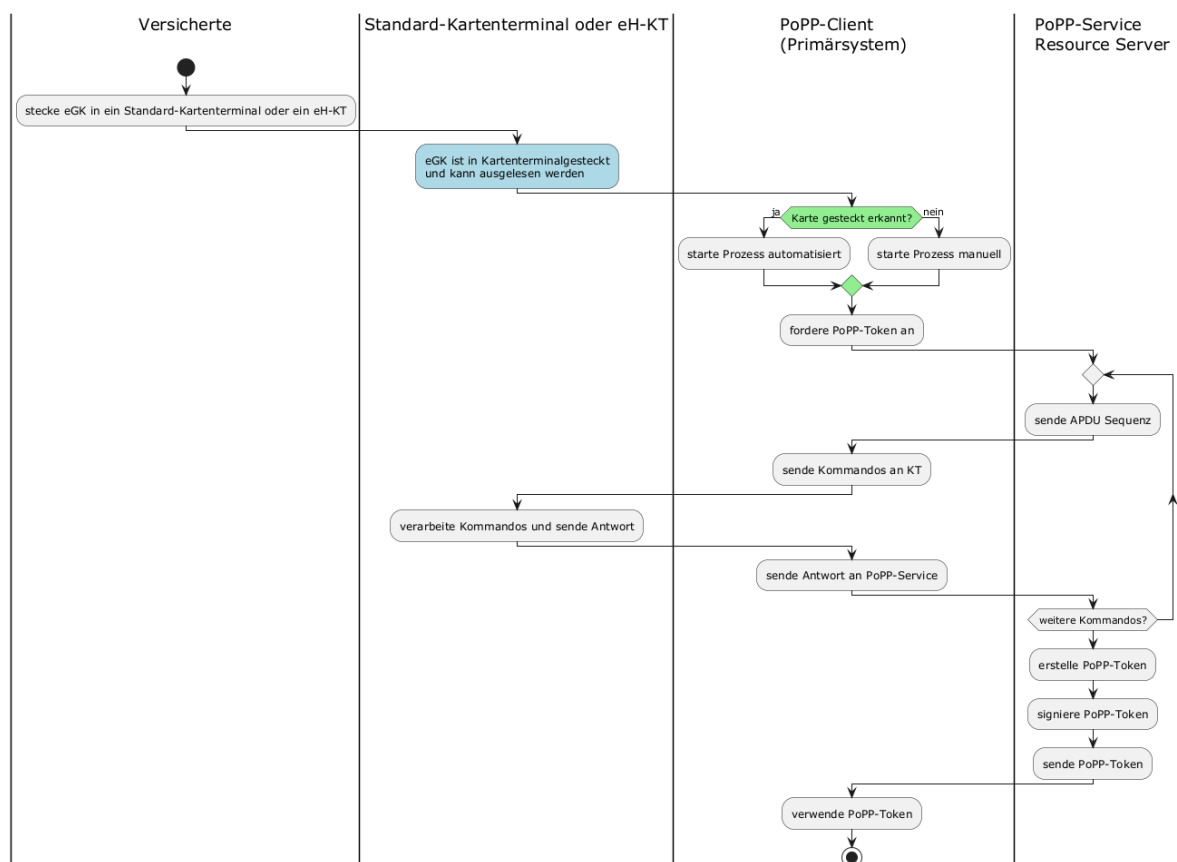


Abbildung 11: Ausstellung PoPP-Token nach Stecken der eGK in LEI

AF_10387 - PoPP-Token mittels eGK im Standard-Kartenterminal

Attribute	Bemerkung
Beschreibung	<p>Erkennt der PoPP-Client als Bestandteil des PS das "Einstecken" (kontaktbehaftet oder kontaktlos) einer eGK in einen Kartenleser, so ist es möglich, dass der Prozess zum Ausstellen eines PoPP-Token automatisch startet. Alternativ wird der Prozess manuell im PS gestartet.</p> <p>Die Kommunikation des PoPP-Service mit der "gesteckten" Karte wird durch den PoPP-Client vermittelt. Nach erfolgreichem Abschluss der Kommunikation stellt der PoPP-Service ein PoPP-Token aus und sendet dieses an den PoPP-Client.</p>
Vorbedingung	<ol style="list-style-type: none"> 1. Das PS der LEI ist über einen Einboxkonnektor mit eH-KT und SMC-B oder über ein TI-Gateway mit Highspeed-Konnektor und SMC-B als Karte im eH-KT oder als SM-B im HSM des HSK an die TI angeschlossen. 2. Der PoPP-Client ist am PoPP-Service registriert und angemeldet (siehe Anwendungsfall "Leistungserbringerinstitution (LEI) am PoPP-Service registrieren und anmelden"). 3. Zur Authentifizierung am PoPP-Service hat der PoPP-Client ein

	<p>gültiges PoPP-Client Access Token.</p> <p>4. Der PoPP-Client hat die Möglichkeit auf eine Anbindung der eGK über einen Standard-Kartenleser oder ein eH-KT zu reagieren ("Stecken der eGK", egal, ob kontaktbehaftete oder kontaktlose Kommunikation).</p>
Ablauf	<ol style="list-style-type: none"> 1. Der Versicherte "steckt" seine eGK in einen Standard-Kartenleser oder in ein eH-KT. 2. Der PoPP-Client reagiert auf das "Stecken" der eGK (bspw. über PC/SC oder WinCard API oder Ereignisnachrichten des Konnektors) entweder automatisch oder manuell im PS getriggert. 3. Der PoPP-Client öffnet eine Verbindung zum PoPP-Service. Die Verbindung wird über das PoPP-Client Access Token authentifiziert. 4. Der PoPP-Service sendet eine Reihe von Kommando APDUs an den PoPP-Client. 5. Der PoPP-Client leitet die Kommando APDUs an die eGK weiter. 6. Die eGK verarbeitet die Kommando APDUs und sendet die korrespondierenden Antwort APDUs an den PoPP-Client. 7. Der PoPP-Client sendet die Antwort APDUs der eGK an den PoPP-Service. 8. Schritte 4-7 werden wiederholt, bis der PoPP-Service alle notwendigen Kommandos abgearbeitet hat: <ol style="list-style-type: none"> a. Der PoPP-Service überprüft die Echtheit der eGK mittels CV-Zertifikaten. b. Der PoPP-Service liest das X.509 Zertifikat CH.AUT der eGK aus. c. Prüfung des X.509 Zertifikats hinsichtlich Vertrauensraum der TSL, dass es sich um ein eGK-Zertifikat mit entsprechenden Werten handelt, zeitlicher Gültigkeit und Sperrstatus Online Certificate Status Protocol (OCSP) durch den PoPP-Service. 9. Der PoPP-Service erstellt und signiert das PoPP-Token. <ol style="list-style-type: none"> a. Die Informationen über den Versicherten werden aus dem X.509 Zertifikat der eGK entnommen. b. Die Informationen über die LEI werden aus der PoPP-Client Authentifizierungs-Session (PoPP-Client Access Token) entnommen. 10. Der PoPP-Service übermittelt das PoPP-Token an den PoPP-Client.
Nachbedingung	<p>Das PoPP-Token liegt im PS vor, ein Anwendungsmodul innerhalb des PS kann das PoPP-Token als Autorisierung bei einem FD verwenden, bspw. zum Abruf der Versichertenstammdaten.</p>

Akzeptanzkriterien	<ul style="list-style-type: none"> • Prüfung der eGK vor Ausstellung eines PoPP-Tokens • Verwendung der Versichertendaten der eGK
Alternativen	Alternativ zur eGK kann der Versicherte den Versorgungskontext mit seiner GesundheitsID attestieren.

[<=]

AF_10393 - PoPP-Token mittels eGK im eH-KT

Attribute	Bemerkung
Beschreibung	Erkennt der PoPP-Client als Bestandteil des PS das "Einstecken" (kontaktbehaftet oder kontaktlos) einer eGK in einen Kartenleser, so ist es möglich, dass der Prozess zum Ausstellen eines PoPP-Token automatisch startet. Alternativ wird der Prozess manuell im PS gestartet. Die Kommunikation des PoPP-Service mit der "gesteckten" Karte wird durch den PoPP-Client vermittelt. Nach erfolgreichem Abschluss der Kommunikation stellt der PoPP-Service einen PoPP-Token aus und sendet dieses an den PoPP-Client.
Vorbedingung	<ol style="list-style-type: none"> 1. Das PS der LEI ist über einen Einboxkonnektor mit eH-KT und SMC-B oder TI-Gateway mit einen Highspeed-Konnektor und SMC-B als Karte im eH-KT oder als SM-B im HSM des HSK an die TI angeschlossen. 2. Der PoPP-Client ist am PoPP-Service registriert und angemeldet (siehe Anwendungsfall "Leistungserbringerinstitution (LEI) am PoPP-Service registrieren und anmelden"). 3. Zur Authentifizierung am PoPP-Service hat der PoPP-Client ein gültiges PoPP-Client Access Token. 4. Der PoPP-Client hat die Möglichkeit auf eine Anbindung der eGK über ein eH-KT an einem Konnektor ("Stecken der eGK" gleich kontaktbehaftete oder kontaktlose Kommunikation) zu reagieren.
Ablauf	<ol style="list-style-type: none"> 1. Der Versicherte "steckt" seine eGK in ein eH-KT. 2. Der PoPP-Client reagiert auf das "Stecken" der eGK (bspw. über die Auswertung von Konnektornachrichten) entweder automatisch oder manuell im PS getriggert. 3. Der PoPP-Client öffnet eine Verbindung zum PoPP-Service. Die Verbindung wird über das PoPP-Client Access Token authentifiziert. 4. Der PoPP-Service sendet eine Reihe von Kommando APDUs an den PoPP-Client. 5. Der PoPP-Client leitet die Kommando APDUs über den Konnektor an die eGK weiter. 6. Die eGK verarbeitet die Kommando APDUs und sendet die korrespondierenden Antwort APDUs über den Konnektor an den PoPP-Client. 7. Der PoPP-Client sendet die Antwort APDUs der eGK an den

	<p>PoPP-Service.</p> <ol style="list-style-type: none"> 8. Schritte 4-7 werden wiederholt, bis der PoPP-Service alle notwendigen Kommandos abgearbeitet hat: <ol style="list-style-type: none"> a. Der PoPP-Service überprüft die Echtheit der eGK mittels CV-Zertifikaten. b. Der PoPP-Service liest das X.509 Zertifikat CH.AUT der eGK aus. c. Prüfung des X.509 Zertifikats hinsichtlich Vertrauensraum der TSL, dass es sich um ein eGK-Zertifikat mit entsprechenden Werten handelt, zeitlicher Gültigkeit und Sperrstatus Online Certificate Status Protocol (OCSP) durch den PoPP-Service. 9. Der PoPP-Service erstellt und signiert das PoPP-Token. <ol style="list-style-type: none"> a. Die Informationen über den Versicherten werden aus dem X.509 Zertifikat der eGK entnommen. b. Die Informationen über die LEI werden aus der PoPP-Client Authentifizierungs-Session (PoPP-Client Access Token) entnommen. 10. Der PoPP-Service übermittelt das PoPP-Token an den PoPP-Client.
Nachbedingung	Das PoPP-Token liegt im PS vor, ein Anwendungsmodul innerhalb des PS kann das PoPP-Token als Autorisierung bei einem FD verwenden, bspw. zum Abruf der Versichertenstammdaten.
Akzeptanzkriterien	<ul style="list-style-type: none"> • <u>Prüfung der eGK vor Ausstellung eines PoPP-Tokens</u> • <u>Verwendung der Versichertendaten der eGK</u>
Alternativen	Alternativ zur eGK kann der Versicherte den Versorgungskontext mit seiner GesundheitsID attestieren.

[<=]

ML-163355 - Prüfung der eGK vor Ausstellung eines PoPP-Token

Der PoPP-Service MUSS den Status der eGK prüfen. Ist die eGK nicht gültig, MUSS der PoPP-Service die Ausstellung eines PoPP-Token verweigern.**[<=]**

ML-163356 - Verwendung der Versichertendaten der eGK

Der PoPP-Service MUSS bei gültiger eGK und validiertem PoPP-Client ein PoPP-Token ausstellen, signieren und an den anfragenden PoPP-Client senden. Dabei MUSS der PoPP-Service sicherstellen, dass ausschließlich die Daten aus der eGK und die SMC-B Daten des anfragenden PoPP-Clients bei der Ausstellung des PoPP-Token verwendet werden.

[<=]

5 Übergreifende Festlegungen

5.1 PoPP-Token: Nachweis des Versorgungskontextes

Die Funktionalität "PoPP-Token: Nachweis des Versorgungskontextes" stellt auf Anforderung von PoPP-Clients ein PoPP-Token sowie einen Datensatz "Prüfungsnachweis" gemäß der VSDM-Spezifikation bereit ("VSDM+") . Das PoPP-Token ist ein kryptografisch gesicherter Nachweis eines Versorgungskontextes über zwei Identitäten des Gesundheitswesens (Versicherte und LEI). Der VSDM-Prüfungsnachweis (VSDM-PN) ist ein kryptografischer Nachweis ausschließlich über eine Versichertenidentität und wird lediglich für eine Übergangszeit zusätzlich ausgestellt, um Fachdiensten der TI die Migration vom VSDM-Prüfungsnachweis hin zum PoPP-Token zu erleichtern.

Damit ist die zentrale Businesslogik des PoPP-Service beschrieben. Die weiteren Funktionsmerkmale, die für die Erstellung eines PoPP-Token in den unterschiedlichen Konstellationen benötigt werden, sind logisch in den Kapiteln für den PoPP-Resource Server gefasst.

5.1.1 PoPP-Token-Erstellung

In diesem Kapitel sind die Anforderungen an den PoPP-Service zusammengefasst, die für das Erstellen eines PoPP-Token notwendig sind. Für die Bedingungen, unter denen der PoPP-Service einen PoPP-Token ausstellt, siehe [\[Kapitel Übersicht der Systemanwendungsfälle für die Ausstellung des PoPP-Tokens\]](#).

A_26432 - PoPP-Service - PoPP-Token JWT

Der PoPP-Service MUSS PoPP-Token immer gemäß [RFC7519] als JWT ausstellen und im Compact Serialization Format kodieren. [**<=**]

A_26431 - PoPP-Service - PoPP-Token Claims

Der PoPP-Service MUSS im PoPP-Token die Claims gemäß [I_PoPP-Token_Generation.yaml], Schema "Token Claims" verwenden. [**<=**]

Tabelle 4: PoPP-Token Claims (informativ)

Name	Wert
version	Version des PoPP-Token-Formats (Fester Wert "1.0.0")
iss	Aussteller des Token. Der Wert muss die URL des PoPP-Service ohne Pfad und ohne trailing Slash sein.
iat	Zeitpunkt der PoPP-Token-Erstellung
proofMethod	Methode, die verwendet wurde um die Identität des Versicherten nachzuweisen. Die zulässigen Werte sind in [I_PoPP-Token_Generation.yaml] spezifiziert. Unterstützt werden diverse eGK und GesundheitsID basierte Nachweismethoden.

patientProofTime	Der Zeitpunkt, zu dem der Nachweis des Patienten durchgeführt wurde. <ul style="list-style-type: none">Bei Nachweismethoden mit eGK ist dies der Zeitpunkt, zu dem die eGK verwendet wurde.Bei Nachweismethoden mit GesundheitsID ist dies der Zeitpunkt, zu dem die Identität mithilfe von OpenID Connect verifiziert wurde.
patientId	KVNR - Versichertennummer des Patienten
insurerId	Institutionskennzeichen der Krankenversicherung (IK-Nummer)
actorId	Telematik-ID der am PoPP-Service authentifizierten Leistungserbringerinstitution (bspw. über SMC-B), die den Behandlungskontext über die oben angegebene Methode nachgewiesen hat.
actorProfessionOid	OID des agierenden Leistungserbringerinstitution passend zu actorId (Telematik-ID) gemäß [gemSpec_OID].
authorization_details	Das Claim authorization_details gemäß [RFC9396] ist optional. Es dient dazu, Autorisierungsanforderungen detailliert und strukturiert zu definieren. Es ermöglicht die Spezifikation komplexer Berechtigungen, wie etwa spezifische Operationen oder Bedingungen. Das Claim ist so gestaltet, dass es sich flexibel erweitern lässt und daher für zukünftige Anforderungen und Entwicklungen in der Autorisierungsverwaltung geeignet ist. Anmerkung: Claim-Bezeichnung ist in Snake-Case und entspricht den Vorgaben aus dem [RFC9396] bzw. von IANA.

A_26961 - PoPP-Service - PoPP-Token Claims über Leistungserbringer (LE)

Der PoPP-Service MUSS als "actorId" und "actorProfessionOid" die Werte der Institution setzen, die sich gegenüber dem PoPP-Service authentifiziert hat und den Nachweis über den Versorgungskontext mit dem Versicherten erbracht hat. [≤]

A_26962 - PoPP-Service - PoPP-Token Claims über Versicherte

Der PoPP-Service MUSS Claims über den Versicherten ausschließlich nach der vorherigen Authentifizierung (GesundheitsID oder eGK) in das PoPP-Token aufnehmen und dabei genau die aus der Authentifizierung erhaltenen Daten verwenden. [≤]

A_26433 - PoPP-Service - PoPP-Token Header und Signatur

Der PoPP-Service MUSS die JWT PoPP-Token mit dem Algorithmus ES256 mit dem im HSM gehaltenen PoPP-Token-Signaturschlüssel signieren und dabei Header-Attribute gemäß [I_PoPP-Token_Generation.yaml], Schema "TokenHeaders", setzen und mitsignieren (protected headers). [≤]

Tabelle 5: PoPP-Token Header (informativ)

Name	Wert
------	------

typ	Typ des Token. Fester Wert "vnd.telematik.popp+jwt"
alg	Algorithmus mit welchem das PoPP-Token signiert wurde. Fester Wert 'ES256'.
kid	Key-ID des Schlüssels, der zur Signierung des Token verwendet wurde. Daten zum zugehörigen Signaturprüf Schlüssel lassen sich vom JWK-Endpunkt des PoPP-Service abrufen.

Informatives Beispiel für einen PoPP-Token:

```
{
  "typ": "vnd.telematik.popp+jwt",
  "alg": "ES256",
  "kid": "x_vW4LVDipvu8iUQ5aLksZLWtH6jh4eJ4c5offXtMV0"
}
.
{
  "iat": 1722593256,
  "iss": "https://popp.example.com",
  "proofMethod": "ehc-practitioner-trustedchannel-read-x509",
  "patientProofTime": 1722593255,
  "patientId": "X123456789",
  "insurerId": "123456789",
  "actorId": "1-2012345678",
  "actorProfession0id": "1.2.276.0.76.4.50"
}
```

(Signatur vernachlässigt)

A_26434 - PoPP-Service - Bereitstellung der öffentlichen Schlüssel zur Verifikation der PoPP-Token als JWKS

Der Anbieter eines PoPP-Service MUSS die öffentlichen Schlüssel zur Verifikation der PoPP-Token als JWK-Set nach [RFC7517] bereitstellen und dabei zu jedem öffentlichen Schlüssel die folgenden Attribute angeben:

Name	Wert
kid	In dem JWK-Set eindeutige Kennung des Schlüssels. Es wird empfohlen Thumbprint des öffentlichen Schlüssels gemäß [RFC7638] als 'kid' zu verwenden.
use	Verwendungszweck des Schlüssels. Fester Wert 'sig'.
ktu	Schlüsseltyp. Derzeit werden nur elliptische Kurven unterstützt. Fester Wert 'EC'
crv	Bezeichnung der elliptischen Kurve. Erlaubte Werte: <ul style="list-style-type: none"> P-256 für die NIST Curve

x	X-Koordinate des öffentlichen Schlüssels
y	Y-Koordinate des öffentlichen Schlüssels
alg	Gibt den kryptografischen Algorithmus an, der mit dem Schlüssel verwendet werden soll. Erlaubte Werte: <ul style="list-style-type: none"> ES256 für den P-256 Schlüssel (ECDSA-Signatur mit SHA-256).
x5c	Die X.509-Zertifikatskette, die diesen Schlüssel zertifiziert. Enthält als einziges Element das EE-TI-Zertifikat des PoPP-Service (C.ZD.SIG). Der Zertifikat ist als DER und anschließend als Base64 kodiert, siehe [RFC7517#Abschnitt 4.7].

[<=]

Informatives Beispiel für einen PoPP JWK-Set

```
{
  keys: [
    {
      "kid": "DCHF2-6iG5gC5cPxrMktfZgolieCU_RBZfvwREKpdWc",
      "use": "sig",
      "kty": "EC",
      "crv": "P-256",
      "x": "C3Q12wBw1K49LCeJBjDNhT_0TmWe6zZ_8pUNLF7IEfE",
      "y": "5CNecFcZE0zRPhsuXeDXxJyFjG0vfIgcXqKkst6csto",
      "alg": "ES256",
      "x5c": [
        "MIICBzCCAA6gAwI..."
      ]
    }
  ]
}
```

Hinweis: Siehe auch Tabelle "Entity Statement des PoPP-Service als Protected Resource" im Anhang.

A_26533 - PoPP-Service - Veröffentlichung der öffentlichen PoPP-Token-Verifikations-Schlüssel als signiertes JWKS

Der Anbieter eines PoPP-Service MUSS das JWK-Set zur Verifikation der PoPP-Token als JWT gemäß [RFC7519] bereitstellen. Das JWT MUSS mit dem Entity Statement-Signing Key signiert sein, die Signatur muss spätestens nach 24 Stunden erneuert werden. Die URL zum Herunterladen des JWT mit signierten JWK-Set muss im Entity Statement unter metadata.oauth_resource.signed_jwks_uri angegeben werden. Als Content-Type HTTP-Header muss application/jwk-set+jwt verwendet werden.

[<=]

Hinweis: siehe auch [jwk-set+jwt].

5.1.2 PoPP-Token Prüfung

Das Kapitel enthält die Anforderungen an die Systeme, die PoPP-Token verifizieren und verarbeiten. Dabei sind zwei Wege der Verifikation möglich: via Entity Statement, welches auf den Vertrauensanker des Federation Masters rückführbar ist und via TI-PKI mit der TSL als Vertrauensanker. Dienste die einen PoPP-Token verifizieren, werden im Folgenden als "PoPP-Verifier" bezeichnet.

A_27015 - PoPP-Verifier - Prüfung Signaturzertifikat via TI-PKI möglich

Der PoPP-Verifier KANN die Signatur des PoPP-Token auch gegen die TI-PKI verifizieren.
[<=]

A_27016 - PoPP-Verifier - Prüfung Signaturzertifikat via TI-PKI - Vorgaben

Der PoPP-Verifier, der das Signaturzertifikat des PoPP-Token via TI-PKI prüft, MUSS dabei verifizieren, dass das für die Signatur des PoPP-Token verwendete Signaturzertifikat:

- im jwks des PoPP-Service mit der entsprechenden, im Header des PoPP-Token angegeben kid enthalten ist,
- aus der TI-PKI stammt,
- das Zertifikatsprofil oid_zd_sig (OID 1.2.276.0.76.4.287, "C.ZD.SIG") aufweist,
- die technische Rolle oid_popp-token (OID 1.2.276.0.76.4.320) aufweist und
- per OCSP von der TI-Komponenten-PKI als "good" beauskunftet wird.

[<=]

Hinweis: Der OCSP-Responder ist im Internet erreichbar. Die Adresse des OCSP-Responders ist dem Authority Information Access (AIA) des Zertifikats zu entnehmen.

A_26449 - PoPP-Verifier - Verwendung von PoPP-Service JWK-Sets

Der Anbieter eines PoPP-Verifiers MUSS in regelmäßigen Abständen die JWK-Set des PoPP-Service [RFC7517] über dem im Entity Statement metadata.oauth_resource.signed_jwks_uri angegeben URL abrufen und die öffentlichen Schlüssel zur Verifikation der PoPP-Token verwenden. Spätestens nach 24 Stunden MUSS das Entity Statement des PoPP-Service und das JWK-Set erneut abgerufen werden.

[<=]

A_27358 - PoPP-Verifier - Zugang zum Entity Statement des PoPP-Service

Der PoPP-Verifier KANN die URL zum Laden des Entity Statement des PoPP-Service ermitteln, indem er beim Federation Master die Liste der in der TI-Föderation registrierten Teilnehmer abrufen und daraus die Teilnehmer-URL des PoPP-Service extrahiert. Das Entity Statement ist dann unter <Teilnehmer-URL PoPP-Service>/ .well-known/openid-federation gemäß A_27296* abrufbar.[<=]

Hinweis: Die Liste der registrierten TI-Teilnehmer kann unter [<https://app.federationmaster.de/federation/list>] abgerufen werden.

A_26534 - PoPP-Verifier - PoPP-Service JWK-Set Signatur Prüfung

Der PoPP-Verifier MUSS bei jedem Bezug des JWK-Sets dessen Signatur mit Hilfe des Entity Signing-Keys aus dem Entity Statement prüfen.[<=]

A_26450 - PoPP-Verifier - PoPP-Token Signaturprüfung

Der PoPP-Verifier MUSS sicherstellen, dass die JWT-Signatur des PoPP-Token gemäß [RFC7515] verifiziert wird. Folgende Header-Attribute müssen im signierten JWT enthalten sein:

- typ - fester Wert "vnd.telematik.popp+jwt",
- alg - fester Wert "ES256",
- kid - Key-ID des verwendeten Schlüssels.

Der öffentliche Schlüssel zur Verifikation der Signatur muss aus dem JWK-Set des PoPP-Service über das kid Header-Attribut des PoPP-Token ermittelt werden.[<=]

A_26452 - PoPP-Verifier - JWT Claims Validierung

Der PoPP-Verifier MUSS sicherstellen, dass die folgenden Claims im PoPP-Token vorhanden sind und deren Inhalt prüfen:

- iss - muss die URL des PoPP-Service aus dem Entity Statement sub-Attribut enthalten
- iat - Ausstellungszeitpunkt des PoPP-Token muss anwendungsspezifisch geprüft werden (bspw. nicht älter als 5 Minuten),
- actorId - Telematik-ID der LEI, für die der PoPP-Token ausgestellt wurde, muss abgeglichen werden, gegen die vom PoPP-Verifier authentifizierte LEI, die den PoPP-Token vorlegt

Alle weiteren Claims müssen entsprechend dem fachlichen Bedarfs ausgewertet werden. [\leq]

Hinweis: Die vollständige Liste der Claims und ihrer Ausprägung sind in [A_26431] spezifiziert.*

Ab diesem Punkt kann das PoPP-Token fachlich verarbeitet werden. Die Informationen aus dem PoPP-Token, insbesondere die Patienten- und Leistungserbringer-Identifikation, können zur Autorisierung von Zugriffen auf medizinische Daten verwendet werden.

5.1.3 Ersatz-Prüfungsnachweis (VSDM-PN)

Offener Punkt: Die geplanten Änderungen beim VSDM+-Prüfungsnachweis (C_12143 im Draft_ePAfueralle_3_0_3-1) wirken sich auf den Ersatz-Prüfungsnachweis (VSDM-PN) aus und sind hier noch nicht enthalten.

Es kann der Fall eintreten, dass Fachdienste, die heute eine Zugriffsautorisierung via VSDM-Prüfungsnachweis ("VSDM+") durchführen (E-Rezept und ePA-für-Alle), nicht unmittelbar auf die Nutzung von PoPP-Token umschwenken können (bspw. auf Grund der notwendigen Anpassungsbedarfe in den Diensten und den sich anschließenden Nachweis- und Zulassungsverfahren). Wenn dann die Fachdienste des VSDM ihren Betrieb einstellen, stünde für den E-Rezept und die ePA-für-Alle Fachdienste kein Mechanismus zur Zugriffsautorisierung zur Verfügung.

Deshalb soll für die Zeit der Migration von der Zugriffsaufklärung via "VSDM+" auf PoPP-Token für eine Übergangszeit auch vom PoPP-Service zusätzlich noch ein VSDM-Prüfungsnachweis (identisch zu dem von den VSDM-Fachdiensten ausgestellten Prüfungsnachweis, "VSDM+") erzeugt werden. Dieser Ersatz-Prüfungsnachweis wird im Folgenden mit VSDM-PN bezeichnet. Dieses Migrationsverfahren tritt nur temporär in Kraft und nur für den Zeitraum zwischen Start der Verfügbarkeit von PoPP-Service inklusive VSDM 2.0 und der Bereitstellung der Zugriffsaufklärung mittels PoPP-Token bei E-Rezept und ePA-für-Alle. Sobald also diese Fachdienste den Abruf mittels PoPP-Token produktiv anbietet, wird dieses Verfahren (zusätzliche Bereitstellung VSDM-PN) ersatzlos eingestellt.

Zur Funktionsweise:

Der PoPP-Service wird vorübergehend unter Ersatzvornahme für einen VSDM-Betreiber die Prüfziffer im Kontext der TI 2.0 erstellen. Dazu wird er als weiterer Betreiber einen HMAC-Schlüssel generieren und dem E-Rezept-FD, bzw. den ePA-Aktensystemen zur Verfügung stellen. Siehe [Kapitel Vorgaben zum VSDM-PN-HMAC-Sicherungsschlüssel].

Der PoPP-Service erzeugt bei der Token-Erstellung zusätzlich gemäß [A_26368*] mittels des ihm vorliegenden HMAC-Schlüssels eine gültige Prüfziffer für seine eigene Betreiberkennung und daraus einen VSDM-Prüfungsnachweis.

Dieser Prüfungsnachweis wird analog zum PoPP-Token an das aufrufende Primärsystem (PoPP-Client) übertragen. Das PS ist dadurch in der Lage, mit dem strukturierten Prüfungsnachweis des PoPP-Service beispielsweise einen E-Rezept-Abruf auszuführen, auch wenn der E-Rezept-Fachdienst PoPP noch nicht unterstützt.

Zu Rahmenbedingungen:

Sobald der Anbieter des PoPP-Service diese Funktionalität bereitstellt, gelten für ihn ebenfalls die Anforderungen zur sicheren Aufbewahrung, Übermittlung und Verarbeitung des HMAC-Schlüssels. Siehe auch in [gemSpec_Krypt#A_23460*, A_23461*, A_23463*].

Die Bereitstellung dieser Funktionalität ist temporär begrenzt und endet, sobald die Vornahme des E-Rezept-Abrufs mittels PoPP-Token erfolgen kann, die ePA-Aktensysteme vollständig umgestellt sind und der Rollout der angepassten PS abgeschlossen ist.

Die Nutzung des Ersatznachweises soll LEIs ausschließlich zur fachlichen Nutzung von E-Rezept und ePA-für-Alle zur Verfügung stehen, damit die Versorgungsqualität in der Migrationsphase von VSDM 1.0 zu VSDM 2.0 nicht beeinträchtigt wird.

Die Nutzung des Ersatznachweises VSDM-PN als Abrechnungsnachweis ist nicht erlaubt. Die Durchsetzung des Verbotes erfolgt durch organisatorische Maßnahmen der KTR.

5.1.3.1 Aufbau des VSDM-PN

Es wird für den Aufbau der Prüfziffer und des VSDM-PN der aus den VSDM1.0-Dokumenten hervorgehende Aufbau nachgenutzt. Dabei werden zum Teil aber feste Werte vorgegeben für Felder, die im VSDM1.0-Fall vom VSDM-Fachdienst oder VSDM-Fachmodul dynamisch vergeben werden.

Für die Erzeugung des VSDM-PN gelten entsprechend die folgenden Festlegungen, wobei die beim VSDM1.0 getrennt von Fachdienst und Fachmodul durchzuführenden Tätigkeiten zusammengefasst wurden.

A_26368 - PoPP-Service - Ersatz-Prüfungsnachweis (VSDM-PN) erstellen

Der PoPP-Service MUSS für die Erzeugung des VSDM-PN:

- eine Datenstruktur mit folgendem Aufbau erzeugen:

Nr	Feld	Format	Länge
1	10-stelliger unveränderlicher Teil der KVNR gemäß übergebenem PoPP-Token	alphanummerisch	10
2	aktuelle Unix-Zeit (bspw. "1673551622")	alphanummerisch	10
3	Fester Wert "U"	alphanummerisch	1
4	Fester Wert "2" Kennung des Betreibers PoPP-Service gemäß Liste der gematik	alphanummerisch	1
5	Für den Betreiber des PoPP-Service spezifische Version des HMAC-Schlüssels	alphanummerisch	1
6	Es wird ein HMAC nach [A_23461-*] über die konkatenierten Felder 1-5 mittels des	binär	24

	betreiberspezifischen Schlüssels berechnet. Dieser berechnete HMAC-Wert (256-Bit) wird auf 192 Bit (also 24 Byte) gekürzt (die ersten 24 Byte des HMAC-Wertes werden verwendet, die restlichen 8 Byte werden verworfen). Dieser gekürzte HMAC-Wert ist das 6-te Datenfeld.		
--	--	--	--

- die erhaltene Datenstruktur base64-kodieren: Das Ergebnis ist die Prüfziffer.
- eine XML-Struktur gemäß [VSDMPNSchema] erzeugen, die mit genau nur den folgenden Werten belegt wird:
 - <TS> = Zeitstempel im Format: yyyyymmddHHMMSS,
 - <E> = statischer numerischer Wert: 2,
 - <PZ> = die zuvor erzeugte Prüfziffer,
- und diese XML-Struktur zunächst gzip komprimieren und schließlich Base64-codieren: Das Ergebnis ist der VSDM-PN.

[<=]

Beispiel für einen Prüfungsnachweis aus dem E-Rezept-Kontext, bei dem in der Prüfziffer die Betreiberkennung "T" verwendet wurde:

```
H4sIAAAAAAAAAAB2N3U6DMABGX4X01khbCM6YtssiNf5RRFiXeGPAdghbC1pk4tPb70a70ML3Dln
/mmMw62/
XDZYCHCIQaPsxqM62FGyru8trELiptqo+DLZTsGgH1oy8iMAfraPgc5rGGwhPLmy1qaFuECoN9z
WcnTJwTcc4n6W3afYu+Wv5kItzxjNGqpJFKIpRgq/
QCsV4RaBhhLOIQ04jb0ymGyR6jrK+SPKKR3laLFm/
wXmLpEzvHy+K7V+72zX78qkZXaKbRfAvYw5KPsF4J6MEeokfwf4B14Neo+oAAAA=
```

5.1.3.2 Vorgaben zum VSDM-PN-HMAC-Sicherungsschlüssel

In diesem Kapitel sind die Vorgaben zur Erzeugung und Verteilung des HMAC-Sicherungsschlüssels für die Prüfziffer innerhalb des VSDM-PN zusammengefasst.

A_23459-01 - PoPP-Service - VSDM-PN-HMAC-Schlüsselerzeugung, 4-Augen-Prinzip

Der PoPP-Service MUSS den VSDM-PN-HMAC-Sicherungsschlüssel:

1. im Verarbeitungskontext der VAU erzeugen,
2. ausschließlich innerhalb eines Verarbeitungskontextes im Klartext nutzen,
3. ausschließlich mit dem Persistenzschlüssel entsprechend [A_26604*] und [A_26605*] geschützt außerhalb eines Verarbeitungskontextes speichern,
4. immer mit den folgenden Schlüsselattributen speichern:
 - a. Kennung des Betreibers PoPP-Service, fester Wert "2",
 - b. Version (unterschiedlich für jeden zu speichernden HMAC-Schlüssel) und
 - c. Erzeugungsdatum.

[<=]

Hinweis: Weitere Vorgaben zum HMAC-Schlüssel befinden sich in [gemSpec_Krypt#Kapitel HMAC-Sicherung der Prüfziffer VSDM].

A_26513 - PoPP-Service - VSDM-PN-HMAC-Schlüssel - Auslösen Erzeugung und Verwendung durch Anbieter

Der PoPP-Service MUSS es dem Anbieter ermöglichen:

1. sich die aktuell im PoPP-Service enthaltenen Fachdienst-VAU-Zertifikate ausgeben zu lassen,
2. die Erzeugung eines neuen VSDM-PN-HMAC-Schlüssels auszulösen,
3. einen neu erzeugten VSDM-PN-HMAC-Schlüssels zur Verwendung zu aktivieren (Kontext Schlüsselwechsel).

[<=]

Hinweis: Zwischen Erzeugung und Verwendung vergeht eine gewisse Zeit, bis der neue VSDM-PN-HMAC-Schlüssel bei allen Fachdiensten importiert wurde. Erst wenn alle Fachdienste den erfolgreichen Import gemeldet haben, kann der neue Schlüssel verwendet werden.

A_23464-01 - PoPP-Service - Export des für Fachdienste verschlüsselten VSDM-PN-HMAC-Schlüssels

Der PoPP-Service MUSS dem Anbieter nach dem Erzeugen eines neuen VSDM-PN-HMAC-Schlüssels für jeden Fachdienst, für den ein VAU-Zertifikat im PoPP-Service vorhanden ist, ein Export-Paket so ausgeben, dass für den Anbieter erkenntlich wird, für welchen Fachdienst das Export-Paket erzeugt wurde und dass er jeweils wie folgt erzeugt:

1. der erzeugte VSDM-PN-HMAC-Schlüssel wird nach den Vorgaben aus [A_23463*] auf Basis des im PoPP-Service verfügbaren Fachdienst-VAU-Verschlüsselungszertifikats verschlüsselt, das Ergebnis ist "encrypted_key",
2. es wird der HMAC der leeren Bytefolge berechnet (Kontext: Prüfwert des HMAC-Schlüssels für den Import in die Fachdienst-VAU), das Ergebnis ist "hmac_empty_string",
3. es wird das Export-Paket als JSON-Datenstruktur wie folgt erzeugt, wobei die ersten drei Felder entsprechend der Schlüsselattribute des erzeugten VSDM-PN-HMAC-Schlüssels befüllt werden:

```
{
  "betreiberkennung": "2",
  "version": "1",
  "exp": "2024-02-01",
  "encrypted_key":
    "0160141038f2f9b772621c1cf1b9a71c44fcf24766999392b3d184
    950a78c04f444d130be1f4bebd52f5fb9d1897475cac910b4aecbb4855c2f8692ab0f
    2d165777486
    421f7cc26654aeb5cb192118a5cc677cfad855fdc8d77a106f0d198e1147863171866
    a1e7a80a19c
    e528c94eb3884e4be13c4aaaaa48e292f8a1",
  "hmac_empty_string":
    "5ce3ee26f9956e7ef200481a891341760579ddb566ec9bd43346ef432c2c3cb"
}
```

[<=]

Hinweis: Im Export-Paket wird das Ablaufdatum (exp) des VSDM-PN-HMAC-Schlüssels angegeben, während als Schlüsselattribut das Erzeugungsdatum gespeichert wird. Da der Schlüsseltausch jährlich erfolgen muss, wird als Ablaufdatum das Datum der Erzeugung plus ein Jahr verwendet.

A_26951 - PoPP-Service - Verwendung neuer VSDM-PN-HMAC-Schlüssel nach Aktivierung

Der PoPP-Service MUSS durchsetzen, dass nach Aktivierung eines neuen VSDM-PN-HMAC-Schlüssels ausschließlich dieser Schlüssel im Rahmen der Erzeugung von Prüzziffern verwendet wird. [≤]

A_23465-01 - PoPP-Service Anbieter - VSDM-PN-HMAC-Schlüsselwechsel

Der Anbieter des PoPP-Service MUSS den VSDM-PN-HMAC-Schlüssel des FD mindestens einmal jährlich neu erzeugen und als Export-Paket an den E-Rezept-FD und die ePA-Aktensysteme zur Einpflege übermitteln. [≤]

A_23509-01 - PoPP-Service Anbieter - Alte VSDM-PN-HMAC-Schlüssel nicht verwenden

Der Anbieter des PoPP-Service MUSS nach erfolgreich abgeschlossener Einpflege des neuen VSDM-PN-HMAC-Schlüssels im E-Rezept-FD und in den ePA-Aktensystemen, den neuen VSDM-PN-HMAC-Schlüssel zur Verwendung aktivieren. [≤]

Hinweis: Wenn nach einem VSDM-PN-HMAC-Schlüsselwechsel in einem FD dieser neue VSDM-PN-HMAC-Schlüssel eingebracht worden ist und der alte VSDM-PN-HMAC-Schlüssel im FD gelöscht wurde, dann haben alte VSDM-PN-HMAC-Schlüssel keinen Schutzbedarf bezüglich Vertraulichkeit mehr.

A_26959 - PoPP-Service Hersteller - Bezug Fachdienst-VAU-Verschlüsselungszertifikate

Der Hersteller des PoPP-Service MUSS sicherstellen, dass er

1. die Fachdienst-VAU-Verschlüsselungszertifikate im Mehr-Augen-Prinzip von der gematik erhält (über mindestens zwei unterschiedliche Informationskanäle),
2. die Zertifikate, bevor er sie in das PoPP-Service-VAU-Image einbindet nochmals deren Integrität und Gültigkeit prüft (kann teilweise organisatorisch erfolgen, bspw. direkt vor dem Einbringen den Hashwert des Zertifikats und Laufzeit überprüfen).

[≤]

Hinweis: Vergleiche auch [A_26960] bzgl. Einbindung der Zertifikate in das VAU-Image.*

A_23466-01 - PoPP-Service Anbieter - VSDM-PN-HMAC-Schlüssel an FD übermitteln

Der Anbieter des PoPP-Service MUSS sicherstellen, dass er:

1. vor dem Erzeugen eines neuen VSDM-PN-HMAC-Schlüssels und dem damit verbundenen Export der Export-Pakete für die Fachdienste, die aktuell im PoPP-Service vorliegenden Fachdienst-VAU-Verschlüsselungszertifikate hinsichtlich Integrität und Gültigkeit prüft (bspw. direkt vor Verwendung Zertifikate ausgeben lassen und deren Hashwert und Laufzeit überprüfen, kann teilweise organisatorisch erfolgen) und nur im Falle einer positiven Prüfung
2. das Export-Paket über mindestens zwei sichere Kanäle an den Betreiber des jeweiligen Fachdienst übermitteln, wofür er das Export-Paket zum einen über das TI-ITSM-System an den Betreiber des jeweiligen Fachdienst übermitteln und zum anderen an die gematik per Brief (traditionelle Papier-basierter Brief) an die gematik (Adressat "E-Rezept-Projekt", bzw. "ePA Projekt") sendet.

[≤]

Hinweis: Die gematik stellt Beispiel-Code für die Erzeugung eines Export-Pakets bereit. Für die Übermittlung und Verarbeitung des VSDM-PN-HMAC-Schlüssels gelten in der [gemSpec_Krypt#A_23460, A_23461*, A_23463*].*

5.2 Datenschutz und Sicherheit

Der PoPP-Service ist frei im Internet erreichbar und muss entsprechend seine Außenschnittstellen vor Angriffen und unberechtigten Zugriffen schützen. Dies geschieht im Sinne der TI 2.0 über die Zero Trust Mechanismen bzw. konkret durch das Einbinden des von der gematik bereitgestellten ZETA Guard.

Der PoPP-Service verarbeitet Daten, aus denen genau nachvollziehbar ist, welche Versicherten bei welchen LEI in Behandlung sind. Bereits im Einzelnen, insbesondere aber in der Summe mehrerer solcher Daten pro Versicherten (Profilbildung) sind damit Rückschlüsse auf medizinische Sachverhalte möglich. Daher sind die vom PoPP-Service verarbeiteten Daten, als personenbezogene medizinische Daten zu bewerten. Zudem hat der PoPP-Service Zugriff auf den privaten Signaturschlüssel um PoPP-Token zu erstellen, über die wiederum Zugriffe auf medizinische Daten der Versicherten möglich werden. Daher müssen Zugriffe des Betreibers auf diese Daten mit technischen Mittel verhindert werden, weshalb der PoPP-Service innerhalb einer VAU laufen muss.

Da der ZETA Guard die von den LEI eingehenden TLS-Verbindungen terminieren muss, um die eingehenden Daten analysieren zu können, hat er rein technisch Zugriff auf alle übertragenen Daten im Klartext. Daher muss der ZETA Guard innerhalb der VAU laufen (vgl. [gemSpec_ZETA#A_25608]).

A_26469 - PoPP-Service - Ausschließlich TLS-Verbindungen

Der PoPP-Service MUSS sicherstellen, dass er nur TLS-geschützte Verbindungen zu allen externen Kommunikationspartnern herstellt. [\leq]

A_26467 - PoPP-Service - Prüfung TLS-Zertifikat sektoraler IDP

Der PoPP-Service MUSS beim TLS-Verbindungsaufbau zum sektoralen IDP das präsentierte TLS-Server-Zertifikat wie folgt prüfen:

1. Verifikation der zeitlichen Gültigkeit,
2. Verifikation des Hostname,
3. Prüfung der Rückführbarkeit zu einer CA aus dem CA/Browser Forum

und den Verbindungsaufbau im Falle einer negativen Prüfung abbrechen. [\leq]

A_27082 - PoPP-Service - DDoS-Protection

Der Anbieter des PoPP-Service MUSS Angriffe auf die Verfügbarkeit des PoPP-Service (DDoS) an seinen Schnittstellen zum Internet abwehren und dafür einen qualifizierten Dienstleister zum Schutz vor DDoS-Angriffen beauftragen, der im BSI-Dokument „Qualifizierte DDoS-Mitigation Dienstleister“ ([BSI-QDDoS]) gelistet ist. [\leq][\leq]

A_27219 - PoPP-Service - Absicherung Internet-Schnittstellen mit Paketfiltern

Der Anbieter des PoPP-Service MUSS die Schnittstellen des PoPP-Service zum Internet durch Paketfilter absichern, welche ausschließlich die erforderlichen Protokolle weiterleiten und nicht auf denselben Systemen laufen wie der PoPP-Service selbst und dabei die Empfehlungen des BSI [BSI ISI-LANA] befolgen. [\leq]

A_26470 - PoPP-Service - Schutz vor Angriffen auf Anwendungsebene

Der PoPP-Service MUSS sicherstellen, dass Angriffe auf Anwendungsebene erkannt und abgewehrt werden, indem er mindestens alle Daten und Parameter, die der PoPP-Service über seine API empfängt, sicherheitstechnisch validiert, bevor sie fachlich verarbeitet werden. Erkannte Angriffe MÜSSEN für das Zero Trust Security Monitoring berücksichtigt werden. [\leq]

Hinweis: Der ZETA Guard führt bereits eine gewisse Angriffserkennung durch, jedoch kann er die eingehenden Daten nicht entsprechend den erwarteten Schemata/Mustern bewerten, da diese nur dem PoPP-Service bekannt sind (siehe Kommentar zu in [gemSpec_ZETA#A_25406]). Zudem werden Anfragen von Versicherten über ein PoPP-Modul nicht über den ZETA Guard geleitet, sondern direkt vom Authorization Server des*

PoPP-Service entgegen genommen.
Es sind [A_25421*] und [A_26612*] zu berücksichtigen.

A_27380 - PoPP-Service - Rate-Limit für Anfragen mit ungültige TAN

Der PoPP-Service MUSS ein Rate-Limit für Anfragen mit ungültigen TAN umsetzen und dabei wie folgt vorgehen:

- Im Falle einer als ungültig erkannten TAN wird die Telematik-ID der anfragenden LEI gespeichert und für diese LEI ein Counter mit einer Laufzeit von einer Stunde (1 h) eingerichtet.
- Nach Ablauf der Laufzeit des Counters wird die Telematik-ID und der Counter gelöscht.
- Innerhalb der Laufzeit des Counters:
 - erhöht jede weitere Anfrage mit einer ungültigen TAN den Counter um eins,
 - werden alle weiteren Anfragen der LEI abgelehnt, wenn der Counter 100 erreicht hat.

[<=]

Hinweis: Somit können von einer LEI maximal 100 Aufrufe mit falschen TAN pro Stunde getätigt werden.

A_26472 - PoPP-Service - Eingeschränkte Speicherung von Daten

Der PoPP-Service MUSS sicherstellen, dass keine anderen Anwendungsdaten - weder temporär noch permanent - gespeichert werden außer:

1. TANSet-Records - ausschließlich verschlüsselt und integritätsgeschützt,
2. Einträge in der eGK-Hash-Datenbank - ausschließlich min. integritätsgeschützt.

[<=]

Hinweis: Bzgl. verschlüsselter Speicherung inkl. Integritätsschutz siehe [A_26603, A_26604*, A_26605*]. Bzgl. Einträgen in die eGK-Hash-Datenbank siehe Absatz [Kapitel eGK-Hash-Datenbank]. Von [A_26472*] ausgenommen ist zum einen für die Funktionalität notwendiges Schlüsselmateriale und zum anderen Monitoring-Daten, die durch andere Anforderungen gefordert werden.*

A_26592 - PoPP-Service - Rollentrennung zwischen Hersteller und Anbieter

Der Hersteller bzw. Anbieter eines PoPP-Service MUSS sicherstellen, dass Personen, die an der Herstellung/Implementierung des PoPP-Service beteiligt sind (Rolle Hersteller), nicht zeitgleich am Betrieb des PoPP-Service beteiligt sind (Rolle Anbieter) und dass entsprechende Prozesse definiert und etabliert sind, die dies dauerhaft gewährleisten und eine regelmäßige Validierung der Umsetzung durchsetzen. Die Umsetzung des Rollenausschlusses MUSS die Weisungsbefugnis von Vorgesetzten berücksichtigen. Das bedeutet, dass kein Vorgesetzter direkte Weisungsbefugnis sowohl für Personen mit der Rolle "Hersteller" als auch für Personen mit der Rolle "Anbieter" haben darf. Eine Ausnahme bildet das Management des Unternehmens, wenn beide Rollen vom selben Unternehmen gestellt werden. **[<=]**

5.2.1 Vertrauenswürdige Ausführungsumgebung (VAU)

5.2.1.1 Allgemein

Der PoPP-Service wird innerhalb einer Vertrauenswürdigen Ausführungsumgebung (VAU) betrieben. Dies betrifft alle Komponenten des PoPP-Service: ZETA Guard, PoPP-Service Authorization Server und PoPP-Service Resource Server.

Die VAU besteht aus der Summe von Maßnahmen in Software und Hardware, die den Schutz vor unberechtigten Zugriffen des Anbieters/Betreibers eines TI-Dienstes auf schützenswerte Daten und Schlüssel gewährleisten. Die Software besteht aus dem VAU-Image, das vom Hersteller bereitgestellt wird und aus dem die Verarbeitungskontexte der VAU im Betrieb gestartet werden. Innerhalb eines gestarteten Verarbeitungskontextes werden dann die schützenswerten Daten verarbeitet bzw. kann aus diesem Verarbeitungskontext auf schützenswerte Schlüssel zugegriffen werden. Diese schützenswerten Schlüssel werden in einem Hardware Security Module HSM gespeichert und ebenso werden im HSM Prüfungen zur Validierung von VAU-Images durchgeführt.

Die Sicherheitsleistung beruht u. a. auch auf der Nutzung Hardware (HW)-naher Funktionen, weshalb auch die zugrundeliegende Hardware zur VAU gehört und somit Teil des Produkts ist.

A_26471 - PoPP-Service - VAU - Umsetzung einer VAU

Der PoPP-Service MUSS eine VAU umsetzen und durchsetzen, dass:

1. nur innerhalb eines Verarbeitungskontextes der VAU eingehende Daten von Versicherten und LEIs im Klartext verarbeitet werden,
2. nur durch einen Verarbeitungskontext der VAU die folgenden Schlüssel im HSM nutzbar sind:
 - a. privater Schlüssel für die PoPP-Token-Signatur,
 - b. Schlüssel zur Authentisierung ggü. anderen Verarbeitungskontexten,
3. nur durch einen Verarbeitungskontext der VAU die folgenden Schlüssel im HSM erzeugbar und aus dem HSM exportierbar sind:
 - a. privater Schlüssel PoPP-Service-TLS-Server-Identitäten (Richtung PS und PoPP-Modul integrierender App sowie eGK-CVC|X.509-Hashwert-Import),
 - b. privater Schlüssel PoPP-Service-TLS-Client-Identität (Richtung sektorialem IDP),
 - c. privater Schlüssel für die APDU-Paket-Signatur,
 - d. privater Schlüssel für die Entschlüsselung von ID Token,
 - e. privater Schlüssel für die Access Token-Signatur
 - f. privater Schlüssel für die Access Token-Entschlüsselung
4. nur Verarbeitungskontexte der VAU Persistenzschlüssel aus dem HSM ableiten können,
5. innerhalb eines Verarbeitungskontextes erzeugte Daten entsprechend [A_26472*] ausschließlich mittels Persistenzschlüssel verschlüsselt außerhalb der VAU abgelegt werden.

[<=]

A_27042 - PoPP-Service - VAU - Gehärtete Schnittstellen für Anbieter

Die VAU des PoPP-Service MUSS die für den Anbieter zugänglichen Schnittstellen härten und robust machen gegenüber Angriffen wie bspw. Fehleingaben oder dem Import maliziöser Daten.**[<=]**

Hinweis: Die Spezifikation fordert gewisse Konfigurations- und Import-Möglichkeiten an der VAU für den Anbieter.

Der Schutz vor Angriffen an den Außenschnittstellen erfolgt zum Teil über den ZTC und ist zudem in [A_26470] geregelt.*

5.2.1.2 Einbinden des ZETA Guard der gematik

Der PoPP-Service verwendet als TI 2.0-Service die Mechanismen des Zero Trusts für die Zugriffskontrolle. Dazu wird von der gematik zentral ein Software-Image für den ZETA Guard bereitgestellt, der von den Diensten der TI 2.0 eingebunden wird.

Für die Funktionsfähigkeit des ZETA Guard muss dieser den TLS-Kanal terminieren um die notwendigen Daten für die Zugriffsentscheidung zu erhalten und auswerten zu können. Bei PoPP fungiert TLS als VAU-Kanal, muss also innerhalb eines Verarbeitungskontextes (VK) der VAU terminieren. Entsprechend muss der ZETA Guard ebenso als Verarbeitungskontext (entweder als eigener VK oder als Teil eines Gesamt-VK mit der PoPP-Logik zusammen) in der VAU betrieben werden.

Da der von der gematik bereitgestellte ZETA Guard ein reines Docker-Image ist, muss es vom Hersteller PoPP in die Lage versetzt werden, als VAU-Image in der VAU des PoPP-Service importiert werden zu können und dort lauffähig zu sein.

Der ZETA Guard ist also so im Build-Prozess zu berücksichtigen, dass dieser ohne manuelle Anpassungen am Code automatisiert integriert werden kann. Da häufige Updates des ZETA Guard zu erwarten sind (insbesondere schnelle Patches bei neuen, relevanten CVE), ist ein manueller Anpassungsprozess zur Herstellung der Kompatibilität des ZETA Guard zur VAU des PoPP-Service inakzeptabel.

Im Folgenden wird das System, das den Prozess zur Erzeugung von VAU-Images umsetzt und dabei automatisiert den ZETA Guard einbindet VAU-Image-Build-Pipeline genannt.

A_26468 - PoPP-Service - Bereitstellung VAU-Image-Build-Pipeline und automatisiertes Einbinden des ZETA Guard

Der Hersteller des PoPP-Service MUSS eine VAU-Image-Build-Pipeline bereitstellen und nutzen, von der:

1. das seitens gematik bereitgestellte ZETA Guard-Image entgegengenommen wird, wobei:
 - a. die gematik-Signatur des Images gegen den als vertrauenswürdig hinterlegten gematik-Signatur-Prüf Schlüssel verifiziert wird und
 - b. das Image genau nur bei erfolgreicher Signaturprüfung übernommen wird, und anschließend automatisiert:
1. entweder aus der PoPP-Service-Logik und dem ZETA Guard-Image ein gemeinsames VAU-Image erzeugt wird
2. oder aus jeweils PoPP-Service-Logik und ZETA Guard-Image ein eigenes VAU-Image erzeugt wird, wobei in jedes VAU-Image ein Vertrauensanker für die Authentifizierung anderer Verarbeitungskontexte hinterlegt wird, und anschließend automatisiert:
1. zu jedem VAU-Image der signierte Attestierungswert mit der gleichen Methodik/Technik ermittelt wird, wie sie auch in der VAU im Betrieb verwendet wird und
2. das/die VAU-Image(s) und die dazugehörigen signierten Attestierungswerte ausgegeben werden.

[<=]

Hinweis: Der in der zweiten Variante ("oder") genannte Vertrauensanker wird bei der gegenseitigen Authentifizierung bei der Kommunikation Verarbeitungskontext-zu-Verarbeitungskontext verwendet. Die Identitäten des jeweiligen Verarbeitungskontextes und die ausstellende CA sind auf dem HSM der VAU gespeichert [A_26610] und werden bei der initialen Zeremonie [A_26623*] erzeugt. Dabei wird der öffentliche Schlüssel der CA exportiert, der dann als Vertrauensanker in die VAU-Images eingebracht wird. Die Authentifizierung eines anderen Verarbeitungskontext ist in ersterer Variante ("entweder") nicht notwendig, da die Kommunikation ZETA Guard<=>PoPP-Service-Logik dort innerhalb des Verarbeitungskontext stattfindet.*

Ggf. ist zudem der Import eines Vertrauensankers für die Kommunikation zum HSM (Authentifizierung des HSM durch den Verarbeitungskontext) notwendig. Es kann hier dieselbe CA verwendet werden (so ist es im Hinweis unter [A_26623] beschrieben). Grundsätzlich sind aber auch andere Methoden zur Etablierung eines beidseitig authentisierten Kanals zwischen Verarbeitungskontext und HSM möglich, solange der Verarbeitungskontext das HSM eindeutig authentifizieren kann.*

Die VAU-Image-Build-Pipeline muss im Rahmen der Produkt-Begutachtung des PoPP-Service geprüft werden. Der ZETA Guard selbst hat einen von der gematik abgenommenen Sicherheitsnachweis (Produktgutachten). Daher muss dieser bei dem beschriebenen Vorgehen nicht noch einmal sicherheitstechnisch betrachtet werden.

A_26822 - PoPP-Service - Sichere VAU-Image-Erzeugung (Prozess)

Der Hersteller des PoPP-Service MUSS einen sicheren Gesamtprozess zur VAU-Image-Erzeugung umsetzen und dabei:

1. die geprüfte VAU-Image-Build-Pipeline nutzen,
2. im 4-Augen-Prinzip abgesichert den gematik-Signaturprüfschlüssel für den ZETA Guard in die VAU-Image-Build-Pipeline einbringen und
3. Abwehrmaßnahmen umsetzen gegen Manipulationen der VAU-Image-Build-Pipeline durch einen Innentäter, was auch das Verhindern des unberechtigten Einbringens von Signatur-Prüfsschlüsseln umfasst.

[<=]

5.2.1.3 Informative Erläuterung zu den Zielen der VAU und den konkreten Umsetzungshinweisen

Das Ziel der VAU ist der Ausschluss unberechtigter Zugriffe des Anbieters/Betreibers des Dienstes auf schützenswerte Daten und Schlüssel. Darüber hinaus sind die Sicherheitsanforderungen an die VAU und die Anforderungen an die Qualität der sicherheitstechnischen Begutachtung der genutzten Hardware und Software geeignet, auch gegen unberechtigte Zugriff anderer Angreifer zu schützen.

Bei PoPP sind die zu schützenden Daten zum einen die Information, welche Versicherten zu welchem Zeitpunkt welche LEI aufsuchen, woraus ein detailliertes Profil mit Rückschlüssen auf medizinische Daten des Versicherten erstellt werden kann. Zum anderen ist dies der PoPP-Token-Signaturschlüssel, mit dem PoPP-Token erzeugt werden können, die wiederum für den Zugriff auf medizinische Daten von Versicherten autorisieren.

Die zu berücksichtigen Angriffsszenarien schließen auch Zugriffe durch einzelne Innentäter beim Betriebspersonal ein. Personen aus diesem Kreis haben aufgrund Ihrer Position erhöhte Rechte und bessere Möglichkeiten grundsätzlich auf Daten zuzugreifen. Unabhängig von diesbezüglich getroffenen organisatorischen Maßnahmen sind zusätzliche technische Maßnahmen notwendig, um auch Angriffe von solchen Innentätern abzuwehren.

Ziel der VAU ist aber auch, trotz des umzusetzenden Betreiberausschlusses bei den Maßnahmen eine gute Balance zwischen Sicherheit und Betreibbarkeit zu finden. Insbesondere soll vermieden werden, dass das Einspielen von Updates jedes Mal mit aufwändigen Prozessen und der Beteiligung verschiedener Rollen verbunden ist. Im Gegensatz dazu ist ein aufwändiger Prozess unter Beteiligung mehrerer Rollen bei einer einmaligen oder zumindest sehr seltenen Zeremonie zur Inbetriebnahme vertretbar.

Entsprechend wird im Folgenden (vorrangig über Hinweise zu den Anforderungen) eine Umsetzung beschrieben, die sowohl die hier gestellten Anforderungen an die VAU erfüllt, als aber auch einen geringen Aufwand beim Einspielen von Updates im Betrieb erzeugt. Durch eine technisch durchgesetzte und geschützte Protokollierung sind dennoch jederzeit unberechtigte Veränderungen durch Dritte (gematik) eindeutig nachvollziehbar. In solchen Fällen werden dann entsprechende Maßnahmen zur Klärung und Behebung unternommen. Somit kann der Anbieter bzw. ein etwaige Innentäter auch ohne eine direktes Mehr-Augen-Prinzip nicht unbemerkt handeln.

Als Sicherheitsanker muss immer ein HSM zum Einsatz kommen, wobei durch die vorgeschlagene Umsetzung Firmwareanpassungen in Form eines HSM-Moduls notwendig werden. Auch diese Aufwände wirken sich nicht negativ auf den Betrieb aus, sondern fallen nur vor der Inbetriebnahme an.

Der kurz zusammengefasste Umsetzungsansatz

Der Anbieter kann eigenständig VAU-Images (PoPP und ZETA Guard) im HSM als Hashwert bekannt machen und das Image in die VAU einspielen. Das HSM prüft bei der Bekanntmachung, dass der Hashwert vom Hersteller signiert ist. Nach Übernahme eines Hashwerts protokolliert das HSM diesen und signiert das Protokoll, mit Schlüsseln, auf die nur das HSM zugreifen kann. Das Protokoll kann exportiert werden. Der Prüfschlüssel für die Protokollsignatur liegt der gematik vor. Da die gematik jedes VAU-Update vom Hersteller gemeldet bekommt und in diesem Zuge auch den Hashwert des fertigen VAU-Images erhält, kann jederzeit über das Protokoll aus dem HSM nachvollzogen werden, dass vom Anbieter nur die VAU-Images bekannt gemacht wurden, die auch vom Hersteller gemeldet worden sind. Ein aus einem VAU-Image gestarteter Verarbeitungskontext muss über Mittel der VAU attestiert werden und nur mit gültigen Attestierungsinformationen kann der Verarbeitungskontext auf Schlüssel im HSM zugreifen bzw. diese dort erzeugen lassen und exportieren. Das HSM erkennt zulässige Verarbeitungskontexte am Hashwert des VAU-Images, aus dem der Verarbeitungskontext gestartet wurde, da dieser Teil der Attestierungsinformationen ist und gegen die im HSM hinterlegten Hashwerte abgeglichen werden kann. Die Attestierungsinformationen sind von sicher in der VAU gespeicherten Schlüsseln signiert, sodass das HSM die Validität der präsentierten Informationen prüfen kann (wenn es zuvor die öffentlichen Prüfschlüssel für die sicher in der VAU gespeicherten Signatur-Schlüssel erhalten hat).

Ebenso wie VAU-Images bzw. deren Hashwert können dann auch erzeugte Schlüssel (bzw. deren öffentlicher Teil) protokolliert werden. Somit ist auch eine Verifikation möglich, dass für die verschiedenen Identitäten des PoPP-Service (bspw. für TLS) auch tatsächlich nur Schlüssel verwendet werden, die ausschließlich durch einen Verarbeitungskontext der VAU genutzt werden können.

Für das Vorgehen ist eine initial sichere Zeremonie notwendig, bei der u. a. alle notwendigen Prüfschlüssel in das HSM importiert werden und der Protokollprüfschlüssel exportiert wird. Zudem wird der Anbieter von allen Zugriffen auf das HSM ausgeschlossen, die nicht absolut notwendig sind (bspw. der Import signierter VAU-Image-Hashwerte ist für den Anbieter möglich).

In den Hinweisen zu einem Teil der Anforderungen wird im Folgenden dieses Vorgehen detailliert.

5.2.1.4 Lifecycle eines Verarbeitungskontextes

A_26594 - PoPP-Service - VAU - Import VAU-Images nur nach erfolgreicher Signaturprüfung

Die VAU des PoPP-Service MUSS vor der Übernahme eines importierten VAU-Images die Signatur des Images verifizieren und prüfen, dass diese vom Dienst-Hersteller ausgestellt wurde und das Image nur im Positivfall übernehmen. [≤]

A_26593 - PoPP-Service - VAU - Ausschluss Manipulationen der Software bei Start eines Verarbeitungskontextes

Die VAU des PoPP-Service MUSS technisch sicherstellen, dass ausschließlich das unveränderte, aktuelle, vom Dienst-Hersteller autorisierte VAU-Image (bzw. das jeweils aktuelle PoPP- und ZETA Guard-VAU-Image, wenn getrennte VAU-Images verwendet werden) als Verarbeitungskontext gestartet wird, wobei die Attestierungsinformationen durch die VAU ermittelt und kryptographisch geschützt werden müssen. Die Prüfung der Attestierungsinformationen, ob es sich um ein autorisiertes VAU-Image handelt, muss auf einem in einem HSM gespeicherten Vertrauensanker beruhen. [≤]

Hinweis: Eine technische Umsetzung von [A_26593] ist die Ermittlung des Hashwerts des zu startenden VAU-Images durch die VAU und die Signatur dieses Hashwerts mit einem sicher gespeicherten (bspw. in einem TPM) Signaturschlüssel des Herstellers der HW-Plattform (Chip-Hersteller) oder des Herstellers des PoPP-Service. Diese Attestierungsinformation kann dann an prüfende Systeme, wie bspw. das HSM übermittelt werden, wobei das verwendete Protokoll vor Replay-Attacken schützen muss (das HSM muss erkennen können, dass die Attestierungsinformationen frisch für das HSM erzeugt wurden). Dem HSM müssen entsprechend über einen sicheren Prozess zum einen die Prüfschlüssel des Chip-Herstellers bzw. PoPP-Service-Herstellers und zum anderen die zulässigen Hashwerte von VAU-Images bekannt gemacht werden. Um einen späteren Rollback zu verhindern wird immer genau nur gegen den letzten hinzugefügten also den aktuellen Hashwert eines jeweiligen VAU-Images geprüft bzw. ist nur kurzzeitig nach dem Einspielen die Möglichkeit eines Rollback auf das letzte davor verwendete Image möglich (siehe A_27373*).*

A_27373 - PoPP-Service - VAU - Temporäre Möglichkeit des Rollback auf vorherige Version

Die VAU des PoPP-Service MUSS es ermöglichen, dass nach dem Einspielen eines neuen VAU-Image, für eine Übergangszeit von zwei Tagen ein Rollback auf das letzte davor verwendete VAU-Image durchgeführt werden kann. [≤]

Hinweis: Nach Einspielen eines neuen Hashwerts ins HSM akzeptiert dieses somit für zwei Tage auch Verarbeitungskontexte, die in ihren Attestierungsinformationen den zweit jüngsten im HSM vorliegenden Hashwert vorweisen. Dies dient der Möglichkeit eines schnellen Rollback, falls nach Einspielen und Inbetriebnahme einer neuen Version massive Fehler im Betrieb auftreten.

A_26595 - PoPP-Service - VAU - Regelmäßiger Neustart der Verarbeitungskontexte

Die VAU des PoPP-Service MUSS durchsetzen, dass:

1. Ein Verarbeitungskontext maximal eine Stunde (1 h) verwendet wird und somit fortlaufend neue Verarbeitungskontexte frisch aus dem jeweiligen Image gestartet werden.
2. Dabei dürfen aktuell verwendete Verarbeitungsprozesse (Abarbeiten eines Operationsaufrufs läuft noch) nicht abgebrochen werden, sondern müssen entsprechend der funktionalen Vorgaben zu Ende geführt werden, bevor der Verarbeitungskontext geschlossen wird und
3. für parallel eintreffende neue Operationsaufrufe ein anderer, zeitlich noch gültiger Verarbeitungskontext verwendet wird.

Der VAU ist es auch erlaubt für jeden Operationsaufruf einen neuen eigenen Verarbeitungskontext zu starten und nach Abarbeiten des Aufrufs sofort wieder zu schließen. [≤]

Hinweis: Es wird davon ausgegangen, dass die VAU es leistet, dass mehrere Verarbeitungskontexte parallel ausführbar sind.

A_26596 - PoPP-Service - VAU - Attestierung durch Systeme außerhalb der VAU

Die VAU des PoPP-Service MUSS es technisch ermöglichen, dass es für Dritte außerhalb der VAU prüfbar ist, dass ein Verarbeitungskontext aus einem integren, autorisierten VAU-Image gestartet wurde. [≤]

Hinweis: Bei den in [A_26596] genannten Dritten handelt es sich beispielsweise um die gematik, Systeme beim Anbieter PoPP-Service (bspw. andere Verarbeitungskontexte) oder auf den PoPP-Service zugreifende Clients.*

A_26597 - PoPP-Service - VAU - Erkennen von Manipulationen an der HW der VAU - Softwareanteil

Die VAU des PoPP-Service MUSS technisch sicherstellen, dass Maßnahmen zur Manipulationserkennung seitens der Hardware der VAU oder der die VAU umgebenden HW, von der VAU so unterstützt werden, dass Zugriffe auf die HW von der VAU erkannt werden und in diesem Fall sämtliche Verarbeitungskontexte beendet werden, so dass ein unberechtigter Zugriff auf Daten (Extraktion oder Manipulation) durch den physischen Zugriff auf die Hardwarekomponenten der VAU ausgeschlossen ist. [≤]

Hinweis: Es ist zulässig, dass physische Schutzmaßnahmen in der Hardware der VAU umgesetzt werden (bspw. in etwa im Ansatz vergleichbar mit denen eines HSMS) und/oder in zusätzlicher vom Anbieter bereitgestellter Hardware (bspw. durch einen mit zusätzlichem Zutrittsschutz ausgestatteten Serverchrank). In jedem Fall besteht eine Kopplung dieser physischen Schutzmaßnahmen zur VAU-Software, damit bei durch diese Schutzmaßnahmen erkannten Zugriffen eine Reaktion der VAU stattfindet, so dass Verarbeitungskontexte geschlossen und somit alle flüchtigen Daten aus dem System entfernt werden.

A_26598 - PoPP-Service - VAU - Erkennen von Manipulationen an der Hardware der VAU - Hardwareanteil

Die VAU des PoPP-Service oder der Anbieter des PoPP-Service MUSS technische Maßnahmen zum physischen Schutz umsetzen, die Zugriffe auf die Hardwarekomponenten der VAU erkennen und diese unmittelbar an die VAU weiterleiten (vgl. [A_26597*]). Auch bei einer Umsetzung durch den Anbieter MUSS die konkrete technische Umsetzung vollständig im Produktgutachten beschrieben werden. [≤]

A_26599 - PoPP-Service - VAU - Isolation der VAU von Datenverarbeitungsprozessen des Anbieters

Die VAU des PoPP-Service MUSS die in ihren Verarbeitungskontexten ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Anbieters (unabhängig, ob für TI-Dienste oder andere Dienste) trennen und damit gewährleisten, dass diese Datenverarbeitungsprozesse sowie der Anbieter der VAU selbst technisch vom Zugriff auf die in den Verarbeitungskontexten verarbeiteten Daten ausgeschlossen sind. [≤]

A_26600 - PoPP-Service - VAU - Isolation zwischen Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU

Die VAU des PoPP-Service MUSS mit technischen Mitteln ausschließen, dass sich die Verarbeitungen innerhalb eines Verarbeitungskontextes schadhaf auf die Verarbeitungen eines anderen Verarbeitungskontextes auswirken können. [≤]

A_26601 - PoPP-Service - VAU - Löschen aller Daten beim Beenden des Verarbeitungskontextes

Die VAU des PoPP-Service MUSS sicherstellen, dass beim Beenden eines Verarbeitungskontextes sämtliche Daten dieses Verarbeitungskontextes aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [≤]

5.2.1.5 Anforderungen an das HSM

A_26602 - PoPP-Service - VAU - Prüfungsfunktionalität und Schlüsselmanagement im HSM

Der Anbieter eines PoPP-Service MUSS über ein HSM verfügen, welches neben der sicheren Schlüsselspeicherung und -verwaltung, folgendes umsetzt:

- eine Funktionalität zur Validierung von VAU-Images und Attestierungsinformationen zu solchen Images, wobei zwischen verschiedenen Arten von VAU-Images unterschieden werden kann (konkret PoPP-VAU-Image und ZETA Guard-Image),
- für die aus diesen Images gestarteten verschiedenen Arten von Verarbeitungskontexten (PoPP und ZT) jeweils genau nur die für diesen vorgesehenen Identitäten (Schlüssel) zur Nutzung freigeben bzw. Schlüsselerzeugung und -export ermöglichen und
- sonstige Schlüsselerzeugungen (abgesehen von etwaigen spezifizierten Ausnahmen) und den Import von Prüfschlüsseln nur im technisch abgesicherten Vier-Augen-Prinzip ermöglichen.

[≤]

Hinweis: Eine valide technische Umsetzung ist ein HSM-Modul, welches:

1. *Prüfschlüssel importieren und an bestimmte Zwecke/Anwendungsfälle binden kann,*
2. *Schlüsselpaare erzeugen und diese an bestimmte Zwecke/Anwendungsfälle bzw. an bestimmte authentifizierte Nutzer (ZETA Guard- und PoPP-Verarbeitungskontexte) des HSM binden kann,*
3. *autorisierte VAU-Images in Form von signierten Hashwerten dieser Images importieren kann und dabei die Signatur gegen zuvor importierte Prüfschlüssel prüft, bevor Hashwerte übernommen werden,*
4. *eine beidseitig authentifizierte, verschlüsselte und integritätsgeschützte Verbindung zu Verarbeitungskontexten aufbauen kann,*
5. *Attestierungsprotokolle mit Schutz vor Replay-Attacken unterstützt und somit:*
 - a. *frische Attestierungsinformationen von Verarbeitungskontexten entgegennehmen kann, deren Signatur gegen zuvor importierte Prüfschlüssel prüft,*
 - b. *die Attestierungsinformation (Hashwert) gegen die aktuell als autorisiert hinterlegten Hashwerte von VAU-Images validiert,*
 - c. *ggf. die Art von VAU-Image detektiert (falls PoPP-VAU- oder ZETA Guard-Image getrennt sind) und nur im Erfolgsfall*
 - i. *private Schlüssel zur Nutzung für genau den attestierten Verarbeitungskontext freigibt, wobei nur die für diese Art von Verarbeitungskontext zulässigen Schlüssel freigegeben (Unterscheidung PoPP-Logik und ZETA-Logik sofern verschiedene Kontexte) werden und*
 - ii. *Schlüsselpaare für den attestierten Verarbeitungskontext erzeugt und an diesen übergibt*
6. *die Anmeldung von Benutzern am HSM/HSM-Modul zur Erzeugung von Schlüsseln (abgesehen von etwaigen spezifizierten Ausnahmen) und zum Import von*

Prüfchlüsseln nur über sichere Authentisierungsmittel, die zwischen mehreren Rollen aufgeteilt werden können, ermöglicht.

5.2.1.6 Schlüsselnutzung direkt im Verarbeitungskontext

Der PoPP-Service verfügt über ein oder mehrere HSMs, welche sowohl die sichere Nutzung und Speicherung von Schlüsseln gewährleisten als auch eine performante Nutzung der Schlüssel ermöglichen. Nichtsdestotrotz ist die Nutzung von Schlüsseln im HSM weniger performant, als für Schlüssel die direkt im Verarbeitungskontext der VAU verfügbar sind. Dies liegt u.a. auch am Overhead für die sichere Kommunikation mit dem HSM, die bei jeder Nutzung eines Schlüssels im HSM anfällt.

Um Performanceprobleme beim PoPP-Service zu vermeiden soll daher die Anzahl der HSM-Zugriffe, die für die jeweiligen Anwendungsfälle notwendig sind gering gehalten werden. Da die VAU und deren Verarbeitungskontexte gerade für die Verarbeitung vertraulicher Daten konzipiert und implementiert wird, ist es sicherheitstechnisch grundsätzlich denkbar Schlüssel direkt im Verarbeitungskontext zu nutzen, statt sie im HSM zu speichern. Dabei muss der Zweck des Schlüssels und auch die Laufzeit betrachtet werden, da die Speicherung außerhalb des HSM ein leicht erhöhtes Restrisiko der Offenbarung des Schlüssel hervorruft und dessen Eintrittswahrscheinlichkeit mit der Zeit, in der der Schlüssel genutzt wird, steigt.

Entsprechend dieser Betrachtungen wird der private Schlüssel für die Signatur von PoPP-Token im HSM gespeichert und Schlüssel für TLS-Identitäten dürfen zwar außerhalb des HSM direkt vom Verarbeitungskontext der VAU verarbeitet, jedoch nicht länger drei Monate genutzt werden.

A_26687 - PoPP-Service - VAU - Schlüssel- und CSR-Erzeugung im HSM durch Verarbeitungskontext

Die VAU des PoPP-Service MUSS es dem Anbieter ermöglichen Schlüsselpaare für die folgenden Identitäten erzeugen zu können:

1. PoPP-Service-TLS-Server (Richtung PS und PoPP-Modul integrierender App sowie für eGK-Zertifikat-Hashwert-Import),
2. PoPP-Service-TLS-Client (Richtung sektorialem IDP),
3. APDU-Paket-Signatur
4. ID Token-Verschlüsselung (durch den sektoralen IDP) und
5. Access Token-Signatur (durch den PoPP AuthZ)
6. Access Token-Ver-/Entschlüsselung (durch AuthZ bzw. Resource Server)

und dabei wie folgt vorgehen:

1. Auslösen der Schlüsselerzeugung durch den Verarbeitungskontext am HSM unter Angabe des Zwecks bzw. der zu Erzeugenden Identität,
2. Export des Schlüsselpaars aus dem HSM in den Verarbeitungskontext,
3. mit dem Persistenzschlüssel verschlüsselte Ablage des Schlüsselpaars außerhalb des Verarbeitungskontext unter Angabe der zugehörigen Identität, des Zeitpunkts der Schlüsselerzeugung sowie des Status "neu" und
4. Ausgabe eines mit dem jeweiligen privaten Schlüssel signierten CSR für die TLS-Identitäten und die APDU-Paket-Signatur-Identität an den Anbieter.

[<=]

Hinweis: Für die TLS-Client-Identität (Richtung sektorialem IDP) ist ggf. kein CSR notwendig, da nicht zwingend ein Zertifikat erforderlich ist. Die Nachvollziehbarkeit, dass die genannten Schlüssel im HSM erzeugt wurden, ist entsprechend der Hinweise zur

Umsetzung für die gematik über das signierte und exportierbare Protokoll des HSM möglich. Dafür wird im Rahmen der initialen Zeremonie ein Protokoll-Signatur-Schlüsselpaar erzeugt und von der gematik der öffentliche Signaturprüf Schlüssel exportiert. In diesem Protokoll werden - neben den Hashwerten der importierten VAU-Images - die öffentlichen Schlüssel der in [A_26687*] genannten Schlüsselpaare unter Angabe des Zwecks bzw. der zugehörigen Identität protokolliert. Neu erzeugte Schlüsselpaare sind nicht automatisch aktiv, da für einige Identitäten zunächst Zertifikate durch den Anbieter bezogen werden müssen und / oder öffentliche Schlüssel in JWKSs / Entity Statements veröffentlicht werden müssen, bevor die Identität einsatzbereit ist und aktiviert werden kann.

A_27038 - PoPP-Service - VAU - Aktivierung außerhalb des HSMs gespeicherter Schlüssel

Die VAU des PoPP-Service MUSS es dem Anbieter ermöglichen,

1. für über den Verarbeitungskontext im HSM erzeugte und exportierte Identitäten (neue Schlüsselpaare) Zertifikate zu importieren sowie
2. die neuen Schlüsselpaare für die Nutzung zu aktivieren (Status "neu" > "aktiv")

und der PoPP-Service MUSS dabei

1. Zertifikate ausschließlich dann übernehmen, wenn diese zum für die jeweilige Identität vorhandenen neuen Schlüsselpaar passen,
2. etwaige für die Identität bereits vorhandene Schlüsselpaare deaktivieren (Status "aktiv" > "inaktiv")
3. fortan das neue Schlüsselpaar für die jeweilige Identität verwenden.

[<=]

Hinweis: Es ist aktuell nicht vorgesehen einmal deaktivierte Schlüssel reaktivieren zu können (Status "inaktiv" > "aktiv").

A_27039 - PoPP-Service - VAU - Nutzung außerhalb des HSMs gespeicherter Schlüssel

Die VAU des PoPP-Service MUSS beim Start eines Verarbeitungskontext prüfen,

1. ob mit dem Persistenzschlüssel geschützte Identitäten (Schlüsselpaare) verfügbar sind,
2. ob diese als aktiv gekennzeichnet sind und
3. ob im Falle der Identitäten für TLS, Access Token-Signatur, Access Token-Verschlüsselung und ID Token-Verschlüsselung diese nicht älter als drei Monate sind

und nur im Positivfall diese Identitäten verwenden.[<=]

5.2.1.7 Speicherung von Daten

A_26603 - PoPP-Service - VAU - Verschlüsselung von Daten vor Speicherung außerhalb des Verarbeitungskontextes

Die VAU des PoPP-Service MUSS sicherstellen, dass schützenswerte Daten, insbesondere auch Schlüssel, die außerhalb eines Verarbeitungskontextes gespeichert werden sollen, ausschließlich mit einem Persistenzschlüssel verschlüsselt aus dem Verarbeitungskontext in Speichersysteme ausgeleitet werden und die Verschlüsselung einen Integritätsschutz inkludiert.[<=]

A_26604 - PoPP-Service - VAU - Ableitung Persistenzschlüssel durch ein HSM

Die VAU des PoPP-Service MUSS sicherstellen, dass der Verarbeitungskontext Persistenzschlüssel von im HSM gespeicherten Master-Schlüsseln im HSM ableitet.[<=]

A_26605 - PoPP-Service - VAU - Nutzung Persistenzschlüssel ausschließlich im Verarbeitungskontext

Die VAU des PoPP-Service MUSS sicherstellen, dass Persistenzschlüssel ausschließlich in einem Verarbeitungskontext genutzt werden. [≤]

5.2.1.8 Transport von Daten und Authentisierung/Authentifizierung bei Kommunikation

A_26606 - PoPP-Service - VAU - Sicherer VAU-Kanal vom Kommunikationspartner in den Verarbeitungskontext

Die VAU des PoPP-Service MUSS sicherstellen, dass schützenswerte Daten zwischen dem PoPP-Service und einem VAU-Client oder dem PoPP-Service und dem sektoralen IDP ausschließlich über einen TLS-Kanal übermittelt werden, der in einem Verarbeitungskontext der VAU des PoPP-Service terminiert. [≤]

Hinweis: Für PoPP wird der VAU-Kanal somit durch TLS realisiert. Der von VAU-Clients etablierte TLS-Kanal endet im PEP des ZETA Guard, der in einem Verarbeitungskontext läuft. Der TLS-Kanal zum sektoralen IDP wird aus einem Verarbeitungskontext des PoPP-Service aufgebaut.

A_26607 - PoPP-Service - VAU - Authentisierung gegenüber VAU-Clients

Die VAU des PoPP-Service MUSS sicherstellen, dass der Verarbeitungskontext sich gegenüber VAU-Clients mittels der PoPP-Service-spezifischen TLS-Server-Identität ausweist, deren privater Schlüssel nur im Verarbeitungskontext genutzt werden kann und außerhalb für den Verarbeitungskontext verschlüsselt gespeichert ist, so dass auf den Schlüssel nur attestierte Verarbeitungskontexte Zugriff haben. [≤]

Hinweis: Vorgaben zum TLS-Zertifikat werden in [A_26497] definiert.*

A_26608 - PoPP-Service - VAU - Authentisierung gegenüber sektorialem IDP

Die VAU des PoPP-Service MUSS für die Client-Authentisierung im TLS-Handshake mit dem sektoralen IDP eine TLS-Client-Identität verwenden, deren privater Schlüssel nur im Verarbeitungskontext nutzbar ist und außerhalb für den Verarbeitungskontext verschlüsselt gespeichert ist, so dass auf den Schlüssel nur attestierte Verarbeitungskontexte Zugriff haben. [≤]

Hinweis: Weitere Vorgaben zur TLS-Client-Authentisierung von Relying Parties ggü. dem sektoralen IDP werden in [gemSpec_IDP_FD#A_23183, A_23185*, A_23196*] getroffen.*

A_26609 - PoPP-Service - VAU - Sichere Kommunikation zwischen Komponenten

Die VAU des PoPP-Service MUSS sicherstellen, dass alle Komponenten der VAU ausschließlich transportverschlüsselt, integritätsgeschützt und beidseitig authentisiert mit anderen Komponenten (außerhalb oder innerhalb) der VAU kommunizieren, einschließlich der Kommunikation zwischen dem ZETA Guard- und den PoPP-Verarbeitungskontexten (sofern diese nicht in einem gemeinsamen Verarbeitungskontext laufen) und der Kommunikation zum HSM. Die Verbindung müssen auch gegen Zugriffe durch den Anbieter geschützt sein. [≤]

A_26610 - PoPP-Service - VAU - Identitäten zur Authentisierung für Kommunikation zwischen Verarbeitungskontexten

Die VAU des PoPP-Service MUSS sicherstellen, dass - sofern eigene VAU-Images und somit auch Verarbeitungskontexte für PoPP-Fachlogik und ZETA Guard verwendet werden - für die Kommunikation zwischen den Verarbeitungskontexten beide Kontexte eine Identität verwenden, deren privater Schlüssel im HSM gespeichert ist und auf den der jeweilige Kontext ausschließlich nach Attestierung, dass der Kontext integer aus einem autorisierten Image gestartet wurde, im HSM zugegriffen werden kann. [≤]

A_26611 - PoPP-Service - VAU - Sichere Verbindung zwischen bekannten VAU-Image und HSM

Die VAU des PoPP-Service MUSS technisch sicherstellen, dass:

1. Zwischen einem Verarbeitungskontext der VAU und dem HSM eine beidseitige authentifizierte, integritätsgeschützte und vertrauliche Verbindung besteht.
2. sich ausschließlich Verarbeitungskontexte mit dem HSM verbinden können, die Instanz eines VAU-Images sind, welches dem HSM bekannt gemacht wurde und
3. die Verarbeitungskontexte auch das HSM authentifizieren können.

[<=]

Hinweis: Eine technische Umsetzung des Aspekts "Verarbeitungskontext ist Instanz eines bekannten VAU-Images" ist die Bekanntmachung des vom Dienst-Hersteller signierten Hashwerts eines VAU-Images ggü. dem HSM. Das HSM kann die Signatur gegen Prüfschlüssel verifizieren, die über sichere Prozesse ins HSM eingebracht wurden. Im Zuge des Zugriffs eines Verarbeitungskontext auf das HSM lässt dieses den Verarbeitungskontext von der VAU attestieren und kann die wiederum signierten Attestierungsinformationen (Quote) gegen den ebenfalls vorab eingebrachten Prüfschlüssel verifizieren. Die Attestierung muss Übergabe und Prüfung einer Challenge umfassen, um Replay-Attacken auszuschließen.

5.2.1.9 Protokollierung und Monitoring

A_26612 - PoPP-Service - VAU - Datenschutzkonformes Logging und Monitoring des Verarbeitungskontextes der VAU

Die VAU des PoPP-Service MUSS die für den Betrieb des PoPP-Service erforderlichen Logging- und Monitoring-Informationen in solcher Art und Weise erheben und verarbeiten, dass mit technischen Mitteln ausgeschlossen ist, dass dadurch Identitätsdaten von Versicherten und LEI offenbart werden.[<=]

A_26613 - PoPP-Service - VAU - Protokollierung VAU-Image-Hashwerte und öffentliche Schlüssel im HSM

Das HSM des PoPP-Service MUSS:

1. alle ihm bekanntgemachten VAU-Images (Hashwerte)
2. die öffentlichen Schlüssel von erzeugten:
 - a. PoPP-Token-Signatur-Identitäten,
 - b. APDU-Paket-Signatur-Identitäten,
 - c. ID Token-Verschlüsselungs-Identitäten,
 - d. Access Token-Signatur-Identitäten,
 - e. Access Token-Verschlüsselungs-Identitäten,
 - f. PoPP-Service-TLS-Server-Identitäten (Richtung PS und PoPP-Modul integrierender App sowie eGK-Zertifikats-Hash-Import) und
 - g. PoPP-Service-TLS-Client-Identitäten (Richtung sektorialem IDP)

zusammen mit dem jeweiligen Zweck / Identitätsbezeichnung und dem Zeitpunkt des Imports bzw. der Erzeugung so integritätsgeschützt protokollieren, dass Dritte den Integritätsschutz außerhalb des HSM prüfen können. Die jeweiligen Information MÜSSEN für mindestens drei Jahre im Protokoll vorgehalten werden.[<=]

Hinweis: Eine technische Umsetzung ist die Signatur des Protokolls mit einem Protokoll-Signatur-Schlüssel, der über sichere Prozesse im Rahmen der Inbetriebnahme im HSM erzeugt wurde, ausschließlich vom HSM selbst genutzt werden kann und dessen öffentlicher Schlüssel der gematik bekannt ist.

A_26614 - PoPP-Service - VAU - Exportierbarkeit Protokoll für VAU-Image-Hashwerte und öffentliche Schlüssel aus HSM

Das HSM des PoPP-Service MUSS das integritätsgeschützte Protokoll der ihm bekanntgemachten VAU-Images und der öffentlichen Schlüssel der im HSM erzeugten Identitäten exportieren können, damit Dritte prüfen können, dass ausschließlich autorisierte VAU-Images dem HSM bekanntgemacht wurden und welche öffentlichen Schlüssel in Entity Statements und Zertifikaten aufgeführt sein müssen. [≤]

5.2.1.10 Konfigurierbarkeit

A_26615 - PoPP-Service - VAU - Einspielen von VAU-Images durch den Anbieter

Die VAU des PoPP-Service MUSS es dem Anbieter ermöglichen die vom Hersteller übermittelten VAU-Images eigenständig einzuspielen. [≤]

Hinweis: VAU-Images werden entsprechend der Hinweise zur Umsetzung nur nach erfolgreicher Prüfung der Signatur übernommen und werden nur ausgeführt bzw. können nur auf die relevanten Schlüssel zugreifen, wenn diese vom HSM über entsprechende Attestierungsinformationen der VAU als autorisierte Images verifiziert werden. Die dafür notwendigen Hashwerte von Images kann der Anbieter ebenfalls eigenständig ins HSM importieren und auch diese werden nur übernommen, wenn sie vom Hersteller signiert wurden.

5.2.1.11 Anforderungen an den Hersteller

A_26960 - PoPP-Service - VAU - Hersteller - Sicheres Einbringen Fachdienst-VAU-Verschlüsselungszertifikate

Der Hersteller des PoPP-Service MUSS die aktuellen, hinsichtlich Integrität und Gültigkeit geprüften Fachdienst-VAU-Verschlüsselungszertifikate (für Verschlüsselung VSDM-PN-HMAC-Schlüssel) im 4-Augen-Prinzip in das VAU-Image einbringen. [≤]

Hinweis: Vergleich Absatz [Kapitel Ersatz-Prüfungsnachweis (VSDM-PN)] und dort [A_26959].*

Offener Punkt: Die geplanten Änderungen beim VSDM+-Prüfungsnachweis (C_12143 im Draft_ePAfueralle_3_0_3-1) wirken sich auf den Ersatz-Prüfungsnachweis (VSDM-PN) aus und sind hier noch nicht enthalten.

A_27153 - PoPP-Service - VAU - Hersteller - Sicheres Einbringen Signaturzertifikate von Kassen-Dienstleistern

Der Hersteller des PoPP-Service MUSS die von der gematik erhaltenen öffentlichen Signaturzertifikate der Kassen bzw. ihrer Dienstleister als *listSignatureVerificationKeys* in das VAU-Image einbringen. [≤]

Hinweis: Vergleich Absatz [Kapitel eGK-Hash-Datenbank].

Bei der Verwendung von Attestierungsmechanismen der Chip-Plattform wird entsprechend Schlüsselmaterial verwendet, was von den Herstellern der Chips (also bspw. Intel oder AMD) sicher erzeugt und sicher in die Plattform eingebracht wird. Der Hersteller des PoPP-Service hat darauf keinen Einfluss, muss aber dann entsprechend diese Mechanismen sicher verwenden.

Verwendet der Hersteller des PoPP-Service andere Mechanismen muss er selber Schlüsselmaterial, was im Zuge der Attestierung verwendet wird (Attestierungsschlüssel), erzeugen und speichern. Die in den folgenden Anforderungen gemachten Vorgaben bzgl. Attestierungs-Schlüsseln beziehen sich auf dieses Szenario.

A_26617 - PoPP-Service - VAU - Hersteller - Schlüsselqualität Attestierungs- und Autorisierungs-Schlüssel

Der Hersteller des PoPP-Service MUSS

- Schlüssel, die für die Signatur von Attestierungsinformationen (Attestierungs-Schlüssel) - sofern er diese selber erzeugt - und
- Schlüssel, die zur Autorisierung (Signatur) von VAU-Images verwendet werden, entsprechend der Vorgaben aus [gemSpec_Krypt#GS-A_4368] erzeugen. Dies gilt sowohl für die Schlüssel die direkt für Signaturen von Attestierungsinformationen und VAU-Images verwendet werden als auch für Schlüsselmaterial, dass diese Schlüssel bestätigt (CA-Schlüssel). [\leq]

A_26618 - PoPP-Service - VAU - Hersteller - Einbringen und Speichern von Attestierungs-Schlüsseln in VAU

Der Hersteller des PoPP-Service MUSS Schlüssel, die für die Signatur von Attestierungsinformationen von VAU-Images verwendet werden (Attestierungs-Schlüssel), sofern er diese selber erzeugt und verwaltet, im 4-Augen-Prinzip zusammen mit der gematik in die Systeme der VAU einbringen und dort vor Auslesen geschützt speichern. [\leq]

A_26619 - PoPP-Service - VAU - Hersteller - Speichern von Autorisierungs- und CA-Schlüsseln

Der Hersteller des PoPP-Service MUSS

- Schlüssel, die für die Autorisierung (Signatur) von VAU-Images verwendet werden,
- Schlüssel, die Attestierungs-Schlüssel bestätigen (CA-Schlüssel), sofern er diese selber verwaltet,
- Schlüssel, die Autorisierungs-Schlüssel bestätigen (CA-Schlüssel),

vor Auslesen und unberechtigten Zugriffen geschützt speichern, sodass diese nur im 4-Augen-Prinzip verwendet werden können. [\leq]

A_26620 - PoPP-Service - VAU - Hersteller - Bereitstellung Prüfschlüssel für Attestierung und Autorisierung

Der Hersteller des PoPP-Service MUSS die zur Prüfung von VAU-Image-Attestierungsinformationen und VAU-Image-Autorisierungen (Signaturen) benötigten Prüfschlüssel (bspw. öffentlicher CA-Schlüssel) zur HSM-Einrichtung beim Anbieter mitbringen und vorab der gematik und dem Anbieter bereitstellen. [\leq]

Hinweis: Die Bereitstellung von Attestierungs-Prüfschlüsseln an die gematik erfolgt für den Fall, dass der Hersteller diese selbst verwaltet, beim Hersteller vor Ort im Rahmen der gemeinsamen Einbringung der Attestierungs-Schlüssel in die VAU (vgl. A_26618).*

A_26621 - PoPP-Service - VAU - Hersteller - Kryptographische Autorisierung von VAU-Images

Der Hersteller des PoPP-Service MUSS von ihm erstellte VAU-Images im 4-Augenprinzip mit dem Autorisierungsschlüssel kryptographisch autorisieren (signieren). [\leq]

Hinweis: Eine technische Umsetzung ist die Erzeugung des Hashwerts des VAU-Images und die Signatur mit dem privaten Autorisierungsschlüssel.

A_26622 - PoPP-Service - VAU - Hersteller - Übermittlung autorisierter VAU-Images an Anbieter und gematik

Der Hersteller des PoPP-Service MUSS von ihm erstellte und autorisierte VAU-Images an den Anbieter übermitteln und der gematik mindestens die Autorisierungsinformation bereitstellen. [\leq]

Hinweis: Eine technische Umsetzung der Bereitstellung an die gematik ist die Übermittlung des signierten Hashwerts an die gematik.

A_26692 - PoPP-Service - VAU - Hersteller - Protokollierung sicherheitsrelevanter Hersteller-Aktivitäten

Der Hersteller des PoPP-Service MUSS alle Aktivitäten, die den Schutz der Integrität von VAU-Images und die Nachvollziehbarkeit des Rollouts von VAU-Images betreffen, protokollieren und dabei festhalten wann, warum, durch wen, welche Aktion durchgeführt wurde. Dies umfasst mindestens Schlüsselerzeugungen, Prüfschlüssel-Importe, VAU-Image-Erzeugung, VAU-Image-Signatur und VAU-Image-Auslieferung. Das Protokoll ist der gematik auf Nachfrage vorzulegen.【<=】

5.2.1.12 Anforderungen an den Anbieter

A_26623 - PoPP-Service - VAU - Gemeinsame Zeremonie zur HSM-Einrichtung

Der Anbieter des PoPP-Service MUSS eine Zeremonie organisieren und durchführen, bei der gemeinsam mit dem Hersteller und der gematik die Einrichtung des HSM vorgenommen wird.【<=】

Hinweis: Eine Zeremonie, die die folgenden Punkte berücksichtigt, setzt die Anforderung um:

1. *Das HSM befindet sich im Auslieferungszustand.*
2. *Auf dem HSM wird das HSM-Modul des Herstellers des PoPP-Service installiert.*
3. *Der Zugang zum HSM wird so konfiguriert, dass der Anbieter:*
 - a. *neue signierte Hashwerte von VAU-Images ins HSM importieren kann,*
 - b. *Schlüssel für TLS-Server- und TLS-Client-Identität erzeugen und dazugehörige CSRs exportieren kann,*
 - c. *Schlüssel für die ID Token-Verschlüsselung (durch den sektoralen IDP) erzeugen kann,*
 - d. *Schlüssel für die Access Token-Signatur (durch PoPP AuthZ) erzeugen kann,*
 - e. *Schlüssel für die Access Token-Ver-/Entschlüsselung (durch AuthZ bzw. Resource Server) erzeugen kann,*
 - f. *darüber hinaus keine anderen Schlüssel erzeugen, exportieren oder nutzen sowie keine Prüfschlüssel importieren kann, sondern dies nur im Vier-Augen-Prinzip mit der gematik möglich ist.
(Der Export öffentlicher Schlüssel kann und muss immer möglich sein.)*
4. *Auf dem HSM werden Schlüssel für die folgenden Identitäten bzw. Zwecke erzeugt:*
 - a. *Identität PoPP-Token-Signatur,*
 - b. *CA-Schlüsselpaar zur Ableitung von Identitäts-Schlüsselpaaren ("CA-Ident."),*
 - c. *Identität HSM für Verarbeitungskontext-zu-HSM-Kommunikation (aus CA-Ident.),*
 - d. *Identität PoPP-Verarbeitungskontext (aus CA-Ident.),*
 - e. *Identität ZETA Guard-Verarbeitungskontext (aus CA-Ident.),*
 - f. *Protokoll-Signatur-Schlüssel (Signatur des Protokolls der VAU-Image-Hashwerte und öffentlichen Schlüssel von im HSM erzeugten Identitäten).*
5. *Aus dem HSM werden die öffentlichen Schlüssel für PoPP-Token-Signatur, CA-Ident. und Protokoll-Signatur exportiert.*
6. *Der öffentliche Schlüssel für die PoPP-Token-Signatur-Identität geht:*

- a. an den Anbieter zur Bekanntmachung via Entity Statement und zur Beantragung der TI-Identität (der Export eines mit dem privaten Schlüssel signierten CSR muss möglich sein) und
 - b. an die gematik, um diesen später gegen den im Entity Statement und im TI-Zertifikat enthaltenen Schlüssel abgleichen zu können.
7. Der öffentliche Schlüssel der CA-Ident. geht an den Hersteller, der diese über die VAU-Image-Build-Pipeline [A_26468*] in die VAU-Images einbindet.
 8. Der öffentliche Protokoll-Signatur-Schlüssel geht an die gematik zur späteren Prüfung der vom Anbieter übertragenen Protokolle.
 9. In das HSM werden die folgenden Prüfschlüssel - gebunden an den jeweiligen Zweck - importiert, nachdem sie vorab zwischen Hersteller, Anbieter und gematik nochmals abgeglichen wurden:
 - a. Prüfschlüssel zur Signatur der Attestierungsinformationen (vom Hersteller; geht bei Eigenverwaltung dieser Schlüssel durch den Hersteller in einer vorgelagerten Zeremonie - zur Einbringung der Attestierungs-Schlüssel in die VAU - an die gematik),
 - b. Prüfschlüssel zur Signatur von VAU-Image-Hashwerten (vom Hersteller).

A_26968 - PoPP-Service - VAU - Prozess für Vertrauensanker-Management

Der Anbieter des PoPP-Service MUSS einen Prozess entwerfen und umsetzen, der das Wechseln oder Hinzufügen von in das HSM importierten Vertrauensankern, sowie das Erneuern von im HSM erzeugten Vertrauensankern zusammen mit dem Hersteller des PoPP-Service und der gematik ermöglicht und diesen so anstoßen, dass mindestens eine Erneuerung von im HSM erzeugten Vertrauensankern erfolgt, bevor die Laufzeit der aktuellen Anker zwei Jahre überschreitet.【<=】

Hinweis: Da von den in das HSM importierten Vertrauensanker ggf. nicht alle unter der Kontrolle des Herstellers des PoPP-Service stehen, ist ein Wechsel oder Hinzufügen eines Vertrauensankers bereits deutlich vor Ablauf von zwei Jahren nicht auszuschließen.

A_26624 - PoPP-Service - VAU - Sichere Erzeugung und Speicherung privater und geheimer Schlüssel der VAU

Der Anbieter des PoPP-Service MUSS alle privaten und geheimen Schlüssel, die für den Betrieb des Dienstes und der VAU benötigt werden, in einem HSM erzeugen und im HSM oder innerhalb eines Verarbeitungskontext anwenden, bspw. private bzw. geheime Schlüssel, die:

1. zur Authentisierung der Verarbeitungskontexte gegenüber von VAU-Clients und Diensten,
2. zur Ver- und Entschlüsselung oder
3. zur Signatur

genutzt werden.【<=】

Hinweis: Der Schutz der Schlüssel wird entsprechend der Anforderungslage technisch vom Produkt durchgesetzt. Schlüssel werden entweder innerhalb der initialen Zeremonie gemeinsam mit Hersteller und gematik erzeugt oder deren Erzeugung wird vom Anbieter über entsprechende Schnittstellen der VAU ausgelöst. Ausnahmen bilden die Signaturschlüssel für Attestierungsinformationen die in der Hardware der VAU (bspw. TPM) sicher gespeichert sind. Der Anbieter erzeugt nicht selber Schlüssel. Explizit davon ausgenommen und hier in den Anforderungen nicht erwähnt sind die Schlüssel zum Signieren des Entity Statements des PoPP-Service. Diese können unter der Hoheit des Anbieters stehen. Die gematik ist über die Zeremonie zur HSM-Einrichtung und über das

vom HSM signierte Protokoll jederzeit in der Lage, die Authentizität der in Entity Statements und Zertifikaten veröffentlichten Schlüssel zu verifizieren.

A_27041 - PoPP-Service - VAU - Prozesse zur Regelmäßigen Erneuerung von Schlüsseln und Zertifikaten

Der Anbieter des PoPP-Service MUSS einen Prozess entwerfen und umsetzen, der gewährleistet, dass

1. die im Verarbeitungskontext der VAU verarbeiteten Schlüssel der Identitäten für TLS, Access Token-Signatur, Access Token-Verschlüsselung und ID Token-Verschlüsselung und die dafür ggf. notwendigen Zertifikate rechtzeitig vor dem Ablauf ihrer dreimonatigen Laufzeit erneuert werden,
2. die Schlüssel und Zertifikate für die Identitäten zur PoPP-Token-Signatur und APDU-Paket-Signatur rechtzeitig vor dem Ablauf von zwei Jahren (vgl. A_26968*) Laufzeit erneuert werden und
3. die notwendigen Veröffentlichungen der öffentlichen Schlüssel und Zertifikate in JWKs und Entity Statements erfolgt.

[<=]

Hinweis: Entsprechend [A_27039] wird die maximale Laufzeit der im ersten Punkt genannten Schlüssel technisch von der VAU durchgesetzt. Entsprechend den Vorgaben der TI-PKI ist die Laufzeit fünf Jahre für die im zweiten Punkt genannten Zertifikate, wobei die Schlüssel abweichend davon nur zwei Jahre genutzt werden sollen. Für die Erneuerung der PoPP-Token-Signatur-Identität ist ein Mehraugenprinzip mit der gematik notwendig. Vergleiche dazu auch [A_26968*] weiter oben.*

A_26625 - PoPP-Service - VAU - Eingeschränkte HSM Administration

Der Anbieter des PoPP-Service MUSS sicherstellen, dass der Zugriff auf das HSM so eingeschränkt ist, dass nur im Vier-Augen-Prinzip mit der gematik folgende Aktionen möglich sind:

1. Die Erstellung, Sicherung und Wiederherstellung von Schlüsseln,
2. der Import von Prüfschlüssel in das HSM und
3. die Administration des HSM.

[<=]

Hinweis: Die Einrichtung des HSM findet innerhalb der initialen Zeremonie mit der gematik statt. Durch die beschriebene Umsetzung, bei der neue VAU-Images über den Import von signierten Hashwerten der Images im HSM bekannt gemacht werden, ergibt sich keine Abhängigkeit des Anbieters zur gematik im Regelbetrieb, da dieser Import durch den Anbieter eigenständig vorgenommen werden kann.

A_26626 - PoPP-Service - VAU - Einsatz zertifizierter HSM

Der Anbieter des PoPP-Service MUSS HSMs verwenden, deren Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common Criteria oder Federal Information Processing Standard (FIPS) in Frage. Die Prüftiefe MUSS mindestens:

1. FIPS 140-2/140-3 Level 3 oder
2. Common Criteria EAL 4+ mit hohem Angriffspotenzial

entsprechen. **[<=]**

A_26627 - PoPP-Service - VAU - Ausschluss von Manipulationen über physische Angriffe

Der Anbieter des PoPP-Service MUSS mit zusätzlichen organisatorischen Mitteln ausschließen, dass ein Angreifer aus dem betrieblichen Umfeld des Anbieters physische Angriffsmittel zur Kompromittierung der VAU zum Einsatz bringen kann. [≤]

Hinweis: Die Anforderung besteht für den Anbieter zusätzlich zum in [A_26598] geforderten Schutz.*

A_26628 - PoPP-Service - VAU - Physischer Zugriff auf Systeme der VAU nur im 4-Augen-Prinzip

Der Anbieter des PoPP-Service MUSS gewährleisten, dass physischer Zugriff auf die Hardware der VAU nur im 4-Augen-Prinzip möglich ist. [≤]

Hinweis: Die Anforderung besteht für den Anbieter zusätzlich zum in [A_26598] und [A_26597*] geforderten Schutz.*

5.2.1.13 Bereitstellung durch die gematik

Die gematik stellt den ZETA Guard als Docker-Container-Image und eine dazugehörige Signatur bereit.

Die gematik stellt den Prüfschlüssel für die Prüfung der Signatur des ZETA Guard bereit.

5.3 Identitäten und Zertifikate PoPP-Service

5.3.1 Überblick

Die folgende Tabelle gibt einen Überblick über die verwendeten Schlüssel, wo sie erzeugt werden und wo der private bzw. geheime Schlüssel gespeichert und verwendet wird. Öffentliche Schlüssel die als Prüfschlüssel/Vertrauensanker dienen, sind nicht mit aufgeführt. (VK = Verarbeitungskontext)

Tabelle 6: Übersicht über die im PoPP-Service verwendeten Schlüssel

Schlüssel/Zertifikat & Zweck	Erzeugung	Speicherung	Verwendung im	Verwendung durch
TLS-Server (Richtung PS & PoPP-Modul integrierender App)	HSM der VAU	für VK verschlüsselt	VK ZETA & PoPP	VK ZETA & PoPP
TLS-Client (Richtung sektoraler IDP)	HSM der VAU	für VK verschlüsselt	VK PoPP	VK PoPP
PoPP-Token-Signatur	HSM der VAU	HSM der VAU	HSM der VAU	VK PoPP
APDU-Paket-Signatur	HSM der VAU	für VK verschlüsselt	VK PoPP	VK PoPP
VSDM-PN-HMAC-Schlüssel	VK PoPP	für VK verschlüsselt	VK PoPP	VK PoPP
Access Token-Signatur	HSM der VAU	für VK verschlüsselt	VK ZETA & PoPP	VK ZETA & PoPP

ID Token-Verschlüsselung	HSM der VAU	für VK verschlüsselt	VK ZETA & PoPP	VK ZETA & PoPP
Access Token-Verschlüsselung	HSM der VAU	für VK verschlüsselt	VK ZETA & PoPP	VK ZETA & PoPP
Entity Statement-Signatur	Anbieter-spezifisch	Anbieter-spezifisch	Anbieter-spezifisch	Anbieter-spezifisch
CV-Zertifikat	Hersteller-spezifisch	VAU-Image	VK PoPP	VK PoPP
HSM-Identität	HSM der VAU	HSM der VAU	HSM der VAU	HSM der VAU
PoPP-VK-Identität*	HSM der VAU	HSM der VAU	HSM der VAU	VK PoPP
ZETA-VK-Identität*	HSM der VAU	HSM der VAU	HSM der VAU	VK ZETA
HSM-Protokoll-Signatur	HSM der VAU	HSM der VAU	HSM der VAU	HSM der VAU

*sofern getrennte VAU-Images und somit VK verwendet werden

5.3.2 Algorithmus für Schlüsselpaare

A_26498 - PoPP-Service - Schlüsselpaare und X.509-Zertifikate immer auf Basis P-256

Der PoPP-Service, der Hersteller PoPP-Service und der Anbieter PoPP-Service MÜSSEN durchsetzen, dass die für die kryptographischen Operationen und Identitäten im Betrieb des PoPP-Service notwendigen asymmetrischen Schlüsselpaare sowie etwaige dafür erzeugte X.509-Zertifikate (Zertifikatssignaturschlüssel) alle auf der NIST Kurve P-256 basieren, siehe [SP800-186#3.2.1.3].[<=]

A_26954 - PoPP-Service - Schlüsselpaare für CV-Zertifikate immer auf Basis von Brainpool

Der PoPP-Service, der Hersteller PoPP-Service und der Anbieter PoPP-Service MÜSSEN durchsetzen, dass die für die kryptographischen Operationen und Identitäten im Betrieb des PoPP-Service notwendigen asymmetrischen Schlüsselpaare für CV-Zertifikate sowie die dafür erzeugten CV-Zertifikate (Zertifikatssignaturschlüssel) alle auf der folgenden Kurve aus [RFC5639] basieren: brainpoolP256r1.[<=]

5.3.3 Entity Statement

A_26828 - PoPP-Service - Sichere Erzeugung und Speicherung Entity Statement-Signaturschlüssel

Der Anbieter des PoPP-Service MUSS das Schlüsselpaar für die Signatur seines Entity Statements sicher erzeugen und so vor unberechtigtem Zugriff geschützt speichern, dass auch ein potentieller einzelner Innentäter den Signaturschlüssel nicht verwenden kann. [<=]

5.3.4 Token-Signaturen

A_26495 - PoPP-Service - PoPP-Token-Signatur-Identität

Der Anbieter des PoPP-Service MUSS für das Signaturschlüsselpaar für PoPP-Token ein Zertifikat mit dem Profil C.ZD.SIG und der Rolle OID 1.2.276.0.76.4.320 (oid_popp-token) aus der auf der NIST-P-256-Kurve basierenden TI-Komponenten-CA, welche aus der gematik-X.509-Root-CA abgeleitet ist, beziehen und dem Hersteller des PoPP-Service zur Verfügung stellen. [\leq]

Hinweis: Für den Token-Signatur-Schlüssel wird zusätzlich zur Veröffentlichung via Entity Statement/JWKS (siehe [A_26434] und [A_26533*]) ein Zertifikat mit entsprechender Rolle aus der Komponenten-PKI der TI ausgestellt und in die PoPP-Token eingebettet. Somit können FD entscheiden, ob sie die Token über den vom Federation Master oder den von der TI-PKI aufgespannten Vertrauensraum prüfen. Der Hersteller benötigt das Zertifikat um das Einbetten dieses Zertifikats in die PoPP-Token umsetzen zu können.*

A_26496 - PoPP-Service - APDU-Paket-Signatur-Zertifikat

Der Anbieter des PoPP-Service MUSS für das Signaturschlüsselpaar für APDU-Pakete ein Zertifikat mit Profil C.ZD.SIG und Rolle OID 1.2.276.0.76.4.293 (oid_popp) aus der auf der NIST-P-256-Kurve basierenden TI-Komponenten-CA beziehen und in den PoPP-Service importieren. [\leq]

Hinweis: Der Hersteller benötigt die Information zum Signaturzertifikat um die Erzeugung des Requests für die im Folgenden geforderte OCSP-Abfrage umsetzen zu können.

A_26631 - PoPP-Service - APDU-Paket-Signatur - Einbetten OCSP-Response

Der PoPP-Service MUSS in die Signatur von APDU-Paketen eine OCSP-Response für das verwendete Signaturzertifikat einbetten, die nicht älter als 23 h ist. [\leq]

Hinweis: Die Grace-Period für OCSP-Antworten im Konnektor ab PTV6 beträgt 24h. Der OCSP-Responder ist im Internet erreichbar. Die Adresse des OCSP-Responders ist dem Authority Information Access (AIA) des Zertifikats zu entnehmen.

5.3.5 TLS

A_26497 - PoPP-Service - TLS-Server-Zertifikat an Client-Schnittstelle

Der Anbieter des PoPP-Service MUSS sicherstellen, dass für die Authentisierung als TLS-Server an allen seinen Client-Schnittstellen ein TLS-Zertifikat eines Herausgebers gemäß [CAB Forum] verwendet wird, das für die Domäne ausgestellt ist, die zur Verbindung in den Verarbeitungskontext der VAU vorgesehen ist und eine Laufzeit von maximal drei Monaten aufweist. [\leq]

A_26616 - PoPP-Service - TLS-Server-Zertifikate - Certificate Transparency

Der Anbieter des PoPP-Service MUSS

1. das TLS-Zertifikat für seine Clientschnittstelle aus einer CA beziehen, welche Certificate Transparency gemäß [RFC 6962] / [RFC 9162] unterstützt,
2. täglich sicherstellen, dass für die Domäne, die zur Verbindung in den Verarbeitungskontext der VAU vorgesehen ist, keine unbekannten Zertifikate im Certificate Transparency Log gelistet werden und
3. im Fehlerfall (es wird ein unbekanntes Zertifikat gelistet) einen Security Incident entsprechend den Vorgaben zur betrieblichen Sicherheit aus [gemSpec_DS_Anbieter] erstellen.

[\leq]

A_26827 - PoPP-Service - TLS-Server-Zertifikate - Certification Authority Authorization (CAA) Records

Der Anbieter des PoPP-Service MUSS für das TLS-Zertifikat für seine Clientschnittstelle Certification Authority Authorization (CAA) DNS Resource Records nach [RFC 6844] bereitstellen, welche die Validität der ausstellenden CA verifizieren. [\leq]

Hinweis: Anforderungen zu Schlüsseln/Zertifikaten bei der TLS-Client-Authentisierung bei der Verbindung zum sektoralen IDP finden sich in gemSpec_IDP_FD, wobei der PoPP-Service die dort genannte Rolle Authorization Server/Anbieter von FD einnimmt.

A_26975 - PoPP-Service - OCSP-Stapling an Client-Schnittstelle

Der PoPP-Service MUSS an der HTTPS-Schnittstelle zum Internet für Clients (PoPP-Modul integrierende Apps und PS) OCSP-Stapling [RFC 6066] unterstützen und dabei OCSP-Responses verwenden, die nicht älter als eine Stunde sind. [\leq]

Hinweis: Die OCSP-Adresse ist im "Authority Information Access" (AIA) des Zertifikats zu finden.

5.3.6 CV-Zertifikat

Für die Verifikation der Versichertenidentität via kontaktbehaftet angebundener eGK benötigt der PoPP-Service ein CV-Zertifikat aus der TI-CVC-PKI.

A_26499 - PoPP-Service - CV-Identität für eGK-Kommunikation

Der Hersteller des PoPP-Service MUSS für die Durchführung der Card-to-Card-Authentisierung mit einer eGK ein entsprechendes Schlüsselpaar nach den Vorgaben für CV-Zertifikate in gemSpec_Krypt erzeugen und dafür ein CV-Zertifikat beziehen, dass:

1. aus der TI-CVC-PKI abgeleitet ist,
2. eine Flaglist besitzt, die ausschließlich Nullen enthält, und
3. als CHR (12 Byte Wert) einen Zähler verwendet, der mit jedem für den PoPP-Service ausgestellten CV-Zertifikat inkrementiert wird, beginnend mit '0000 80 987 00000 00000000001'.
4. einen öffentlichen Schlüssel auf der Kurve gemäß [RFC 5639] brainpoolP256r1 enthält und das CV-Zertifikat und den privaten Schlüssel in das VAU-Image des PoPP-Service einbringen.

[\leq]

Hinweis: Die erste CHR ist in A_26499 mit '0000 80 987 00000 00000000001' spezifiziert. Diese CHR enthält mit KeyID='0000' einen Wert, der in keiner Smartcard verwendet wird. Der Anfang des ICCSN-Teils der CHR weist mit dem Wert '80' auf das Gesundheitswesen hin. Die folgenden drei Stellen '987' stehen als CountryCode zur applikationsspezifischen Verfügung und werden im Regelungsbereich der gematik für TI-interne Zwecke verwendet. Die folgenden fünf Zeichen '00000' stehen in einer ICCSN für den Herausgeber und codieren in der TI den PoPP-Service.

5.3.7 TSL-Handling

Für die Prüfung von eGK-CV- und X.509-Zertifikaten benötigt der PoPP-Service eine aktuelle TSL.

A_27150 - PoPP-Service - TSL - Aktualisierung

Der PoPP-Service MUSS stündlich über den Internet-Downloadpunkt des TSL-Dienstes (vgl. [gemSpec_TSL#A_17680*]) prüfen, ob eine neue TSL zum Download bereit steht, wenn ja, diese beziehen, und dabei folgendes durchsetzen:

1. Prüfung des TLS-Server-Zertifikats des TLS-Dienstes, inkl. Hostname-Validierung und dass dieses von einer gängigen Internet-CA und auf die "gematik GmbH" ausgestellt ist (vgl. [gemSpec_TSL#TIP1-A_4058*]).
2. Abgleich des Hashwerts der aktuell im System vorliegenden TSL gegen den Hashwert am Downloadpunkt,
3. Wenn der Hashwert unterschiedlich ist, wird die TSL vom Downloadpunkt geladen.
4. Die TSL wird wie folgt geprüft:
 - a. Signaturprüfung:
 - i. Die Signatur ist gegen den in der TSL enthaltenen TSL-Signer gültig.
 - ii. Das Signaturzertifikat (TSL-Signer) ist auf den im System vorhandenen TSL-Vertrauensanker (TSL-Signer-CA-Zertifikat) rückführbar.
 - iii. Das Signaturzertifikat wird per OCSP als "good" beauskunftet.
 - iv. Die Signatur der OCSP-Response ist auf einen in der TSL enthaltenen Signer rückführbar.
 - v. Nur im Falle, dass alle Prüfungen positiv verlaufen sind, wird fortgefahren.
 - b. Die Sequenznummer der geladenen TSL ist höher als die in der im System vorhandenen TSL.
 - c. Die TSL ist zeitlich gültig.

Der PoPP-Service MUSS durchsetzen, dass ausschließlich nachdem die o.g. Punkte erfolgreich, positiv geprüft wurden, die TSL und etwaige mit der TSL transportierte TSL-Vertrauensanker übernommen werden.

Punkt 4. (Prüfung der TSL) des in dieser Anforderung genannten Ablaufs MUSS im Verarbeitungskontext der VAU durchgeführt werden (vgl. [A_27202*]).[<=]

Hinweis: Der OCSP-Responder des TSL-Dienstes ist im Internet erreichbar. Die Adresse des OCSP-Responders ist dem Authority Information Access (AIA) des Signaturzertifikats zu entnehmen.

A_27202 - PoPP-Service - TSL - Proxy für Verarbeitungskontexte

Der PoPP-Service SOLL einen TSL-Proxy umsetzen, der die TSL vom Internet-Downloadpunkt unter Berücksichtigung der Punkte 1. bis 3. aus [A_27150*] lädt und den Verarbeitungskontexten zur Verfügung stellt, um die Last auf dem TSL-Downloadpunkt gering zu halten.[<=]

Hinweis: Das SOLL in [A_27202] ermöglicht auf einen solchen Proxy zu verzichten, wenn stets nur ein oder sehr wenige Verarbeitungskontexte des PoPP-Service laufen. Der Verzicht auf die Umsetzung ist mit der gematik abzustimmen.

A_27151 - PoPP-Service - TSL - Prüfung auf Aktualität

Der PoPP-Service MUSS stündlich die Aktualität der ihm vorliegenden TSL prüfen (zeitliche Gültigkeit) und den Anbieter alarmieren, wenn die Gültigkeit sieben Tage unterschreitet. [<=]

A_27152 - PoPP-Service - TSL - Keine abgelaufene TSL verwenden

Der PoPP-Service DARF eine TSL, die zeitlich abgelaufen ist, NICHT verwenden.[<=]

5.4 ZETA Guard im PoPP-Service

Der ZETA Guard im PoPP-Service übernimmt wesentliche Sicherheitsleistungen für den Zugang zum PoPP-Service und erfüllt folgende Aufgaben. Das Gegenstück zum ZETA Guard des PoPP-Service ist der ZETA Client, der - wie der PoPP-Client - Teil des PS ist.

Die **Policy-basierte Zugriffskontrolle** stellt sicher, dass alle Zugriffe auf den PoPP-Service sicher und autorisiert sind, indem er kontinuierlich die Aktivitäten überwacht und analysiert. Solange der ZETA Guard noch keine Versicherten Clients unterstützt (Stufe 2) werden lediglich die PoPP Schnittstellen `I_PoPP_Token_Generation` durch den ZETA Guard abgesichert. Über diese findet die fachliche Kommunikation zwischen PoPP-Service und PS statt.

Die **LEI-Authentifizierung mittels SM-B** erfolgt automatisch bei freigeschalteter SM(C)-B, indem das PS ein Client Assertion JWT erstellt und mit der SM(C)-B signiert. Dieses JWT nutzt DPOP, um sicherzustellen, dass die Anfragen vom autorisierten PS stammen und Replay-Attacken verhindert werden.

Das **Session Management** für den PoPP-Service im ZETA Guard verwendet OAuth2, wobei Access- und Refresh-Token sicher verwaltet und bei Bedarf erneuert werden. Die Token sind durch DPOP an spezifische Client-Instanzen (sprich PS Instanzen) gebunden, um sicherzustellen, dass nur autorisierte Clients Zugriff haben. Bei abgelaufenen Sessions ist eine erneute Authentifizierung erforderlich.

Der PoPP-Service Anbieter verwendet den von der gematik bereitgestellten ZETA Guard, der gemäß [gemSpec_ZETA] implementiert ist. Die Beschreibung des ZETA Guard sowie Anforderungen an PoPP-Service und PoPP-Service Anbieter rund um die Einbindung und Verwendung des ZETA Guard finden sich in [gemSpec_ZETA]. In diesem Dokument sind PoPP-Service spezifische Anforderungen und Hinweise rund um das ZETA Guard enthalten (dieses Kapitel und [Kapitel Datenschutz und Sicherheit]).

Alle konkreten Informationen und Regelungen zu Bereitstellung, Konfiguration und Verwendung des ZETA Guard sind dem Betriebshandbuch des ZETA Guard-Herstellers zu entnehmen.

5.4.1 Bereitstellung, Konfiguration und Verwendung vom ZETA Guard

Zusätzlich zu den Anforderungen aus [gemSpec_ZETA] insbesondere [A_25773*] und [A_25776*], gelten für den PoPP-Service Anbieter die folgenden Anforderungen.

A_26539 - PoPP-Service Anbieter - Informationspflicht via Betriebshandbuch ZETA Guard Hersteller

Der Anbieter des PoPP-Service MUSS alle Informationen und Regelungen zu Bereitstellung, Konfiguration und Verwendung des ZETA Guard dem Betriebshandbuch des ZETA Guard-Herstellers entnehmen und anwenden. [≤]

A_26540 - PoPP-Service - ZETA Guard - PoPP Policy erstellen

Der Anbieter des PoPP-Service MUSS bei der Erstellung der Policy für den PoPP-Service mit der gematik zusammenarbeiten. Diese Policy wird über den PAP deployed und durch die Policy-Engine verarbeitet.

Hinweis: Die PoPP-Service Policy wird in GIT erstellt (CI/CD-Prozess) [≤]

Hinweis: Die Gültigkeitsdauern für Access Token und Refresh Token werden über die PoPP-Service Policy gesteuert.

A_26543 - PoPP-Service - Kommunikation zu den Zero Trust Komponenten der gematik

Der Anbieter des PoPP-Service MUSS sicherstellen, dass die Kommunikation zwischen seinem ZETA Guard und den dem PIP/PAP Server der gematik sowie dem Zero Trust git-Repository der gematik möglich ist.

[<=]

Hinweis: Der Zugriff auf den PIP/ PAP-Server erfolgt über die in [A_25670] festgelegte URL; für den PoPP-Service unter dem application Endpunkt popp.*

Die URL inklusive Endpunkt für den PoPP-Service für das Zero Trust git-repository der gematik wird organisatorisch übermittelt

5.5 Vertrauenswürdige Uhrzeit im PoPP-Service

Mit der Einführung der Telematikinfrastruktur TI1.0 wurde ein zentraler Zeitdienst eingeführt, mit dem sich alle zentralen Komponenten sowie Konnektoren regelmäßig synchronisieren müssen. Im Rahmen des Sicherheitskonzepts der TI1.0 - als geschlossenes System bekannter Nutzer - wird diese Uhrzeit als vertrauenswürdige angenommen.

Der PoPP-Service stellt für verschiedene (aktuelle und zukünftige) Anwendungsfälle ein Zeugnis über einen real existierenden Versorgungskontext zentral aus. Da der Dienst über das Internet angesprochen wird und Clientsysteme und ein PoPP-Token-nachnutzendes System (PoPP-Verifier) sich mit unterschiedlichen Zeit-Servern synchronisieren könnten als der PoPP-Service, muss die Uhrzeit des PoPP-Service vertrauenswürdige sein.

A_26508 - PoPP-Service - Vertrauenswürdige Uhrzeit

Der Anbieter des PoPP-Service MUSS seine lokale Systemzeit mindestens einmal täglich mit einem qualifizierten Zeitstempel eines eIDAS-Vertrauensdiensteanbieters synchronisieren und dafür Sorge tragen, dass die lokale Systemzeit zwischen zwei Synchronisierungen nie mehr als eine Sekunde vom Sollwert abweicht. **[<=]**

Hinweis 1: Das PoPP-Token muss in der Signatur nicht über einen qualifizierten Zeitstempel verfügen, weil das PoPP-Token auch im ersten Anwendungsfall des VSDM 2.0 keine Rolle in den abrechnungsbegründeten Informationen spielt. Durch den sicheren Betrieb des PoPP-Service und die Prüfung dieser Afo im Zulassungsverfahren des PoPP-Service kann die Uhrzeit eines ausgestellten PoPP-Token als zuverlässig betrachtet werden.

Hinweis 2: Die Bundesnetzagentur listet unter [AnbieterVZeitD] verschiedene Anbieter für qualifizierte Zeitstempel.

5.6 Federation Entity Statement

Der PoPP-Service stellt Kommunikationspartnern notwendige Informationen bereit, indem er ein Entity Statement gemäß [OpenID Federation 1.0] unter <Identifier-URL>/ .well-known/openid-federation verfügbar macht.

Das Entity Statement beaufkundet allgemeine Informationen wie:

1. Identifier (iss),

2. Schlüssel, mit denen das Entity Statement signiert wird (jwks),
3. Ausstellungszeitpunkt (iat),

und Metadaten Informationen zur Konfiguration als:

1. OAuth Authorization Server (*oauth_authorization_server*),
2. Relying Party (*openid_relying_party*),
3. OAuth Protected Resource (*oauth_resource*),
4. Teilnehmer der TI-Föderation (*federation_entity*).

Die Metadaten enthalten u. a. die Endpunkte, unter denen der PoPP-Service Authorization Server erreichbar ist und Informationen zu Signatur- und Verschlüsselungsschlüssel. Die Tabelle "Entity Statement des PoPP-Service" im Anhang stellt das Entity Statement des PoPP-Service Authorization Server exemplarisch dar.

A_27294 - PoPP-Service - Bereitstellung .well-known für PoPP-Service

Der Anbieter eines PoPP-Service MUSS sicherstellen, dass unter <Identifizier-URL>/ .well-known/openid-federation ein Entity Statement gemäß [[OpenID Federation 1.0](#)] veröffentlicht ist. Das Entity Statement MUSS über das Internet erreichbar sein. Das Metadaten-Statement MUSS mindestens die folgenden Werte enthalten:

Tabelle 7: Attribute im well-known document des PoPP-Service

Name	Werte	Beispiel / Beschreibung
iss	URL	URL des PoPP-Service, Identifizier in der TI- Föderation
sub	URL	URL des PoPP-Service, (=iss)
jwks	JWKS Objekt	Federation Entity Key für die Signatur des Entity Statements [OpenID Federation 1.0]
iat	Alle time Werte in Sekunden seit 1970, [RFC7519#Sect.2]	1645484401 für 2022-02-22 00:00:01
exp	Alle time Werte in Sekunden seit 1970, [RFC7519#Sect.2]	1645570800 für Ablauf 24h nach iat
authority_hints	[string]	iss Bezeichnung des Federation Masters (PU: "https://app.federationmaster.de")

[<=]

A_27295 - PoPP-Service - Bereitstellung .well-known für PoPP-Service Resource Server

Der Anbieter eines PoPP-Service MUSS sicherstellen, dass in dem unter <Identifizier-URL>/ .well-known/openid-federation gemäß [[OpenID Federation 1.0](#)] bereitgestellten Entity Statement die Metadaten als OAuth Resource Server in einem

Metadaten-Statement `oauth_resource` veröffentlicht sind.
Das Metadaten-Statement MUSS mindestens die folgenden Werte enthalten:

Tabelle 8: Attribute des Metadatenblock `oauth_resource` im well-known document des PoPP-Service

Name	Werte	Beispiel
<code>signed_jwks_uri</code>	URL	"https://popp-resource.de/jwks.jose"

[<=]

A_27296 - PoPP-Service - Bereitstellung .well-known als Teilnehmer der TI-Föderation

Der Anbieter eines PoPP-Service MUSS sicherstellen, dass in dem unter <Identifizier-URL>/`.well-known/openid-federation` gemäß [[OpenID Federation 1.0](#)] bereitgestellten Entity Statement die Metadaten als Teilnehmer der TI-Föderation in einem Metadaten-Statement `federation_entity` veröffentlicht sind.
Das Metadaten-Statement MUSS mindestens die folgenden Werte enthalten:

Tabelle 9: Attribute des Metadatenblock `federation_entity` im well-known document des PoPP-Service

Name	Werte	Beispiel
<code>organization_name</code>	String (max. 128 Zeichen) Wertebereich: <code>^[ÄÖÜäöüß\w\ \.\&\+*V]{1,128}</code>	<Herstellername PoPP-Service>
<code>homepage_uri</code>	URL	"https://popp-hersteller.de"
<code>contacts</code>	[string]	["support@popp-hersteller.de", "info@popp-hersteller.de"]

[<=]

A_26545 - PoPP-Service - Bereitstellung .well-known für PoPP-Service Authorization Server

Der Anbieter eines PoPP-Service MUSS sicherstellen, dass in dem unter <Identifizier-URL>/`.well-known/openid-federation` gemäß [[OpenID Federation 1.0](#)] bereitgestellten Entity Statement die Metadaten als Relying Party der TI-Föderation in einem Metadaten-Statement `openid_relying_party` veröffentlicht sind (siehe [gemSpec_IDP_FD]).

Der Anbieter eines PoPP-Service Authorization Server MUSS außerdem sicherstellen, dass in dem unter <Identifizier-URL>/`.well-known/openid-federation` gemäß [[OpenID Federation 1.0](#)] bereitgestellten Entity Statement die Metadaten als OAuth Authorization Server in einem Metadaten-Statement `oauth_authorization_server` veröffentlicht sind.
Das Metadaten-Statement MUSS mindestens die folgenden Werte enthalten:

Tabelle 10: Attribute des Metadatenblock `oauth_authorization_server` im well-known document des PoPP-Service

Name	Werte	Beispiel
<code>authorization_endpoint</code>	URL	"https://popp-auth.de/auth"

token_endpoint	URL	"https://popp-auth.de/token"
signed_jwks_uri	URL	"https://popp-auth.de/jwks.jose"
openid_providers_endpoint	URL	URL, unter welcher die Liste aller registrieren sektoralen IDP abrufbar ist (bspw. direkt am Federation Master PU [https://app.federationmaster.de/federation/listidps]
response_types_supported	<i>code</i>	-
response_modes_supported	<i>query</i>	-
grant_types_supported	<i>authorization_code</i>	-
token_endpoint_auth_methods_supported	<i>none</i>	-
token_endpoint_auth_signing_alg_values_supported	<i>ES256</i>	-
code_challenge_methods_supported	<i>S256</i>	

[<=]

Hinweis: Anforderungen an die Erstellung und Pflege des Entity Statements als Relying Party der TI-Föderation finden sich in [gemSpec_IDP_FD#Kapitel Entity Statements]. Die Tabelle "Entity Statement des PoPP-Service" im Anhang stellt das Entity Statement des PoPP-Service Authorization Server exemplarisch dar.

6 Funktionsmerkmale

6.1 PoPP-Service - Authorization Server

Der PoPP-Service Authorization Server schützt den PoPP-Service Resource Server vor unberechtigten Zugriffen von unbekannten Clients aus dem Internet. Auf Basis des OAuth Framework [RFC6749] stellt er Access Tokens für in der Föderation registrierte Clients aus.

Schnittstellen des PoPP-Service, die eine Nutzeridentifikation benötigen, werden vom PoPP-Service Authorization Server mit Access Token versorgt. Der PoPP-Service Authorization Server in seiner Rolle als Relying Party der Identitätsföderation delegiert dabei die Nutzerauthentifizierung an einen geeigneten sektoralen IDP. In Nutzungsszenarien mit eGK (ohne Verwendung der GesundheitsID) werden diese Identitätsinformationen vom PoPP-Service auf sichere Art und Weise aus der eGK ausgelesen.

6.1.1 Standard Authorization Server mit Versicherten Authentisierung

Da der von der gematik bereitgestellte ZETA Guard in der ersten Stufe noch keine Authentisierung von Versicherten unterstützt, wird diese Funktion übergangsweise von einem separaten PoPP-Service Authorization Server übernommen. Dieser muss vom Hersteller des PoPP-Service umgesetzt und in den PoPP-Service integriert werden.

Die Anforderungen an einen PoPP-Service Authorization Server für die Nutzung sektoraler Identity Provider (IDP), sind in [gemSpec_IDP_FD] beschrieben. Das vorliegende Dokument enthält lediglich einen kurzen Überblick und abweichende oder zusätzliche Anforderungen an einen PoPP-Service Authorization Server.

Der PoPP-Service Authorization Server erfüllt im Kontext der Nutzerauthentisierung mit GesundheitsID die Funktionen:

1. eines OAuth Server für Client-Registrierung einer Anwendung, welche ein PoPP-Modul integriert und
2. eines OAuth Server für Autorisierungsanfragen eines registrierten Clients und
3. einer Relying Party in der TI-Föderation.

Die Abbildung "Komponentendiagramm PoPP-Service Authorization Server bei Authentifizierung mit GesundheitsID" veranschaulicht die Komponenten des PoPP-Service in diesem Kontext. Das in eine App integrierte PoPP-Modul ist der OAuth Client, mit welchem der Versicherte interagiert. Der PoPP-Service Authorization Server in seiner Funktion als OAuth Server stellt dem OAuth Client nach erfolgreicher Nutzerauthentisierung mit GesundheitsID ein "eHealth-ID-check" Access Token aus. Mit diesem "eHealth-ID-check" Access Token kann der OAuth Client dann auf die OAuth Protected Resource - den PoPP-Service - zugreifen.

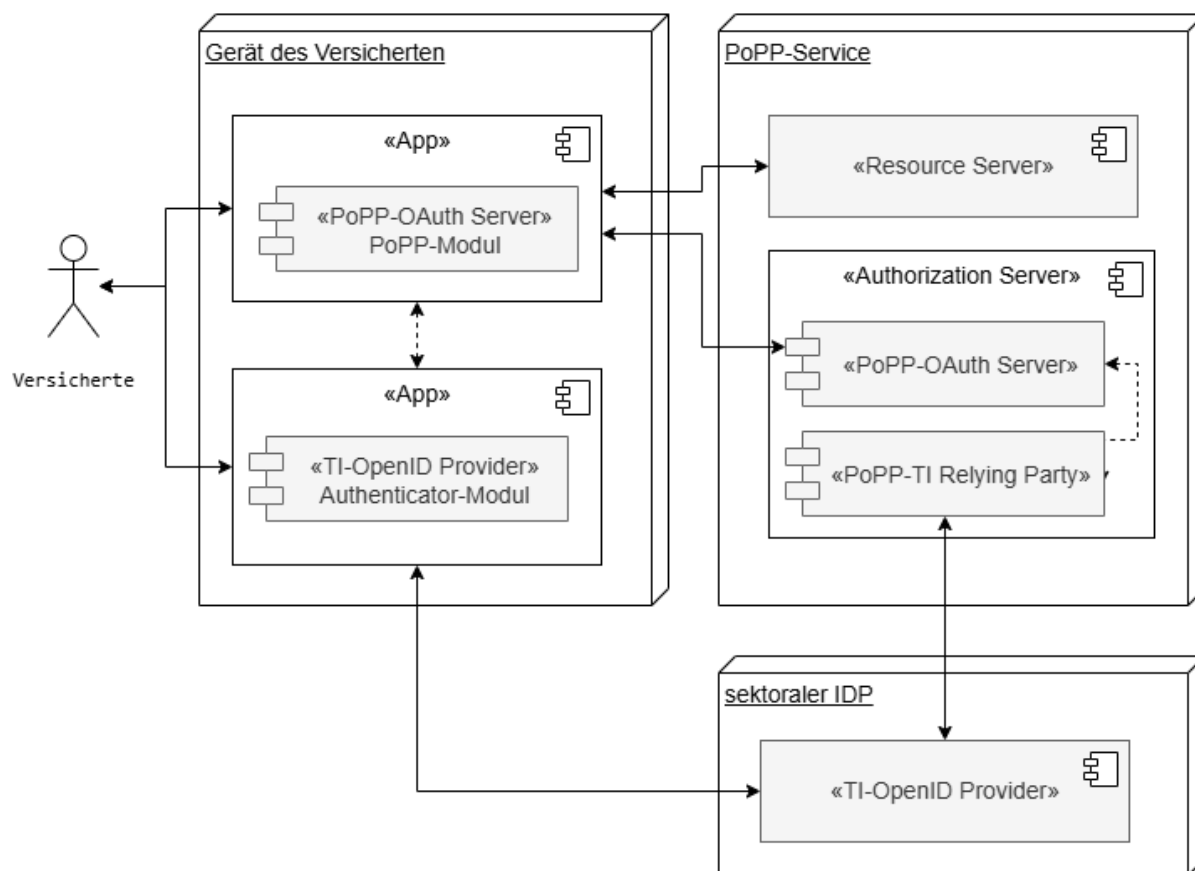


Abbildung 12: Komponentendiagramm PoPP-Service Authorization Server bei Authentifizierung mit GesundheitsID

Zur Nutzer-Authentisierung verwendet der Versicherte die Authenticator-Funktionalität der GesundheitsID in der Kassen-App oder, wenn dort nicht integriert, eine separate Authenticator-App. Das Authenticator-Modul ist die Frontend-Komponente des sektoralen IDP der Krankenkasse, also eines in der TI-Föderation registrierten OpenID-Providers.

Der PoPP-Service Authorization Server ist zur Durchführung der Authentifizierung der Versicherten als Relying Party in der TI-Föderation registriert. Weitere Informationen zur TI-Föderation sind unter [IDP-Wissensdatenbank] zu finden.

Zur Bestätigung valider Client-Instanzen durchläuft jede Anwendung mit integriertem PoPP-Modul, die den PoPP-Service nutzen möchte, eine organisatorische Client-Registrierung im Registrierungsprozess der gematik für den PoPP-Service Authorization Server - ähnlich, wie es heute bereits beim E-Rezept Fachdienst Authorization Server praktiziert wird. Dabei wird der Anwendung im Registrierungsprozess eine Client-ID zugewiesen und ein API-Key - beide Parameter sind in Autorisierungsanfragen der Client-Instanzen mitzusenden. Anfragen nicht-registrierter Anwendungen werden vom PoPP-Service Authorization Server abgewiesen.

6.1.2 Authorization Server Zusatzfunktion Authentifizierung eGK mobil

Neben den Funktionen zur Authentifizierung des Versicherten mit seiner GesundheitsID (OAuth Server, Relying Party) bietet der PoPP-Service Authorization Server eine weitere

Funktionalität an: die Authentifizierung der an das Mobilgerät des Versicherten angebrachten eGK (eGK mobil). Dies ist für den PoPP-Service - neben GesundheitsID und Nutzung der eGK in einer LEI - ein alternativer Weg die Informationen zur Versichertenidentität zu erhalten.

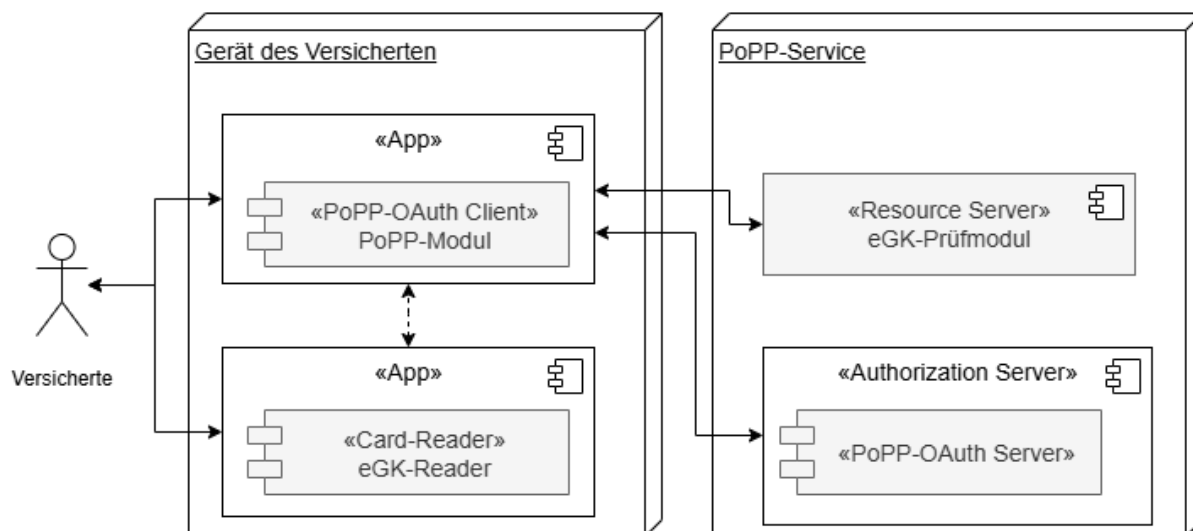


Abbildung 13: Komponentendiagramm PoPP-Service Authorization Server bei Authentifizierung einer eGK mobil

Eine App (etwa Videosprechstunde, Apotheken) implementiert für die Authentifizierung der eGK des Nutzers ein PoPP-Modul und einen eGK-Reader (beispielsweise auf Basis der NFC-Funktionalität des Mobilgeräts des Versicherten). Das PoPP-Modul ist auch hier der OAuth Client zum PoPP-Service Authorization Server. Ist das PoPP-Modul ein OAuth Client, der dem PoPP-OAuth Server bekannt ist (registrierter OAuth Client), so stellt dieser dem OAuth Client "card-check" Access Token aus. Mit diesem "card-check" Access Token kann der OAuth Client dann auf die OAuth Protected Resource - den PoPP-Service Resource Server - zugreifen. Der PoPP-Service Resource Server tauscht mit der eGK dann direkt Daten aus, über die der PoPP-Service die eGK authentifiziert.

6.1.3 Anforderungen an den PoPP-Service Authorization Server in der Funktion OAuth Server

6.1.3.1.1 Service Discovery

Der PoPP-Service Authorization Server stellt Kommunikationspartnern notwendige Informationen im Metadatenblock `openid_relying_party` im Entity Statement des PoPP-Service gemäß [OpenID Federation 1.0] bereit.

Die Metadaten enthalten u. a. die Endpunkte, unter denen der PoPP-Service Authorization Server erreichbar ist und Informationen zu Signatur- und Verschlüsselungsschlüssel. Die Tabelle "Entity Statement des PoPP-Service" im Anhang stellt den Metadatenblock im Entity Statement des PoPP-Service exemplarisch dar.

6.1.3.1.2 Client Registrierung

A_26544 - PoPP-Service Authorization Server - Ermöglichung einer organisatorischen Registrierung von PoPP-Modul

Der Anbieter eines PoPP-Service MUSS an seinem PoPP-Service Authorization Server eine organisatorische Registrierung von PoPP-Modul ermöglichen. Der Anbieter eines PoPP-Service Authorization Server MUSS jedem registrierten PoPP-Modul eine eindeutige `client_id` zuweisen.

Die Registrierung erfolgt einmalig für ein Anwendungsfrontend und muss bei Updates nicht wiederholt werden. Die Registrierung eines Anwendungsfrontends beinhaltet mindestens die Attribute aus Tabelle "Attribute zur Registrierung von Anwendungsfrontends".

Tabelle 11: Attribute zur Registrierung von Anwendungsfrontends

Client Eigenschaft	Beschreibung
Produkt-Name	Produkt-Name, vergeben durch den Hersteller
Hersteller-ID	Kennung des Herstellers aus TI-ITSM
Hersteller-Name	Name des Herstellers aus TI-ITSM
Produkt-Plattform	Android oder Apple (iOS, macOS etc.)
<code>redirect_uri</code>	Adresse des Authorization Server Endpunkts zur Annahme des vom sektoralen IDP ausgestellten Authorization Code zur Weiterleitung an den PoPP-Service Authorization Server

[<=]

6.1.3.2 Ausstellung eines "eHealth-ID-check" Access Token

A_26546 - PoPP-Service Authorization Server - Signatur des vom PoPP-Service Authorization Server ausgestellten Access Token

Der PoPP-Service Authorization Server MUSS sicherstellen, dass das von ihm ausgestellte Access Token unter Verwendung eines privaten Schlüssels signiert ist, zu welchem der zugehörige öffentliche Schlüssel unter der im Entity Statement des PoPP-Service im Claim `metadata.oauth_authorization_server.signed_jwks_uri` angegebenen URL bezogen werden kann.[<=]

Hinweis: Anforderungen an die Signaturschlüssel sind in [gemSpec_IDP_FD#Kapitel Entity Statements] beschrieben.

A_26564 - PoPP-Service Authorization Server - Verschlüsselung des Access Token

Der PoPP-Service Authorization Server MUSS sicherstellen, dass ein Verschlüsselungsschlüssel des PoPP-Service über den `use` Parameter ("`use = enc`") aus dem Attribut `metadata.oauth_authorization_server.signed_jwks_uri` im Metadatenblock `oauth_authorization_server` des Entity Statements des PoPP-Service bezogen wird und mit diesem das Access Token verschlüsseln. Im JWE-Header des Token referenziert der PoPP-Service Authorization Server über den Parameter `kid` den Schlüssel-Identifikator des verwendeten Verschlüsselungsschlüssels. Als Verschlüsselungsverfahren MUSS hierbei ECDH-ES [RFC7518] verwendet werden.[<=]

A_26562 - PoPP-Service Authorization Server - Ausstellen und Inhalt des "eHealth-ID-check" Access Token

Der PoPP-Service Authorization Server MUSS bei einer Nutzerauthentifizierung mit GesundheitsID sicherstellen, dass ein "eHealth-ID-check" Access Token ausschließlich für registrierte Clients ausgestellt wird. Die benötigten Attribute (Tabelle "Befüllung der Attribute nach Bestätigung durch einen sektoralen Identity Provider") in den Claims für das auszustellende "eHealth-ID-check" Access Token MÜSSEN aus den entsprechenden Claims des ID Token des sektoralen IDP oder aus dem Registrierungsprozess bezogen werden.

Tabelle 12: "ehealthId-check" Access Token nach Bestätigung durch einen sektoralen Identity Provider

Attribute	Wert/Wertebereich	Informationsquelle
	KVNR, entspricht dem Claim <code>urn:telematik:claims:id</code> aus dem vom sektoralen IDP ausgestellten ID Token	ID Token des sektoralen IDP
	Herausgeber-ID (Institutionskennzeichen), entspricht dem Claim <code>urn:telematik:claims:organization</code> aus dem vom sektoralen IDP ausgestellten ID Token	ID Token des sektoralen IDP
actorId	Telematik-ID der LEI, für die ein Check-in ausgeführt wird (optional)	PoPP-Modul, Auswahl der LEI durch die Versicherten
amr	Der Claim amr entspricht dem Claim amr aus dem vom sektoralen IDP ausgestellten ID Token	ID Token des sektoralen IDP
acr	Der Claim acr entspricht dem Claim acr aus dem vom sektoralen IDP ausgestellten ID Token	ID Token des sektoralen IDP
aud	URL des PoPP-Service Resource Server	PoPP-Service Entity Statement
iat	Alle time Werte in Sekunden seit 1970, [RFC7519#Sect.2]	Ausstellungszeitpunkt des Access Token
exp	Alle time Werte in Sekunden seit 1970, [RFC7519#Sect.2]	Ablaufzeitpunkt des Access Token

[<=]

6.1.3.3 Ausstellung eines "card-check" Access Token

A_27216 - PoPP-Service Authorization Server - Austellen des "card-check" Access Token

Der PoPP-Service Authorization Server MUSS bei der Authentifizierung mit eGK(mobil), sicherstellen, dass ein "card-check" Access Token ausschließlich für PoPP-Module von am PoPP-Service Authorization Server registrierte Anwendungen ausgestellt wird.

Tabelle 13: "card-check" Access Token für die Prüfung der eGK(mobil)

Attribute	Wert/Wertebereich	Informationsquelle
actorId	Telematik-ID der LEI, für die ein Check-in ausgeführt wird	PoPP-Modul, Auswahl der LEI durch die Versicherten
aud	URL des PoPP-Service Resource Server	PoPP-Service Entity Statement
iat	Alle time Werte in Sekunden seit 1970, [RFC7519#Sect.2]	Ausstellungszeitpunkt des Access Token
exp	Alle time Werte in Sekunden seit 1970, [RFC7519#Sect.2]	Ablaufzeitpunkt des Access Token

[<=]

6.1.4 Mobile Verfahren zur Bestätigung der Versicherten-Identität

Für die Erstellung des PoPP-Token ist es möglich, dass der Versicherte seine Identität bestätigt, indem er sich mit seiner GesundheitsID gegen den sektoralen IDP seiner Krankenversicherung authentifiziert. Der Ablauf der eigentlichen Authentisierung aus dem Frontend ist für den Versicherten für jeden TI-Fachdienst (E-Rezept, Patientenakte, PoPP) immer gleich.

Über die Benutzeroberfläche löst der Versicherte die gewünschte Funktion aus. Das Frontend sendet daraufhin einen Request an den Authorization Server des jeweiligen Fachdienst. Dieser stellt daraufhin eine Autorisierungsanfrage (Pushed Authorization Request) an den sektoralen IDP, welcher die Identitätsdaten des Versicherten hält.

Der Versicherte muss sich dann geeignet authentisieren. Dazu hat entweder die Kassen-App ein integriertes Authenticator-Modul oder es ist eine zusätzliche Authentisierungs-App auf dem Gerät des Versicherten installiert. Nach erfolgreicher Authentisierung erhält der Versicherte Zugang zu den eigentlichen Funktionen des TI-Fachdienstes.

Der PoPP-Service ist in diesem Kontext der TI-Fachdienst. Dem Versicherten zum "Check-in" wird für eine Behandlung (bspw. in einer Praxis) ein Frontend, das PoPP-Modul, angeboten. Technisch muss der PoPP-Service neben der Benutzeroberfläche, also dem in eine App integrierten PoPP-Modul, auch einen PoPP-Service Authorization Server bereitstellen.

Neben der Authentisierung mittels GesundheitsID ist auch die mobile Authentisierung der eGK möglich. Die Authentisierung der eGK erfolgt durch das Senden von APDU-Commands vom PoPP-Service Resource Server direkt an eGK.

Nach erfolgreicher Authentisierung mit GesundheitsID oder eGK erhält das PoPP-Modul, je nach Konstellation und Konfiguration, ein TAN-Set mit "langen" TAN oder eine "kurze" TAN. Diese können dann je nach Anwendungsfall in Form eines QR-Code oder als Zahlenwert (bei "kurze" TAN) im PoPP-Modul angezeigt werden kann.

Die folgende Abbildung zeigt den Ablauf zur Erlangung einer TAN durch das PoPP-Modul für die beiden unterscheidlichen Check-in Prozesse.

Abbildung 14: Sequenzdiagramm Nutzer Authentisierung mit GesundheitsID oder eGK und die Erlangung einer TAN oder eines TAN-Sets über ein PoPP-Modul

Unabhängig von der Wahl des mobilen Check-in Prozesses über GesundheitsID oder mit eGK hat der Versicherte die Möglichkeit eine LEI (und damit eine Telematik-ID) auszuwählen, zu der eine "kurze" TAN generiert werden soll. Wird keine LEI ausgewählt, so wird ein TAN-Set mit "langen" TAN ohne LEI-Bezug generiert.

Nach Auswahl des Check-in Prozess unterscheiden sich die Abläufe jedoch. Die folgende Tabelle zeigt die Schritte im Ablauf, wenn der Check-in über die Authentisierung des Versicherten mit GesundheitsID erfolgt.

Tabelle 14: Kurzbeschreibung des Ablaufs der Nutzerauthentisierung mit GesundheitsID für die Erlangung einer TAN oder eines TAN-Sets über ein PoPP-Modul

Schritt	Kurzbeschreibung	Beschreibung
	Versicherter hat Check-in mit GesundheitsID gewählt	Der Versicherte hat den Check-in Prozess über eine Funktion des PoPP-Moduls, welches in eine App integriert ist, gestartet und für den Check-in die Authentisierung mit seiner GesundheitsID ausgewählt.
1	chooseIDP	Der Versicherte muss seine Krankenkasse (und damit die eindeutige Adresse iss-idp des sektoralen IDP der Krankenkasse) auswählen, damit die Nutzerauthentisierung gegen diesen sektoralen IDP erfolgen kann. Ist die Zuordnung in der App bereits bekannt, entfällt dieser Schritt.
2	sendAuthorizationRequest	Das PoPP-Modul sendet einen OAuth2 konformen Authorization Request an den PoPP-Service Authorization Server (OAuth Server) [RFC6749].
3	checkRegisteredClient	Der PoPP-Service Authorization Server prüft, ob ein PoPP-Modul mit der Client-ID registriert ist, der Request also von einem vertrauenswürdigen Client kommt. Zur Sicherstellung der Vertrauenswürdigkeit muss das PoPP-Modul den API-Key im Request mitgeben, welchen er im Registrierungsprozess vom PoPP-Service Authorization Server erhalten hat.
4-14	Ablauf der Nutzerauthentisierung	Der PoPP-Service Authorization Server (OpenID Relying Party) stößt den Prozess der Nutzerauthentisierung an. Der Ablauf der Nutzerauthentisierung ist in [gemSpec_IDP_Sek#Kapitel Ablaufbeschreibung App-App-Flow]

		beschrieben.
15	generateEHealthIdCheckAccessToken	<p>Nach erfolgreicher Nutzerauthentisierung und Erhalt des ID Token vom sektoralen IDP erstellt der PoPP-Service Authorization Server (OAuth Server) ein "eHealth-ID-check" Access Token. Das Access Token beinhaltet u.a.:</p> <ol style="list-style-type: none"> 1. die KVNR des Versicherten, 2. die IK-Nummer der Krankenkasse des Versicherten, 3. die vom Nutzer ausgewählte Telematik-ID (optional)
16	encryptEHealthIdCheckAccessToken	Der PoPP-Service Authorization Server verschlüsselt das Access Token mit dem öffentlichen Schlüssel des PoPP-Service Resource Server (veröffentlicht im Entity Statement).
17	signEHealthIdCheckAccessToken	Der PoPP-Service Authorization Server erzeugt ein weiteres Access Token, in das das verschlüsselte Access Token eingebettet wird (nested jwt) und signiert dieses Access Token mit seinem privaten Schlüssel (der öffentliche Schlüssel ist im Entity Statement veröffentlicht).
18	responseHTTP200	Das PoPP-Modul erhält als Antwort auf den Authorization Request ein HTTP-200 und das vom PoPP-Service Authorization Server (OAuth Server) ausgestellten "eHealth-ID-check" Access Token.
19	generateTAN2KVNR	Das PoPP-Modul ruft den PoPP-Service Resource Server für die Generierung einer TAN oder eines TAN-Sets auf. Für die Legitimierung des Aufrufs übergibt das PoPP-Modul des "eHealth-ID-check" Access Token.
20	validateEHealthIdCheckAccessToken	Der PoPP-Service Resource Server prüft die Signatur des "eHealth-ID-check" Access Token.
21	decryptEHealthIdCheckAccessToken	Der PoPP-Service Resource Server entschlüsselt das "eHealth-ID-check" Access Token.
22	extractKVNR	Der PoPP-Service Resource Server

		extrahiert die KVNR aus dem entschlüsselten "eHealth-ID-check" Access Token.
23	extractIKNR	Der PoPP-Service Resource Server extrahiert die IK-Nummer aus dem entschlüsselten "eHealth-ID-check" Access Token.
24	extractTelematicId	Der PoPP-Service Resource Server extrahiert, wenn vorhanden, die Telematik-ID der ausgewählten LEI aus dem entschlüsselten "eHealth-ID-check" Access Token.

Der Ablauf bei der Verifizierung der eGK läuft etwas anders ab. Die folgende Tabelle beschreibt die Schritte nach der optionalen Auswahl einer LEI und der Auswahl "eGK(mobil)" für den Check-in Prozess.

Tabelle 15 : Kurzbeschreibung des Ablaufs der Authentifizierung der eGK für die Erlangung einer TAN oder eines TAN-Sets über ein PoPP-Modul

Schritt	Kurzbeschreibung	Beschreibung
	Versicherter hat Check-in mit eGK(mobil) gewählt	Der Versicherte hat den Check-in Prozess über eine Funktion des PoPP-Moduls, welches in eine App integriert ist, gestartet und den Check-in mit eGK ausgewählt.
1	sendAuthorizationRequest	Das PoPP-Modul sendet einen OAuth2 konformen Authorization Request an den PoPP-Service Authorization Server (OAuth Server) [RFC6749].
2	checkRegisteredClient	Der PoPP-Service Authorization Server prüft, ob ein PoPP-Modul mit der Client-ID registriert ist, der Request also von einem vertrauenswürdigen Client kommt. Zur Sicherstellung der Vertrauenswürdigkeit muss das PoPP-Modul den API-Key im Request mitgeben, welchen er im Registrierungsprozess vom PoPP-Service Authorization Server erhalten hat.
3	generateCardCheckAccessToken	Der Authorization Server generiert ein "card-check" Access Token. Wurde im Nutzer bereit eine LEI ausgewählt, so beinhaltet das Access Token auch die Telematik-ID der LEI.
4	signCardCheckAccessToken	Der Authorization Server signiert das generierte "card-check" Access Token.

5	responseHTTP200	Der Authorization Server antwortet dem PoPP-Modul mit HTTP-200 und dem "card-check" Access Token.
6	generateTAN2EHCCheck	Das PoPP-Modul fordert beim PoPP-Service Resource Server die Prüfung der eGK und die Generierung einer TAN an. Die Übergabe des "card-check" Access Token autorisiert die Anfrage.
7	validateCardCheckAccessToken	Der PoPP-Service Resource Server prüft die Signatur des "card-check" Access Token.
8-13	Ablauf der Kartenprüfung	Die Kartenprüfung erfolgt durch Kommunikation des in den PoPP-Service Resource Server integrierten eGK-Prüfmoduls über das PoPP-Modul direkt mit der eGK (siehe auch 6.2.1- eGK-Handling).
14	readKVNR	Der PoPP-Auth Server extrahiert die KVNR aus den Daten der eGK.
15	readIKNR	Der PoPP-Auth Server extrahiert die IK-Nummer aus den Daten der eGK.
16	extractTelematicId	Der PoPP-Service Resource Server extrahiert, wenn vorhanden, die Telematik-ID der ausgewählten LEI aus dem entschlüsselten "eHealth-ID-check" Access Token.

Nach der Authentisierung mit GesundheitsID oder eGK liegen im PoPP-Service Resource Server alle Information gesichert vor, um die TAN-Generierung durchzuführen. Dabei werden noch folgende Schritte durchlaufen.

Tabelle 16 : Kurzbeschreibung des Ablaufs nach Authentifizierung mit GesundheitsID oder eGK für die Erstellung einer TAN oder eines TAN-Sets und Übergabe an das PoPP-Modul

Schritt	Kurzbeschreibung	Beschreibung
	Informationen für TAN Generierung liegen im PoPP-Service Resource Server vor	<p>Durch den Abschluss des Check-in Prozess mit GesundheitsID oder eGK sind folgende Informationen im PoPP-Service Resource Server gesichert vorhanden:</p> <ol style="list-style-type: none"> 1. KVNR des Versicherten, 2. IK-Nummer der Krankenkasse des Versicherten, 3. Telematik-ID einer LEI (optional),

		<p>4. Zeitstempel des Abschlusses des Check-in,</p> <p>5. Check-in Methode (GesundheitsID oder eGK).</p> <p>Außerdem liegen weitere Informationen durch die Konfiguration des PoPP-Service vor:</p> <ol style="list-style-type: none"> 1. Maximale Anzahl von "langen" TAN in einem TAN-Set, 2. Maximale Gültigkeit eines TANSet-Record und damit der zugeordneten TAN.
1	generateTANOrTANSet	<p>Der PoPP-Service Resource Server generiert eine "kurze" TAN, wenn eine Telematik-ID vom PoPP-Modul übergeben wurde oder ein TAN-Set mit der in der Konfiguration des PoPP-Service hinterlegten Anzahl "langen" TAN.</p>
2	generateTANSetRecord	<p>Der PoPP-Service Resource Server generiert ein TANSet-Record mit den Daten</p> <ol style="list-style-type: none"> 1. KVN-R des Versicherten, 2. IK-Nummer der Krankenkasse des Versicherten, 3. Telematik-ID einer LEI (optional), 4. Zeitstempel des Abschlusses des Check-in, 5. Check-in Methode (GesundheitsID oder eGK), 6. Zeitstempel für den Ablauf der Gültigkeit des TANSet-Record 7. generierte TAN oder TAN-Set. <p>Der Zeitstempel für den Ablauf der Gültigkeit des TANSet-Record wird dabei aus dem Zeitstempel des Abschlusses des Check-in und der in der Konfiguration des PoPP-Service hinterlegten Gültigkeitsdauer berechnet.</p>
3	saveTANSetRecord	<p>Der PoPP-Service Resource Server speichert den erstellten TANSet-Record.</p>
4	responseHTTP200	<p>Der PoPP-Service Resource Server antwortet dem PoPP-Modul mit HTTP-200 und der generierten TAN bzw. des generierten TAN-Sets sowie einem Zeitstempel, die Gültigkeit von TAN/TAN-Set abläuft..</p>
5	saveTANOrTANSet	<p>Das PoPP-Modul speichert,</p> <ol style="list-style-type: none"> 1. wenn eine "kurze" TAN übermittelte wurde, diese zur ausgewählten LEI,

		2. sonst das übermittelte TAN-Set zusammen mit dem Zeitstempel für den Ablauf der Gültigkeit im Gerätespeicher des Smartphones.
--	--	--

A_26503 - PoPP-Service Authorization Server - Bereitstellung Authorization Server für Nutzung GesundheitsID

Der PoPP-Service Authorization Server in der Funktion Relying Party der TI-Föderation MUSS zur Unterstützung der Authentisierung eines Versicherten mit seiner GesundheitsID einen Authorization Server umsetzen, der den Anforderungen an FD der TI-Föderation genügt. [≤]

Hinweis: Die Anforderungen an einen FD als Relying Party in der TI-Föderation sind in [gemSpec_IDP_FD] beschrieben.

A_26547 - PoPP-Service Authorization Server - Registrierung benötigte Scopes und Claims für Versicherte

Der Anbieter eines PoPP-Service Authorization Server in der Funktion Relying Party der TI-Föderation MUSS bei der Registrierung am Federation Master sicherstellen, dass ausschließlich der Scope urn:telematik:versicherter beantragt wird. [≤]

Hinweis: Der Scope urn:telematik:versicherter enthält als Claim die KVNR des Versicherten (siehe auch [gemSpec_IDP_Sek#Kapitel Token-Endpunkt Ausgangsdaten]).

A_26549 - PoPP-Service Authorization Server - Liste der redirect_uris im Entity Statement

Der Anbieter eines PoPP-Service Authorization Server in der Funktion Relying Party der TI-Föderation MUSS im Metadatenblock openid_relying_party des Entity Statements im Claim redirect_uris die redirect_uris aller Clients listen, welche eine Authentisierung mit GesundheitsID unterstützen. [≤]

A_26548 - PoPP-Service Authorization Server - Pushed Authorization-Request des PoPP-Service Authorization Server an den sektoralen Identity Provider

Der PoPP-Service Authorization Server in der Funktion Relying Party der TI-Föderation MUSS sicherstellen, dass der Pushed Authorization Request (PAR) an den vom PoPP-Modul übergebenen Parameter idp-iss adressierten sektoralen IDP gemäß [gemSpec_IDP_FD#AF_10117] erfolgt. Für die Parametern im PAR sind folgende Werte zu setzen:

Tabelle 17: Werte für spezifische Parameter im PAR

Parameter	Wert	Anmerkung
scope	openid urn:telematik:versicherte	notwendige Informationen zum Versicherten für die Erstellung eines PoPP-Token
acr_values	gematik-ehealth-loa-high	angefordertes Niveau der Nutzerauthentisierung
redirect_uri	Übernahme der redirect_uri aus dem initialen GET Request des Anwendungsfrontends	Diese URI muss zu einem registrierten Client gehören und unter dem Claim redirect_uri im Entity Statement des PoPP Authorization Services enthalten sein.

[<=]

6.1.5 Schnittstellen

Die Schnittstellenbeschreibung für die Erlangung eines Access Token, um auf den PoPP-Service zugreifen zu können, ist als OpenAPI-Dokumentation in [I_PoPP_Checkin_AuthorizationServer.yaml] hinterlegt. Die relevanten Anforderungen verweisen auf die dort dokumentierte Schnittstellendefinition.

A_27309 - Schnittstellen des PoPP-Service Authorization Server

Der PoPP-Service Authorization Server MUSS die Anwendungsfälle [[Mobiler Check-in mit GesundheitsID](#)] und [[Mobiler Check-in mit eGK](#)] für PoPP-Module unterstützen. Er MUSS Operationen zum Erhalt von Access Token gemäß [I_PoPP_Checkin_AuthorizationServer.yaml] für die Anfragen von PoPP-Modulen bereitstellen. Die Schnittstellen für den Zugriff der PoPP-Module auf den PoPP-Service Authorization Server müssen über das Internet verfügbar sein. [<=]

6.2 PoPP-Service - Resource Server

Innerhalb des PoPP-Service Resource Server sind die Komponenten und Funktionalitäten zusammengefasst, die zur Erstellung der PoPP-Token als Nachweis des Versorgungskontextes beitragen.

Im Wesentlichen werden die LEI-Informationen (TelematikID) und die Versicherten Informationen (KVNR und IK-Nummer) verarbeitet, ggf. temporär gespeichert, und ein PoPP-Token erstellt.

Die Zugriffsautorisierung wird für Primärsysteme (PS) der LEI dabei vom ZETA Guard in Form von signierten Access Token erzeugt und über das DPoP-Verfahren an das Client-System gebunden.

Für den PoPP-Service nutzende Client-Systeme (mobile Apps) der Anwendungen in den Händen der Versicherten, stellt der PoPP-Service Authorization Server entsprechende Access Token aus.

A_27348 - PoPP-Service - Validierung signierter Access Token

Der PoPP-Service MUSS bei der Gültigkeitsprüfung von eingereichten Access Token sicherstellen, dass diese Token von vertrauenswürdigen Ausstellern signiert sind.<= [<=]

Hinweis: Eine Vertrauensstellung des PoPP-Service (Resource Server) besteht hierbei zum ZETA Guard und zum Authorization Server des PoPP-Service.

A_27102 - PoPP-Service - Verwenden der LEI Daten im Resource Server

Der PoPP-Service MUSS die TelematikID und professionOID einer LEI aus dem durch den ZETA Guard gesetzten HTTP Header gemäß [A_25669 - PEP HTTP Proxy - Zusätzliche HTTP-Header] auslesen und verwenden.[<=]

6.2.1 eGK-Handling

6.2.1.1 eGK-Handling, Einführung

Ohne hier auf eine Zerlegung des Systems PoPP-Service einzugehen wird in diesem Kapitel beschrieben und spezifiziert, wie das System PoPP-Service Nachrichten mit einer Smartcard austauscht. Der Transport solcher Nachrichten wird in anderen Kapiteln behandelt. Deshalb ist das Kommunikationsmodell hier einfach: Der PoPP-Service schickt Kommando APDU zu einer Smartcard und erhält von dort die korrespondierenden Antwort APDU zur Auswertung.

Der PoPP-Service kommuniziert im Rahmen der folgenden Use Cases mit einer Smartcard:

1. Ein Versicherter "steckt" seine eGK in einen Kartenleser, der über einen PoPP-Client mit dem PoPP-Service kommuniziert. Unterpunkte:
 - a. Der Versicherte befindet sich in einer LEI und
 - i. eGK, kontaktbehaftet in einem eH-KT, oder
 - ii. eGK, kontaktbehaftet in einem Standard-Kartenleser, oder
 - iii. eGK, kontaktlos in einem eH-KT, oder
 - iv. eGK, kontaktlos in einem Standard-Kartenleser.
 - b. Der Versicherte und ein LE befinden sich außerhalb einer LEI. Der LE verfügt über ein mobiles Endgerät mit PS und die eGK kommuniziert
 - i. kontaktbehaftet mit einem am PS angeschlossenen Standard-Kartenleser oder
 - ii. kontaktlos mit einem am PS angeschlossenen Standard-Kartenleser.
2. Ein Versicherter nutzt beim mobilen Check-in ein Versichertenendgerät um vom PoPP-Service ein TAN-Set zu erhalten. Das Versichertenendgerät verfügt über einen Standard-Kartenleser mit dem die eGK
 - a. kontaktbehaftet kommuniziert oder
 - b. kontaktlos kommuniziert.

Im Rahmen der Erzeugung eines PoPP-Token verfolgt der PoPP-Service bei der Kommunikation mit einer Smartcard die folgenden Ziele:

1. Der PoPP-Service überzeugt sich, dass es sich bei der Smartcard um eine echte eGK handelt.
2. Der PoPP-Service überzeugt sich, dass die eGK gültig ist.
3. Der PoPP-Service liest aus der eGK Daten aus, die für die Erstellung des PoPP-Token relevant sind.

Die genannten Ziele werden bei kontaktbehafteter Kartenkommunikation mit einer eGK basierend auf [gemSpec_eGK_ObjSys_G2.1] wie folgt erreicht:

1. Der PoPP-Service baut einen Trusted Channel mit der Identität ID.C.eGK.AUT_CVC.E256 auf. Gelingt dies, dann ist die Echtheit der eGK bestätigt.
2. Der PoPP-Service liest innerhalb des Trusted Channels das X.509 Zertifikat aus der Datei EF.C.CH.AUT.E256 aus und überprüft dieses auf Gültigkeit.
3. Der PoPP-Service entnimmt dem ausgelesenen X.509 Zertifikat die für das PoPP-Token notwendigen Informationen.

Die genannten Ziele werden bei kontaktloser Kartenkommunikation mit einer eGK basierend auf [gemSpec_eGK_ObjSys_G2.1](die einen PACE Kanal voraussetzt) wie folgt erreicht:

1. Der PoPP-Service authentisiert die eGK mit der Identität ID.C.eGK.AUT_CVC.E256. Wegen [gemSpec_COS#N107.235)b] ist es nicht möglich dabei einen Trusted Channel zwischen PoPP-Service und eGK zu etablieren.
2. Der PoPP-Service liest aus der eGK das X.509 Zertifikat aus der Datei EF.C.CH.AUT.E256 aus und überprüft dieses auf Gültigkeit. Da der Kommunikationskanal zwischen PoPP-Service und eGK im kontaktlosen Fall nicht Ende-zu-Ende gesichert ist, ist der PoPP-Service nicht ohne weiteres in der Lage zu beurteilen, ob das im präsentierte X.509 Zertifikat von derselben eGK stammt, deren Echtheit er mit der Identität ID.C.eGK.AUT_CVC.E256 überprüft hat. Deshalb konsultiert der PoPP-Service im kontaktlosen Fall eine Datenbank, welche die Frage beantwortet: Stammen das CV-Zertifikat der Echtheitsprüfung und das präsentierte X.509 Zertifikat aus ein und derselben eGK? So eine Datenbank wird in [Kapitel eGK-Hash-Datenbank] beschrieben.
3. Der PoPP-Service entnimmt dem präsentierten X.509 Zertifikat die für das PoPP-Token notwendigen Informationen.

Der PoPP-Service schaltet in der eGK nichts frei und erwartet auch nicht, dass in der eGK etwas freigeschaltet ist, insbesondere weder durch Card-2-Card noch durch eine PIN-Eingabe. Technisch ist dies gleichbedeutend mit der Aussage, dass der PoPP-Service nur solche Kommando APDU an eine eGK sendet, für die im Rahmen der Objektsystemspezifikation die Zugriffsbedingung "ALWAYS" festgelegt ist ("ALWAYS" = jeder, der im Besitz der Karte ist, ist in der Lage diese Operation auszuführen).

Hinweis 1: Im kontaktlosen Fall funktioniert eine sinnvolle Kartenkommunikation mit der eGK nur nach Aufbau eines PACE-Kanals. Weil die dazu notwendige CAN auf der eGK aufgedruckt ist und somit jeder, der im Besitz der eGK ist so einen PACE-Kanal aufzubauen in der Lage ist, wird hier der Einfachheit halber die Etablierung eines PACE-Kanals und die damit verbundene Freischaltung von Funktionalität in der eGK auch unter "ALWAYS" subsumiert.

Hinweis 2: Im kontaktlosen Fall stehen nach Etablierung eines PACE-Kanals dieselben Daten und Funktionen in einer eGK zur Verfügung, wie im kontaktbehafteten Fall unmittelbar nach Stecken einer eGK.

Hinweis 3: Für die Generation 3 einer eGK ist geplant, dass eine eGK G3 eine Identität besitzt, die sich ohne PIN-Eingabe nutzen lässt und deren zugehöriges X.509 Zertifikat alle Informationen enthält, die für ein PoPP-Token relevant ist.

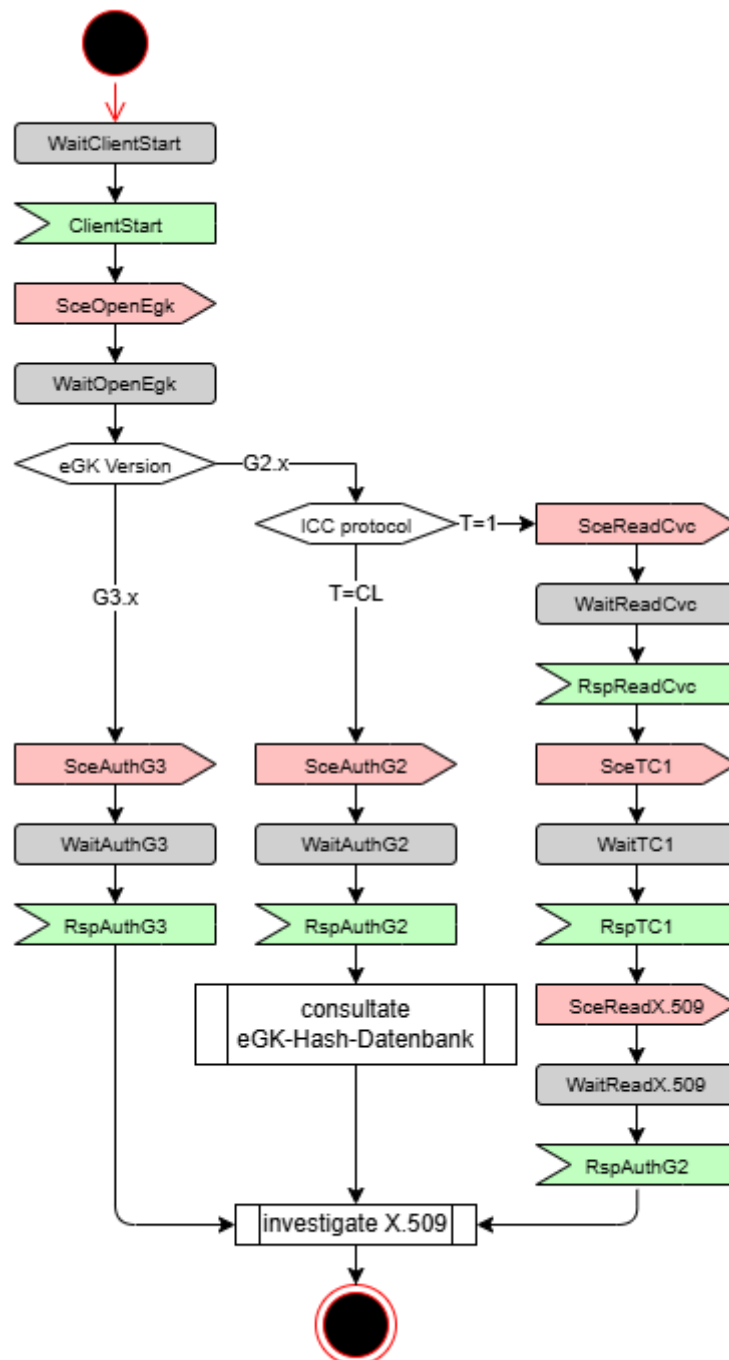


Abbildung 15: Zustandsdiagramm für die Verarbeitung einer eGK

Abbildung "Zustandsdiagramm für die Verarbeitung einer eGK" zeigt das Zustandsdiagramm für die Verarbeitung einer eGK. Der PoPP-Service wartet in jedem der gezeigten Zustände auf den Empfang einer Nachricht. Er bearbeitet die Nachricht, sendet eine passende Nachricht zurück und geht in den Folgezustand über. Berücksichtigt sind die kontaktbehaftete und die kontaktlose Handhabung einer eGK Generation 2.x, sowie die (geplante) Handhabung einer eGK Generation 3 (für welche die Handhabung kontaktbehaftet und kontaktlos identisch ist). Das Zustandsdiagramm berücksichtigt nur Gutfälle. Das bedeutet, Fehlerfälle, Abbrüche und ähnliches sind im abgebildeten Zustandsdiagramm nicht enthalten.

6.2.1.2 Szenario

In diesem Kapitel ist "Szenario" definiert als eine Abfolge von Elementen in einer Liste. Jedes Element beschreibt entweder Statuswörter, die als Gutfall für eine Antwort APDU gewertet werden, oder eine Kommando APDU.

Definition CommandApdu: Eine Kommando APDU gemäß [gemSpec_COS].

Definition ExpectedStatusWord: Eine Menge mit einem oder mehreren Statuswörtern aus [gemSpec_COS].

Definition ScenarioStep: Eine Aggregation von genau einer CommandApdu und einem Objekt ExpectedStatusWord.

Definition Szenario: Eine Liste mit keinem, einem oder mehreren Elementen des Typs ScenarioStep.

A_27000 - PoPP-Service, StandardScenarioMessage

Der PoPP-Service MUSS Objekte vom Typ StandardScenarioMessage generieren so, wie in der Schnittstellspezifikation [I_PoPP_Token_Generation.yaml] beschrieben, wobei das Attribut "steps" ein Szenario ist. [≤]

Hinweis 1: "StandardScenarioMessage.steps" lässt sich auffassen als ein Skript, welches abzuarbeiten ist. Ein "Interpreter" eines "StandardScenarioMessage.steps" wertet das Skript Element für Element aus. Die im Element enthaltene Kommando APDU wird an eine Smartcard gesendet. Falls die korrespondierende Antwort APDU der Smartcard ein Statuswort enthält, welches Element der Menge "ExpectedStatusWord" ist, dann fährt der Interpreter mit dem nächsten Listenelement fort, ansonsten bricht er die Bearbeitung des Skripts ab (Exceptionhandling).

Hinweis 2: Ein "sehr einfacher Interpreter" wird "ExpectedStatusWord" ignorieren und auf die Auswertung der Statuswörter in den Antwort APDU verzichten. So ein Interpreter erkennt keine Fehlerfälle. Im Fehlerfall wird so ein Interpreter ein möglicherweise sehr langes Skript zeitintensiv auch noch dann fortsetzen, wenn ein "intelligenter Interpreter" erkannt hätte, dass ein Fortsetzen wegen eines Fehlers nicht sinnvoll ist.

A_27017 - PoPP-Service, Erlaubnis für abweichende Szenarien

Falls der PoPP-Service Szenarien verwendet, die von den in [gemSpec_PoPP_Service] beschriebenen abweichen, so MUSS der Hersteller des PoPP-Service vor deren Verwendung eine Erlaubnis der gematik einholen. [≤]

Gemäß Abbildung "Systemkontext PoPP-Lösung" schickt der PoPP-Service StandardScenarioMessages entweder an ein PS, wo die Szenarien vom PoPP-Client bearbeitet oder an einen Konnektor weitergeleitet werden, oder an ein anderes Gerät. Hier ist lediglich die Unterscheidung wichtig, ob eine StandardScenarioMessage von einem Konnektor verarbeitet wird oder nicht. Sobald sich ein Gerät mit dem PoPP-Service verbindet, teilt es dem PoPP-Service mit, ob Szenarien von einem Konnektor verarbeitet werden, oder nicht (Property "cardConnectionType" in der "StartMessage").

A_27128 - PoPP-Service, Codierung von Konnektor-Szenarien

Falls der PoPP-Service ein Szenario für einen Konnektor zusammenstellt, dann MUSS er das Szenario in eine ConnectorScenarioMessage gemäß [I_PoPP_Token_Generation.yaml] einstellen. [≤]

A_27129 - PoPP-Service, Codierung von Nicht-Konnektor-Szenarien

Falls der PoPP-Service ein Szenario nicht für einen Konnektor, sondern für ein anderes Gerät zusammenstellt, dann MUSS er das Szenario in eine StandardScenarioMessage gemäß [I_PoPP_Token_Generation.yaml] einstellen. [≤]

6.2.1.3 eGK öffnen

Dieses Kapitel beschreibt, wie ermittelt wird, ob es sich bei der präsentierten Smartcard um eine eGK handelt und welche Version diese hat. Die Vorgehensweise ist unabhängig davon, ob die Smartcard kontaktbehaftet oder kontaktlos betrieben wird. Deshalb wird hier auf eine diesbezügliche Unterscheidung verzichtet.

A_27008 - PoPP-Service, Szenario SceOpenEgk, eGK öffnen

Der PoPP-Service MUSS im ersten Szenario folgende Liste verwenden:

1. Element:
 - a. CommandApdu: '00 a4 040c 07 D2760001448000'
 - b. ExpectedStatusWord: {'9000'}
2. Element:
 - a. CommandApdu: '00 b0 9100 00'
 - b. ExpectedStatusWord: {'9000', '6281'}

[<=]

Hinweis 1: Das erste Listenelement selektiert das Masterfile (MF) einer eGK. Dieses Kommando bringt eine eGK in einen für die nachfolgenden Kommandos definierten Zustand. Antwortet die Smartcard auf dieses Kommando mit einem erwarteten Statuswort, dann handelt es sich um eine eGK (oder um eine Smartcard, die vorgaukelt eine eGK zu sein). Wird irrtümlich eine Karte mit falschem Typ angesprochen (etwa ein HBA oder eine Bankkarte), dann wird das durch ein inakzeptables Statuswort erkannt. Falls eine Karte vorgaukelt eine eGK zu sein, dann wird dies in einem späteren Szenario erkannt.

Hinweis 2: Das zweite Listenelement liest den Inhalt von EF.Version2. Basierend auf den Versionsinformationen ist es möglich eGK unterschiedlicher Generationen zu erkennen, oder beispielsweise wegen Schwachstellen abzulehnen.

Definition: eGKIncludedPtvObjSys ist eine Menge mit Produkttypversionen von eGK Objektsystemen, die der PoPP-Service zu unterstützen hat. Produkttypversionen werden in diese Menge aufgenommen oder aus ihr entfernt, wenn sich die Anforderungslage (also die Vorgaben der gematik) ändern. Basierend auf den Erfahrungen der Vergangenheit ist davon auszugehen, dass sich diese Menge nur wenige Male pro Jahr ändert, während sich die Anzahl zugelassener Kartenprodukte häufiger ändert. Deshalb wird die Menge zulässiger Kartenprodukte über die Produkttypversion definiert.

Definition: eGKexcludedPiObjSys ist eine Menge mit Produktidentifikationen aktiver Objektsysteme, die von der Verwendung durch den PoPP-Service ausgeschlossen werden. Produktidentifikationen der Kartenhersteller werden in diese Menge aufgenommen, wenn es Schwierigkeiten mit einem konkreten Kartenprodukt gibt. Basierend auf den Erfahrungen der Vergangenheit ist davon auszugehen, dass die Mächtigkeit der Menge klein ist und sich nur selten ändert.

A_27018 - PoPP-Service, Zulässige eGK Objektsystemversionen

Der PoPP-Service MUSS Änderungen an der Menge eGKIncludedPtvObjSys, die ihm ausschließlich durch die gematik angezeigt werden, innerhalb von sieben Tagen im Betrieb berücksichtigen.[<=]

A_27019 - PoPP-Service, Unzulässige eGK Objektsystemversionen

Der PoPP-Service MUSS Änderungen an der Menge eGKexcludedPiObjSys, die ihm ausschließlich durch die gematik angezeigt werden, innerhalb von 24 Stunden im Betrieb berücksichtigen. [**<=**]

Hinweis 1: Die Produkttypversion eines Kartenproduktes findet sich in der Datei EF.Version2. Basierend auf der Anforderungslage der gematik besteht die Menge eGKincludedObjSys im Januar 2025 aus folgenden Elementen:

{'040400', '040401', '040500', '040501', '040502', '040600', '040700'}.

Mit Einführung der eGK Generation 3 wird die Menge (laut aktuellem Plan) um den Wert '050000' ergänzt.

Hinweis 2: Die Produktidentifikation des aktiven Objektsystems findet sich in der Datei EF.Version2. Basierend auf dem Kenntnisstand Januar 2025 ist die Menge eGKexcludedObjSys leer.

A_27009 - PoPP-Service, Auswertung SceOpenEgk

Der PoPP-Service MUSS die Kartenantworten auf das Szenario SceOpenEgk wie folgt auswerten:

1. Der Use Case wird mit der Fehlermeldung UnexpectedStatusWordSceOpenEgk beendet, wenn mindestens eine Kartenantwort ein unerwartetes Statuswort enthält.
2. Der Inhalt der Datei EF.Version2 wird gemäß [gemSpec_Karten_Fach_TIP_G2.1#2.1.1] auswerten:
 - a. Falls die Version des aktiven Objektsystems (PT_ObjSys) nicht Element der Menge eGKincludedPtvObjSys ist, dann bricht der Use Case mit der Fehlermeldung InvalidPtvObjectSystem ab.
 - b. Falls die Produktidentifikation des aktiven Objektsystems (PI_ObjSys) Element der Menge eGKexcludedPiObjSys ist, dann bricht der Use Case mit der Fehlermeldung InvalidPiObjectSystem ab.
 - c. Falls die Version des aktiven Objektsystems (PT_ObjSys) eine eGK der
 - i. Generation 2 anzeigt, dann wird im
 - A. kontaktbehafteten Fall mit dem Szenario SceReadCvc aus [A_27001*] fortgefahren.
 - B. kontaktlosen Fall mit dem Szenario SceAuthG2 aus [A_27020*] fortgefahren.
 - ii. Generation 3 anzeigt, dann wird mit dem Szenario SceAuthG3 aus [A_27022*] fortgefahren.

[**<=**]

6.2.1.4 eGK G2 kontaktbehaftet

Dieses Kapitel behandelt die kontaktbehaftete Kommunikation mit einer eGK gemäß [gemSpec_eGK_ObjSys_G2.1]. Dies deckt folgende Anwendungsfälle ab:

1. Versicherter in einer LEI, eGK kontaktbehaftet in einem eH-KT
2. Versicherter in einer LEI, eGK kontaktbehaftet in einem Standard-Kartenleser
3. Versicherter und LE außerhalb einer LEI, LE mit mobilem Endgerät mit PS und kontaktbehaftetem Standard-Kartenleser
4. Versicherter mit Versichertenendgerät am PoPP-Service und kontaktbehaftetem Standard-Kartenleser

Im Gutfall schickt der PoPP-Service drei weitere Szenarien mit jeweils mehreren Kommando APDU an die Karte:

A_27001 - PoPP-Service, Szenario SceReadCvc

Der PoPP-Service MUSS bei kontaktbehafteter Kommunikation mit einer eGK G2 im zweiten Szenario folgende Liste verwenden:

1. Element:
 - a. CommandApdu: '00 b0 8700 00'
 - b. ExpectedStatusWord: {'9000', '6281'}
2. Element:
 - a. CommandApdu: '00 b0 8600 00'
 - b. ExpectedStatusWord: {'9000', '6281'}
3. Element:
 - a. CommandApdu: '80 ca 0100 00 0000'
 - b. ExpectedStatusWord: {'9000'}

[<=]

Hinweis 1: Das erste Listenelement liest den Inhalt von EF.C.CA.CS.E256 mit CVC-Sub-CA aus. Der PoPP-Service benötigt dieses CV-Zertifikat zur Verifikation des End-Entity-CVC (sofern er es nicht aus anderen Quellen bereits kennt).

Hinweis 2: Das zweite Listenelement liest den Inhalt von EF.C.eGK.AUT_CVC.E256 mit dem End-Entity-CVC aus. Der PoPP-Service benötigt dieses CV-Zertifikat für die Berechnung der Sessionkeys.

Hinweis 3: Das dritte Listenelement (LIST PUBLIC KEY) liest die in der Smartcard verfügbaren öffentlichen Schlüssel aus. Basierend auf dieser Liste ist es dem PoPP-Service möglich eine kurze Chain von CV-Zertifikaten zusammenzustellen für den Import seines CV-Authentisierungsschlüssels (siehe Szenario SceTC1). Im besten Fall ist kein CV-Zertifikatsimport erforderlich, weil die eGK bereits über den CV-Authentisierungsschlüssel des PoPP-Service verfügt.

A_27010 - PoPP-Service, Auswertung SceReadCvc

Der PoPP-Service MUSS die Kartenantworten auf das Szenario SceReadCvc wie folgt auswerten:

1. Der Use Case wird mit der Fehlermeldung UnexpectedStatusWordSceReadCvc beendet, wenn mindestens eine Kartenantwort ein unerwartetes Statuswort enthält.
2. Der Use Case wird mit der Fehlermeldung InvalidCaCvc beendet, wenn eine Prüfung des CV-Zertifikates gemäß [gemSpec_COS#(N095.900)b] aus der Datei EF.C.CA.CS.E256 gegen das zugehörige CVC-Root-CA aus der TSL-Liste mit einem Fehler endet, dabei gilt:
 - a. affectedObject aus [gemSpec_COS#(N095.900)b] entspricht dem öffentlichen Signaturprüfschlüssel für das CV-Zertifikat, wie er beispielsweise aus einem CVC-Root-CA entnehmbar ist.
 - b. pointInTime aus [gemSpec_COS] entspricht der lokalen, aktuellen Systemzeit.
3. Der Use Case wird mit der Fehlermeldung InvalidEndEntityCvc beendet, wenn eine Prüfung des CV-Zertifikates gemäß [gemSpec_COS#(N095.900)b] aus der Datei EF.C.eGK.AUT_CVC.E256 mit einem Fehler endet, dabei gilt:
 - a. affectedObject aus [gemSpec_COS#(N095.900)b] entspricht dem öffentlichen Signaturprüfschlüssel für das CV-Zertifikat, wie er beispielsweise aus dem CV-Zertifikat aus der Datei EF.C.CA.CS.E256 entnehmbar ist.
 - b. pointInTime aus [gemSpec_COS] entspricht der lokalen, aktuellen Systemzeit.

4. Dem Antwortdatenfeld auf das LIST PUBLIC KEY Kommando wird eine Liste von Schlüsselreferenzen gemäß [gemSpec_COS#(N099.462)] entnommen und für die Verwendung im Szenario SceTC1 zwischengespeichert.

[<=]

A_27002 - PoPP-Service, Szenario SceTC1

Der PoPP-Service MUSS bei kontaktbehafteter Kommunikation mit einer eGK G2 im dritten Szenario folgende Liste verwenden:

1. Element:
 - a. CommandApdu: '00 22 41A4 06 (84-01-09) || (80-01-54)'
 - b. ExpectedStatusWord: {'9000'}
2. Kein, ein oder mehrere Paare von MSE SET und PSO Verify Certificate Kommandos zum Import des öffentlichen CV-Authentisierungsschlüssels des PoPP-Service. CAR bezeichnet das Feld CAR aus dem zu importierenden CV-Zertifikat, CvcTemplate bezeichnet das Template des zu importierenden CV-Zertifikates.
 - a. Element:
 - i. CommandApdu: '00 22 81 b6 0a (83-08-CAR)'
 - ii. ExpectedStatusWord: {'9000'}
 - b. Element:
 - i. CommandApdu: '00 2a 00 b4 xy CvcTemplate'
 - ii. ExpectedStatusWord: {'9000'}
3. Element:
 - a. CommandApdu: '10 86 0000 10 (7c-0e-(c3-0c-CHR) 00)'
 - b. ExpectedStatusWord: {'9000'}

[<=]

Hinweis 1: Das erste Listenelement ist ein MSE Set Kommando gemäß [gemSpec_COS#(N100.900)] zur Selektion des privaten Schlüssels PrK.eGK.AUT_CVC.E256 für den Algorithmus elcSessionkey4SM. Dieser Schlüssel ist kartenseitig am Aufbau des Trusted Channels beteiligt.

Hinweis 2: Jedes Paar aus MSE Set Kommando und PSO Verify Certificate Kommando importiert einen öffentlichen Schlüssel in die Smartcard.

1. *SceTC1 enthält kein solches Paar, wenn der öffentliche CV-Authentisierungsschlüssel des PoPP-Service bereits in der Smartcard gespeichert ist.*
2. *SceTC1 enthält genau ein solches Paar, wenn der öffentliche Schlüssel zur Verifikation des End-Entity-CVC des PoPP-Service bereits in der Smartcard gespeichert ist: CVC-Chain = End-Entity-CVC.*
3. *SceTC1 enthält genau zwei solche Paare, wenn der öffentliche Root-Schlüssel in der Smartcard gespeichert ist, mit dem sich das CVC-Sub-CA zum End-Entity-CVC des PoPP-Service verifizieren lässt: CVC-Chain = CVC-Sub-CA, End-Entity-CVC.*
4. *SceTC1 enthält genau drei solche Paare, wenn der öffentliche Root-Schlüssel in die Smartcard zu importieren ist, mit dem sich das CVC-Sub-CA zum End-Entity-CVC des PoPP-Service verifizieren lässt: CVC-Chain = Link-CVC-Root, CVC-Sub-CA, End-Entity-CVC.*

5. *SceTC1 enthält mehr als drei solcher Paare, wenn mehr als ein CVC-Root-Schlüssel in die Smartcard zu importieren ist.*

Hinweis 3: MSE Set Kommando gemäß [gemSpec_COS#(N103.300)] zur Selektion eines öffentlichen Signaturprüfchlüssels in der Smartcard. Der Wert CAR entspricht dem Wertfeld des Elementes CAR des CV-Zertifikates, welches im nächsten Kommando importiert wird.

Hinweis 4: PSO VerifyCertificate Kommando gemäß [gemSpec_COS#(N095.410)] zum Import eines CV-Zertifikates. Der Wert CvcTemplate entspricht dem Wertfeld (value-field) des BER-TLV codierten CV-Zertifikates.

Hinweis 5: Das letzte Listenelement ist ein GENERAL AUTHENTICATE Kommando gemäß [gemSpec_COS#(N085.012)]. Dies ist der erste Schritt zur Etablierung eines Trusted Channels zwischen PoPP-Service und Smartcard. Der zweite und letzte Schritt wird in SceReadX.509 ausgeführt.

A_27011 - PoPP-Service, Auswertung SceTC1

Der PoPP-Service MUSS die Kartenantworten auf das Szenario SceTC1 wie folgt auswerten:

1. Der Use Case wird mit der Fehlermeldung UnexpectedStatusWordSceTC1 beendet, wenn mindestens eine Kartenantwort ein unerwartetes Statuswort enthält.
2. Dem Antwortdatenfeld des GENERAL AUTHENTICATE Kommandos wird ein ephemerer, öffentlicher Schlüssel ephemeralPK_eGK gemäß [gemSpec_COS#(N085.052)h] entnommen.

[<=]

A_27003 - PoPP-Service, Szenario SceReadX.509

Der PoPP-Service MUSS bei kontaktbehafteter Kommunikation mit einer eGK G2 im vierten Szenario folgende Liste verwenden:

1. Element:
 - a. CommandApdu: '00 86 0000 xy (7c-xy-(85-xy-ephemeralPK_PoPP-Service))'
 - b. ExpectedStatusWord: {'9000'}
2. Element:
 - a. CommandApdu*: '00 a4 040c 0a a000000167455349474e'
 - b. ExpectedStatusWord: {'9000'}
3. Element:
 - a. CommandApdu*: '00 b0 8400 00 0000'
 - b. ExpectedStatusWord: {'9000', '6281'}

[<=]

Hinweis 1: Das erste Listenelement ist ein GENERAL AUTHENTICATE Kommando gemäß [gemSpec_COS#(N085.016)] mit ephemeralPK_PoPP-Service als ephemere öffentlichen Schlüssel des PoPP-Service. Dies ist der zweite und letzte Schritt zur Etablierung eines Trusted Channels. Der PoPP-Service ist nun in der Lage mit dem von ihm erzeugten ephemeren Schlüsselpaar, seinem privaten CV-Authentisierungsschlüssel und ephemeralPK_eGK aus [A_27011] Sessionkeys gemäß [gemSpec_COS#(N85.054)c] zu berechnen. Alle folgenden Kommandos sind mit den vereinbarten Sessionkeys zu sichern gemäß den Regeln aus [gemSpec_COS#13]. Dies wird in der Anforderung durch einen '*' hinter CommandApdu angedeutet.*

Hinweis 2: Das zweite Listenelement selektiert das Verzeichnis DF.ESIGN. Das Kommando ist in [A_27003] im Klartext notiert. Im real verwendeten Szenario ist es gemäß den Regel aus [gemSpec_COS#13] zu sichern. Die zugehörige Antwort APDU wird von der Smartcard gemäß [gemSpec_COS#13] gesichert.*

Hinweis 3: Das dritte Listenelement liest das X.509 Zertifikat aus der Datei EF.C.CH.AUT.E256. Das Kommando ist in [A_27003] im Klartext notiert. Im real verwendeten Szenario ist es gemäß den Regel aus [gemSpec_COS#13] zu sichern. Die zugehörige Antwort APDU wird von der Smartcard gemäß [gemSpec_COS#13] gesichert.*

A_27006 - PoPP-Service, Szenario mit APDU innerhalb eines Trusted Channels

Sobald der PoPP-Service einen Trusted Channel zu einer Smartcard etabliert hat, MUSS er jede nachfolgende Kommando APDU gemäß den Regeln aus [gemSpec_COS#13] sichern und jede nachfolgende Antwort APDU gemäß den Regeln aus [gemSpec_COS#13] in eine ungesicherte Antwort APDU umwandeln und dabei die ausgehandelten Sessionkeys verwenden. [≤]

A_27013 - PoPP-Service, Auswertung SceReadX.509

Der PoPP-Service MUSS die Kartenantworten auf das Szenario SceReadX.509 wie folgt auswerten:

1. Der Use Case wird mit der Fehlermeldung UnexpectedStatusWordSceReadX.509 beendet, wenn mindestens eine Kartenantwort ein unerwartetes Statuswort enthält.
2. Aus dem Antwortdatenfeld der letzten Antwortnachricht wird ein X.509 Zertifikat erzeugt. Der Use Case wird mit der Fehlermeldung InvalidX509 beendet, wenn die Prüfung dieses Zertifikates gemäß [A_27130*] fehlschlägt.
3. Das CV-Zertifikat aus der Datei EF.C.eGK.AUT_CVC.E256 sowie das X.509 Zertifikat werden der eGK-Hash-Datenbank (siehe [A_27046*]) in der Methode "store(cvc, x509)" übergeben.

[≤]

6.2.1.5 eGK G2 kontaktlos

Dieses Kapitel behandelt die kontaktlose Kommunikation einer eGK gemäß [gemSpec_eGK_ObjSys_G2.1]. Dies deckt folgende Anwendungsfälle ab:

1. Versicherter in einer LEI, eGK kontaktlos in einem eH-KT
2. Versicherter in einer LEI, eGK kontaktlos in einem Standard-Kartenleser
3. Versicherter und LE außerhalb einer LEI, LE mit mobilem Endgerät mit PS und kontaktlosem Standard-Kartenleser
4. Versicherter mit Versichertenendgerät am PoPP-Service und kontaktlosem Standard-Kartenleser

Im Gutfall schickt der PoPP-Service nach dem in [A_27008*] beschriebenen Szenario ein weiteres Szenario mit einer Reihe von Kommando APDU an die Karte:

A_27020 - PoPP-Service, Szenario SceAuthG2

Der PoPP-Service MUSS bei kontaktloser Kommunikation mit einer eGK G2 im zweiten Szenario folgende Liste verwenden:

1. Element:
 - a. CommandApdu: '00 b0 8700 00'
 - b. ExpectedStatusWord: {'9000', '6281'}
2. Element:

- a. CommandApdu: '00 b0 8600 00'
 - b. ExpectedStatusWord: {'9000', '6281'}
3. Element:
 - a. CommandApdu: '00 a4 040c 0a a000000167455349474e'
 - b. ExpectedStatusWord: {'9000'}
4. Element:
 - a. CommandApdu: '00 22 41A4 06 (84-01-09) || (80-01-00)'
 - b. ExpectedStatusWord: {'9000'}
5. Element:
 - a. CommandApdu: '00 b0 8400 00 0000'
 - b. ExpectedStatusWord: {'9000', '6281'}
6. Element:
 - a. CommandApdu: '00 88 0000 10 token 00'
 - b. ExpectedStatusWord: {'9000'}

[<=]

Hinweis 1: Das erste Listenelement liest den Inhalt von EF.C.CA.CS.E256 mit CVC-Sub-CA aus. Der PoPP-Service benötigt dieses CV-Zertifikat zur Verifikation des End-Entity-CVC (sofern er es nicht aus anderen Quellen bereits kennt).

Hinweis 2: Das zweite Listenelement liest den Inhalt von EF.C.eGK.AUT_CVC.E256 mit dem End-Entity-CVC aus. Der PoPP-Service benötigt dieses CV-Zertifikat für die Authentisierung.

Hinweis 3: Das dritte Listenelement selektiert das Verzeichnis DF.ESIGN.

Hinweis 4: Das vierte Listenelement ist ein MSE Set Kommando gemäß [gemSpec_COS#(N100.900)] zur Selektion des privaten Schlüssels PrK.eGK.AUT_CVC.E256 für den Algorithmus elcRoleAuthentication.

Hinweis 5: Das fünfte Listenelement liest das X.509 Zertifikat aus der Datei EF.CH.AUT.E256.

Hinweis 6: Das sechste Listenelement ist ein INTERNAL AUTHENTICATE Kommando gemäß [gemSpec_COS#(N086.400)].

A_27021 - PoPP-Service, Auswertung SceAuthG2

Der PoPP-Service MUSS die Kartenantworten auf das Szenario SceAuthG2 wie folgt auswerten:

1. Der Use Case wird mit der Fehlermeldung UnexpectedStatusWordSceAuthG2 beendet, wenn mindestens eine Kartenantwort ein unerwartetes Statuswort enthält.
2. Der Use Case wird mit der Fehlermeldung InvalidCaCvc beendet, wenn eine Prüfung des CV-Zertifikates gemäß [gemSpec_COS#(N095.900)b] aus der Datei EF.C.CA.CS.E256 gegen das zugehörige CVC-Root-CA aus der TSL-Liste mit einem Fehler endet, dabei gilt:
 - a. affectedObject aus [gemSpec_COS#(N095.900)b] entspricht dem öffentlichen Signaturprüfschlüssel für das CV-Zertifikat, wie er beispielsweise aus einem CVC-Root-CA entnehmbar ist.
 - b. pointInTime aus [gemSpec_COS] entspricht der lokalen, aktuellen Systemzeit.

3. Der Use Case wird mit der Fehlermeldung InvalidEndEntityCvc beendet, wenn eine Prüfung des CV-Zertifikates gemäß [gemSpec_COS#(N095.900)b] aus der Datei EF.C.eGK.AUT_CVC.E256 mit einem Fehler endet, dabei gilt:
 - a. affectedObject aus [gemSpec_COS#(N095.900)b] entspricht dem öffentlichen Signaturprüfchlüssel für das CV-Zertifikat, wie er beispielsweise aus dem CV-Zertifikat aus der Datei EF.C.CA.CS.E256 entnehmbar ist.
 - b. pointInTime aus [gemSpec_COS] entspricht der lokalen, aktuellen Systemzeit.
4. Aus dem Antwortdatenfeld der vorletzten Antwortnachricht wird ein X.509 Zertifikat erzeugt. Der Use Case wird mit der Fehlermeldung InvalidX509 beendet, wenn die Prüfung dieses Zertifikates gemäß [A_27130*] fehlschlägt.
5. Dem Antwortdatenfeld der letzten Antwortnachricht wird eine Signatur entnommen. Die Signatur wird mit dem öffentlichen Schlüssel aus dem CV-Zertifikat aus der Datei EF.C.eGK.AUT_CVC.E256 gegen das token geprüft. Der Use Case bricht mit der Fehlermeldung InvalidAuthentication ab, wenn diese Signaturprüfung fehlschlägt.
6. Die eGK-Hash-Datenbank wird befragt, ob das CV-Zertifikat aus der Datei EF.C.eGK.AUT_CVC.E256 sowie das X.509 Zertifikat aus ein und derselben eGK stammen (siehe Funktion "check(cvc, x509) in [A_27046*]"). Falls die eGK-Hash-Datenbank mit "FALSE" (nein) antwortet, dann wird der Use Case mit der Fehlermeldung UnknownCertificates beendet.

[<=]

6.2.1.6 eGK G3 kontaktbehaftet und kontaktlos

Dieses Kapitel behandelt die kontaktbehaftet und die kontaktlose Kommunikation einer eGK der Generation 3, so wie es Stand Januar 2025 geplant ist. Dies deckt alle Anwendungsfälle aus [Kapitel eGK-Handling, Einführung] ab.

Im Gutfall schickt der PoPP-Service nach dem in [A_27008*] beschriebenen Szenario ein weiteres Szenario mit einer Reihe von Kommando APDU an die Karte:

A_27022 - PoPP-Service, Szenario SceAuthG3

Der PoPP-Service MUSS bei einer Kommunikation mit einer eGK G3 im zweiten Szenario folgende Liste verwenden:

1. Element:
 - a. CommandApdu: '00 a4 040c 0a a0000000167455349474e'
 - b. ExpectedStatusWord: {'9000', '6281'}
2. Element:
 - a. CommandApdu: '00 22 41B6 06 (84-01-91) || (80-01-00)'
 - b. ExpectedStatusWord: {'9000', '6281'}
3. Element:
 - a. CommandApdu: '00 b0 9100 00 0000'
 - b. ExpectedStatusWord: {'9000', '6281'}
4. Element:
 - a. CommandApdu: '00 2a 9e9a xy hashChallenge 00'
 - b. ExpectedStatusWord: {'9000', '6281'}

[<=]

Hinweis 1: Das erste Listenelement selektiert das Verzeichnis DF.ESIGN.

Hinweis 2: Das zweite Listenelement ist ein MSE Set Kommando gemäß [gemSpec_COS#(N102.900)] zur Selektion des privaten Schlüssels PrK.CH.AutU.E256 für den Algorithmus signECDSA.

Hinweis 3: Das dritte Listenelement liest das X.509 Zertifikat aus der Datei EF.CH.AutU.E256.

Hinweis 4: Das vierte Listenelement ist ein PSO Compute Digital Signature Kommando gemäß [gemSpec_COS#(N087.500)] wobei das Kommandodatenfeld einen Hashwert über eine Challenge enthält. Die zugehörige Antwort APDU wird im Erfolgsfall eine Signatur zur Challenge enthalten.

A_27023 - PoPP-Service, Auswertung SceAuthG3

Der PoPP-Service MUSS die Kartenantworten auf das Szenario SceAuthG3 wie folgt auswerten:

1. Der Use Case wird mit der Fehlermeldung UnexpectedStatusWordSceAuthG3 beendet, wenn mindestens eine Kartenantwort ein unerwartetes Statuswort enthält.
2. Aus dem Antwortdatenfeld der vorletzten Antwortnachricht wird ein X.509 Zertifikat erzeugt.
3. Die Signatur im Antwortdatenfeld der letzten Antwortnachricht wird mit dem Signaturprüf Schlüssel aus dem X.509 Zertifikat geprüft. Der Use Case wird mit der Fehlermeldung InvalidAuthentication beendet, wenn die Signaturprüfung oder die Prüfung des X.509 Zertifikates gemäß [A_27130*] fehlschlägt.

[<=]

6.2.1.7 Prüfung des X.509 Zertifikates einer eGK

In [A_27013*], [A_27021*] und [A_27023*] wird gefordert, dass der PoPP-Service das aus einer eGK ausgelesene X.509 Zertifikat zu prüfen hat. Dies geschieht wie folgt:

A_27130 - PoPP-Service, Prüfen von X.509 Zertifikaten einer eGK

Der PoPP-Service MUSS das aus einer eGK ausgelesene X.509 Zertifikat in Anlehnung an [gemSpec_PKI#TUC_PKI_018] mit den folgenden Eingangsparametern prüfen:

1. x509: das zu prüfende Zertifikat,
2. referenceTime: die aktuelle Systemzeit als Referenzzeitpunkt,
3. policyList = {policyIdentifier = <oid_egk_aut>},
4. keyUsage = digitalSignature,
5. extendedKeyUsage = {keyPurposeld = id-kp-clientAuth},
6. ocspGracePeriod = default ,
7. offlineModus = nein,
8. beigefügteOcspResponse: entfällt,
9. timeoutParameter = 10 Sekunden,
10. TOLERATE_OCSP_FAILURE = false,
11. prüfModus = OCSP.

Zu beachten ist A_23225*, wobei die Gültigkeitsdauer D auf 12 Stunden zu setzen ist.

[<=]

Hinweis: Der OCSP-Responder des TSP eGK ist im Internet erreichbar. Die Adresse des OCSP-Responders ist dem Authority Information Access (AIA) des eGK-Zertifikats zu entnehmen.

6.2.1.8 eGK-Handling Fehlercodes

In den vorherigen Kapiteln zum eGK-Handling werden diverse Fehlermeldungen definiert. Dabei ist es das Ziel für jede Stelle, an der ein Fehler detektierbar ist, eine eigene Fehlermeldung zu definieren, für den Fall, dass es an der Außenschnittstelle relevant ist. Derart aussagekräftige Fehlermeldungen unterstützen in der Entwicklungs- und Testphase das Debugging. Für den realen Betrieb ist zweifelhaft, ob aussagekräftige Fehlermeldungen sinnvoll sind. Mitunter wird gewünscht einem Angreifer nicht zu viel darüber zu verraten, an welcher Stelle genau sein Angriff scheiterte. Konkret auf das eGK-Handling bezogen ist es aus Sicht menschlicher Nutzer eher so, dass eine eGK sich eignet um ein PoPP-Token zu erstellen, oder eben nicht. Die Tabelle in diesem Kapitel weist jeder (internen) Fehlermeldung des PoPP-Service eine Fehlermeldung zu, die an der Außenschnittstelle am Interface [I_PoPP-Token_Generation.yaml] oder [I_PoPP_CheckIn_ResourceServer.yaml] sichtbar sind.

A_27049 - PoPP-Service, Mapping von Smartcard Fehlercodes

Der PoPP-Service MUSS interne Fehlermeldungen während des eGK-Handlings auf folgende an Außenschnittstellen sichtbare Fehlermeldungen abbilden:

Tabelle 18: Fehlermeldungen eGK-Handling

Interne Fehlermeldung	Fehlermeldung Außenschnittstelle
InvalidAuthentication	ErrorEgkHandling
InvalidCaCvc	ErrorEgkHandling
InvalidEndEntityCvc	ErrorEgkHandling
InvalidPiObjectSystem	ErrorEgkHandling
InvalidPtvObjectSystem	ErrorEgkHandling
InvalidAuthentication	ErrorEgkHandling
InvalidX509	ErrorEgkHandling
UnexpectedStatusWordSceAuthG2	ErrorEgkHandling
UnexpectedStatusWordSceAuthG3	ErrorEgkHandling
UnexpectedStatusWordSceOpenEgk	ErrorEgkHandling
UnexpectedStatusWordSceReadCvc	ErrorEgkHandling
UnexpectedStatusWordSceReadX.509	ErrorEgkHandling

UnexpectedStatusWordSceTC1	ErrorEgkHandling
UnknownCertificates	ErrorEgkHandling

[<=]

6.2.1.9 eGK-Hash-Datenbank

Die "eGK-Hash-Datenbank" im PoPP-Service beantwortet die Frage: "Stammt ein vorgelegtes CV-Zertifikat und ein vorgelegtes X.509 Zertifikat aus ein und derselben eGK?"

So eine eGK-Hash-Datenbank wird im PoPP-Service für eGK der Generation 2.x für den Fall benötigt, dass die eGK kontaktlos kommuniziert. Die einfachste Art der technischen Umsetzung wäre eine (mathematische) Funktion, die jedem CV-Zertifikat genau ein X.509 Zertifikat zuordnet. Softwaretechnisch wäre das eine Tabelle (in Java ein Map). In dem Fall enthielte die Tabelle personenbezogene Daten, was weder datensparsam noch datenschutzfreundlich wäre. Stattdessen verwendet die eGK-Hash-Datenbank eine Menge `setEgkHashes`, wobei jedes Element der Menge ein SHA-256 Hashwert über die Konkatenation von CV-Zertifikat und X.509 Zertifikat ist. Wenn der eGK-Hash-Datenbank dann ein Pärchen aus CV-Zertifikat und X.509 Zertifikat präsentiert wird, beantwortet die eGK-Hash-Datenbank letztendlich die Frage: "Ist der zugehörige SHA-256 Hashwert für das vorgelegte CV-Zertifikat und X.509 Zertifikat Element der Menge?"

Überlegungen zum Mengengerüst: Es gibt (Stand Januar 2025) fast 75 Millionen gesetzlich Versicherte mit eGK Generation 2.x. Es ist davon auszugehen, dass die Anzahl "nicht abgelaufener eGK" darüber liegt, weil es Versicherte gibt, die über mehr als eine "nicht abgelaufene eGK" verfügen, beispielsweise Ersatz für defekte eGK oder infolge eines Kassenwechsels. Hier wird geschätzt, dass die eGK-Hash-Datenbank so zu dimensionieren ist, dass die Mächtigkeit der Menge `setEgkHashes` bis zu 100.000.000 (100 Millionen) reicht. 100 Millionen SHA-256 Werte beanspruchen netto 3.200 Millionen Byte, also 3,2 Gigabyte rund 3 Gibi Byte. Das ist eine Größenordnung, die für eine moderne Infrastruktur keine besonderen Ansprüche stellt.

Überlegungen zur Befüllung der Menge `setEgkHashes`: Ein neues Element wird der Menge `setEgkHashes` hinzugefügt, wenn ein KTR (oder dessen Dienstleister) das neue Element dem PoPP-Service mitteilt, oder wenn eine eGK Generation 2.x kontaktbehaftet vom PoPP-Service angesprochen wird (lazy-initialization, siehe [A_27013*]). Bei der Anlieferung von Elementen für die Menge `setEgkHashes` verwendet der KTR (oder dessen Dienstleister) eine mTLS Verbindung und übermittelt die Elemente als signierte Nachricht.

Überlegungen zum Entfernen von Elementen aus `setEgkHashes`: Es ist nicht vorgesehen, dass KTR (oder deren Dienstleister) in der Lage sind das Entfernen eines Elementes aus `setEgkHashes` zu veranlassen. Stattdessen ist vorgesehen, dass jedem Element ein Verfallsdatum zugeordnet ist, welches sich aus dem Element "notAfter" aus dem X.509 Zertifikat ergibt. Die eGK-Hash-Datenbank ist damit in der Lage "abgelaufene" Elemente aus der Menge `setEgkHashes` zu entfernen. Die eGK-Hash-Datenbank wird nicht dazu verpflichtet "abgelaufene" Elemente aus der Menge `setEgkHashes` zu entfernen. Falls die eGK-Hash-Datenbank in der Lage ist auch mit einer sehr großen Anzahl an Elementen in `setEgkHashes` umzugehen, dann ist ein Entfernen "abgelaufener" Werte auch nicht erforderlich. Die eGK-Hash-Datenbank beantwortet ja nur die Frage ob ein vorgelegtes Pärchen aus einer eGK stammt, nicht aber, ob das X.509 Zertifikat des Pärchens noch gültig ist. Die Frage "ist ein X.509 Zertifikat noch gültig?" wird nicht von der eGK-Hash-Datenbank, sondern an anderer Stelle beantwortet (siehe Prüfung des X.509 Zertifikats in [A_27130*]).

Definition listImportClients: Die Liste *listImportClients* enthält Identitäten, die der PoPP-Service akzeptiert, wenn diese als Client eine mTLS Verbindung aufbauen zum Zweck des Imports von Hashwerten in die eGK-Hash-Datenbank.

Definition listSignatureVerificationKeys: Die Liste *listSignatureVerificationKeys* enthält Identitäten, die der PoPP-Service akzeptiert, wenn diese signierte Nachrichten zum Zweck des Imports von Hashwerten an die eGK-Hash-Datenbank übermitteln.

A_27043 - Mindestanzahl von Hashwert Lieferanten

Der PoPP-Service MUSS für *listImportClients* und *listSignatureVerificationKeys* mindestens 20 Elemente pro Liste unterstützen. [\leq]

Hinweis: Die Liste listImportClients erhält der Anbieter des PoPP-Service direkt vom jeweiligen Kassen-Dienstleister und die Liste listSignatureVerificationKeys wird dem Hersteller des PoPP-Service von der gematik zur Verfügung gestellt (vgl. [A_27153]).*

A_27044 - PoPP-Service, Schnittstelle I_PoPP_EHC_CertHash_Import

Der PoPP-Service MUSS über eine Schnittstelle I_PoPP_EHC_CertHash_Import mit folgenden Eigenschaften verfügen:

1. Die Schnittstelle I_PoPP_EHC_CertHash_Import ist aus dem Internet erreichbar.
2. Die IP-Adresse über welche die Schnittstelle I_PoPP_EHC_CertHash_Import erreichbar ist wird bekanntgegeben.
3. Änderungen an der IP-Adresse für die Schnittstelle I_PoPP_EHC_CertHash_Import werden mindestens 30 Tage vor der Änderung allen Inhabern der Identitäten aus der Liste listImportClients bekanntgegeben.
4. Die Schnittstelle I_PoPP_EHC_CertHash_Import ist erst nach einem TLS-Handshake nutzbar. Der TLS-Handshake lässt ausschließlich Ciphersuiten gemäß [gemSpec_Krypt] zu. Der TLS-Handshake scheitert, wenn die Identität des Clients nicht Element der Liste listImportClients ist.
5. Über die Schnittstelle I_PoPP_EHC_CertHash_Import wird (nach dem TLS-Handshake auf Applikationsebene) eine oder mehrere signierte Nachrichten mit Hashwerten für die eGK-Hash-Datenbank übertragen (siehe [A_27046*] signedMessage).
6. Ein über die Schnittstelle importierter Hashwert ist spätestens nach 36 Stunden in der Menge setEgkHashes der eGK-Hash-Datenbank enthalten.

[\leq]

A_27045 - PoPP-Service, Hashwert Lieferant

Ein KTR (oder dessen Dienstleister) MUSS die Schnittstelle I_PoPP_EHC_CertHash_Import wie folgt bedienen:

1. Seine Identität für den TLS-Handshake wird dem Anbieter PoPP-Service bekanntgegeben.
2. Seine Identität zur Prüfung von Signaturen wird der gematik bekanntgegeben.
3. Für neu produzierte eGK wird deren Hashwert spätestens 36 Stunden vor Auslieferung der eGK an den PoPP-Service übertragen.
4. Nach einem TLS-Handshake werden bis zu einem "close_notify"-Alert nicht mehr als 100.000.000 Hashwerte übertragen.
5. Die zu signierende Nachricht messageToBeSigned besitzt folgende ASN.1 Struktur:
messageToBeSigned ::= SEQUENCE {
 version INTEGER
 egkInfos SEQUENCE OF egkInfo (SIZE(1..100000000))
}
egkInfo ::= SET {

```
        notAfter UTF8String (SIZE(4)), -- YYYY, excerpt from X.509
    "notAfter"
        hashvalue OCTET STRING
    }
```

6. Die zu signierende Nachricht `messageToBeSigned` wird DER codiert.
7. Als Versionsnummer wird der Wert 0 verwendet.

[<=]

A_27046 - PoPP-Service, eGK-Hash-Datenbank

Der PoPP-Service MUSS über eine eGK-Hash-Datenbank mit folgenden Eigenschaften verfügen:

1. Die eGK-Hash-Datenbank besitzt eine Menge `setEgkHashes`.
2. Die eGK-Hash-Datenbank ist in der Lage in der Menge `setEgkHashes` mindestens 100.000.000 SHA-256 Hashwerte und ein zum jeweiligen Hashwert gehörendes Ablaufdatum zu speichern.
3. Die eGK-Hash-Datenbank besitzt eine Funktion mit der Signatur `"boolean check(cvc, x509)"`:
 - a. Der Parameter `"cvc"` ist ein Bytestring, dessen Inhalt identisch ist zum Inhalt der Datei `EF.C.eGK.AUT_CVC.E256` einer eGK.
 - b. Der Parameter `"x509"` ist ein Bytestring, dessen Inhalt identisch ist zum Inhalt der Datei `EF.C.CH.AUT.E256` einer eGK.
 - c. Die Funktion `check(. . .)` berechnet den SHA-256 Hashwert gemäß [FIPS PUB 180-4] aus der Konkatenation der Parameter `cvc` und `x509`: $hash = SHA-256(cvc || x509)$. Falls der so berechnete Wert `hash` Element von `setEgkHashes` ist, dann gibt die Funktion den booleschen Wert `"TRUE"` (ja) zurück, andernfalls `"FALSE"` (nein).
4. Die eGK-Hash-Datenbank besitzt eine Methode mit der Signatur `"void store(cvc, x509)"`:
 - a. Der Parameter `"cvc"` ist ein Bytestring, dessen Inhalt identisch ist zum Inhalt der Datei `EF.C.eGK.AUT_CVC.E256` einer eGK.
 - b. Der Parameter `"x509"` ist ein Bytestring, dessen Inhalt identisch ist zum Inhalt der Datei `EF.C.CH.AUT.E256` einer eGK.
 - c. Die Methode `store(. . .)` berechnet den SHA-256 Hashwert gemäß [FIPS PUB 180-4] aus der Konkatenation der Parameter `cvc` und `x509`: $hash = SHA-256(cvc || x509)$. Dem Parameter `x509` wird ein Wert `"notAfter"` gemäß [RFC 5280#4.1.2.5] entnommen. Der Hashwert `hash` wird der Menge `setEgkHashes` hinzugefügt und diesem Hashwert `hash` wird das Jahr und der Monat aus `"notAfter"` als Ablaufdatum zugeordnet.
5. Die eGK-Hash-Datenbank besitzt eine Methode mit der Signatur `"void import(signedMessage)"`. Die Method führt folgende Schritte aus:
 - a. Schritt 1: Die Methode prüft die Signatur im Parameter `signedMessage` anhand einer List `listSignatureVerificationKeys`. Falls die Signatur ungültig ist, dann bricht die Methode ab, sonst fährt sie mit dem nächsten Schritt fort.
 - b. Schritt 2: Die Methode entnimmt dem Parameter `signedMessage` die darin enthaltene Nachricht `"messageToBeSigned"`.
 - c. Schritt 3: Die in der Nachricht `messageToBeSigned` enthaltenen Hashwerte und deren jeweiliges Ablaufdatum werden der Menge `setEgkHashes` hinzugefügt.

6. Wenn über die Methoden "store(cvc, x509)" oder "import(signedMessage)" mehr Hashwerte angeliefert werden, als in der Menge setEgkHashes speicherbar sind, dann werden zusätzliche Hashwerte ignoriert.

[<=]

Hinweis 1: Es ist nicht erforderlich, dass die eGK-Hash-Datenbank für jeden Hashwert individuell ein Ablaufdatum speichert. Es ist beispielsweise möglich einem Ablaufdatum eine Menge von Hashwerten zuzuordnen. Der Speicher der eGK-Hash-Datenbank enthält dieses Ablaufdatum dann nur einmal.

Hinweis 2: Aus Sicherheitsgründen ist es erforderlich, dass ein in setEgkHashes gespeicherter Hashwert nicht einem konkreten X.509 Zertifikat zuzuordnen ist. Deshalb enthält das Ablaufdatum in der eGK-Hash-Datenbank nicht den vollständigen Wert "notAfter" aus dem X.509 Zertifikat, sondern lediglich dessen Jahr und Monat.

Hinweis 3: Jedes technische System hat eine Speichergrenze. Das Ignorieren von Hashwerten, die sich nicht mehr speichern lassen, verhindernd undefinierte Zustände durch Speicherüberlauf.

Hinweis 4: Sowohl CV-Zertifikate, als auch X.509 Zertifikate verwenden aktuell SHA-256 als Hashverfahren. Deshalb ist es aus Sicherheitssicht ausreichend in setEgkHashes ebenfalls SHA-256 Werte zu speichern. Insgesamt gibt es $2^{256} = 1,16 \times 10^{77}$ verschiedene SHA-256 Hashwerte. Angenommen jedem dieser Hashwerte wird ein Volumen zugeordnet, wie es ein Coronavirus einnimmt, dann käme im Mittel pro Würfel mit einer Kantenlänge von zwei Lichtjahren ein Coronavirus. Das bedeutet, dass die Menge setEgkHash im Vergleich zu allen möglichen Werten so dünn besetzt ist, dass es für einen Angreifer praktisch unmöglich ist ein Pärchen aus gültigem CV-Zertifikat und gültigem X.509 Zertifikat zu finden, das nicht aus ein und derselben eGK stammt, aber trotzdem von der eGK-Hash-Datenbank eine "ja"-Antwort bekommt.

Hinweis 5: Die Codierung von "signedMessage" wird derzeit mit den Kostenträgern und deren Dienstleistern abgestimmt.

A_27201 - PoPP-Service - eGK-Hash-Datenbank Aspekte für Produktgutachten

Der Hersteller des PoPP-Service MUSS die Umsetzung von:

- Schritt 1 der Methode "void import(signedMessage)" aus [A_27046*] (Signaturprüfung und Abbruch im Fehlerfall) und
- Schritt 4 aus [A_27044*] (Client-Authentisierung gegen listImportClients im TLS-Handshake und Abbruch im Fehlerfall),

im Rahmend des Produktgutachtens prüfen lassen.**[<=]**

6.2.2 Zugriffsautorisierung und Business-Logik

Bei mobilen Szenarien, wie "online Check-in", "online Apotheke" oder "Anmeldung Videosprechstunde" muss der Zugriff eines Anwendungsfrontends (App mit integriertem PoPP-Modul) autorisiert werden.

Die Zugriffsautorisierung erfolgt auf der Basis von Client-Identifikation und Nutzerauthentisierung. Die Prüfung der Nutzerauthentisierung wird entweder durch die Authentifizierung des Versicherten mit seiner GesundheitsID oder durch eGK realisiert.

Beim Verbindungsaufbau zwischen Client und PoPP-Service an Schnittstellen zum Internet wird ein API-KEY übermittelt, welcher durch den PoPP-Service an der Web-Schnittstelle auf Zulässigkeit geprüft wird.

API-KEYs werden durch die gematik in ihrer Rolle als Gesamtverantwortlicher der TI erzeugt. Sie sind Zufallswerte mit hoher Entropie und produkt-spezifisch. Die

Zulässigkeit von API-KEYs wird von der gematik über organisatorische Prozesse dem Betreiber des PoPP-Service und den Herstellern von Clientsystemen mitgeteilt. Die Übermittlung muss vertraulichkeits- und integritätsgeschützt erfolgen. Die gematik muss bei der Übergabe des API-KEY sicherstellen, dass nur ein berechtigter Client-Hersteller einen für ihn erzeugten API-KEY erhält.

Die Veranlassung zur Sperrung eines API-KEYs erfolgt durch die gematik.

Das Ergebnis der Zugriffsautorisierung ist je nach Verfahren:

1. ein "eHealth-ID-check" Access Token bei einer Zugriffsautorisierung mit GesundheitsID oder
2. ein "card-check" Access Token bei einer Zugriffsautorisierung mit eGK(mobil).

Die ausgestellten Access Token unterscheiden sich im Inhalt der transportierten Informationen. Die Access Token berechtigen ein PoPP-Modul zum Zugriff auf die fachlichen Schnittstellen des PoPP-Service zum Erhalt von TAN.

Unter Einsatz der TAN erhalten PS authentifizierter LEI einen Nachweis des Versorgungskontextes in Form eines PoPP-Token.

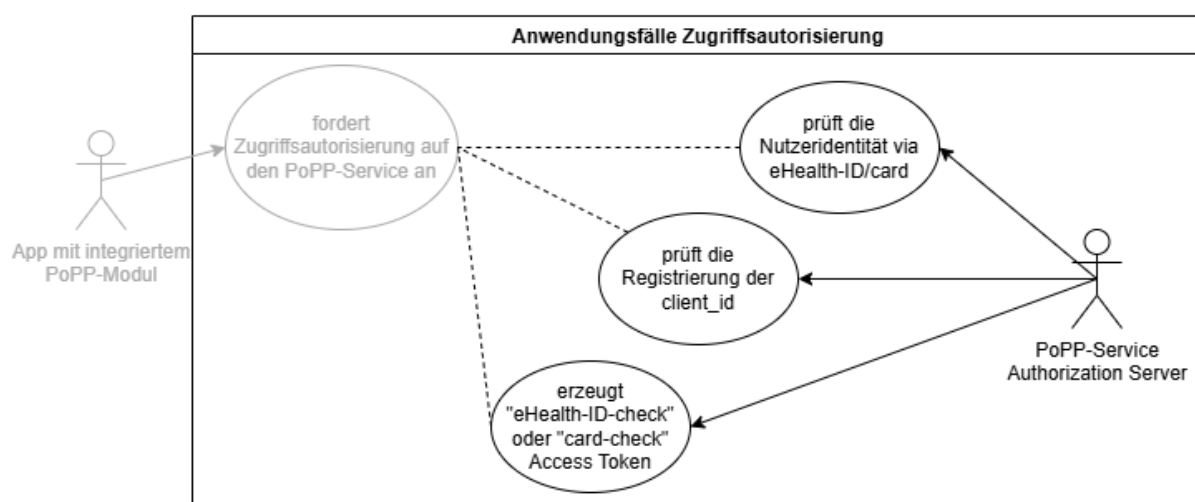


Abbildung 16: Anwendungsfälle des PoPP-Service Authorization Server bei der Zugriffsautorisierung eines in eine App integrierten PoPP-Moduls

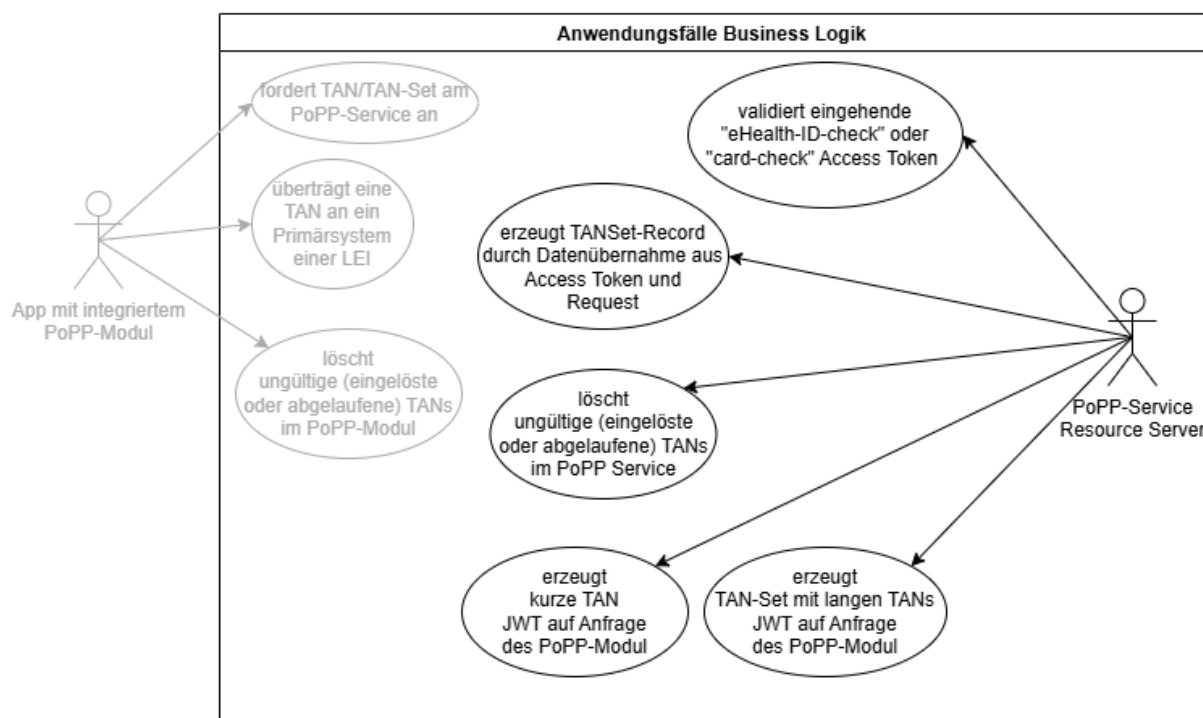


Abbildung 17: Anwendungsfälle des PoPP-Service Resource Server beim Zugriff eines in eine App integrierten PoPP-Moduls

A_27349 - PoPP-Service - Prozess zur Verwaltung von API-KEYs

Der Anbieter des PoPP-Service MUSS organisatorische Prozesse mit der gematik zur Verwaltung von API-KEYs für die Schnittstellen des PoPP-Service zum Internet unterstützen. [≤]

Mittels dieser Prozesse werden zulässige API-KEYs übermittelt und API-KEYs als ungültig erklärt.

A_27350 - PoPP-Service - Zuordnung Abfrageursprung Client (Prüfung API-KEY)

Der PoPP-Service Authorization Server und Resource Server MÜSSEN jeden Versichertenzugriff über eine Schnittstelle im Internet mittels dem HTTP-Header "X-api-key" gegen die Liste zulässiger API-KEYs prüfen. Anfragen ohne HTTP-Header "X-api-key" oder mit einem ungültigen API-KEY MÜSSEN als nicht authentisiert (HTTP-Statuscode 401) abgelehnt werden. [≤]

6.2.2.1 Validierung der Access Token

A_27133 - PoPP-Service - Validierung der Access Token

Der PoPP-Service MUSS die Signatur eines "eHealth-ID-check" Access Token oder "card-check" Access Token prüfen, welches ein PoPP-Modul bei jedem Request im Authorization-Header mitgibt. Das Access Token muss mit einem gültigen Schlüssel des PoPP-Service Authorization Server signiert sein. [≤]

A_26569 - PoPP-Service - Datenübernahme aus "eHealth-ID-check" Access Token und Speicherung in einem TANSet-Record

Der PoPP-Service MUSS sicherstellen, dass die im "eHealth-ID-check" Access Token verschlüsselten Daten KVNR, IK-Nummer, Client-Info und Telematik-ID entschlüsselt und in einem TANSet-Record Datensatz gespeichert werden.

Als proofMethod ist die in [I_PoPP-Token_Generation.yaml] spezifizierte Nachweismethode für die GesundheitsID zu verwenden. [≤]

A_27132 - PoPP-Service - Datenübernahme aus "card-check" Access Token und Speicherung in einem TANSet-Record

Der PoPP-Service MUSS sicherstellen, dass die im "card-check" Access Token verschlüsselten Client-Info und Telematik-ID entschlüsselt und in einem TANSet-Record Datensatz zusammen mit der aus der eGK ausgelesenen KVNR und IK-Nummer gespeichert werden. Als proofMethod ist die in [I_PoPP-Token_Generation.yaml] spezifizierte Nachweismethode für die eGK(mobil) zu verwenden. [≤]

6.2.2.2 TAN-Set, "lange" und "kurze" TAN

Für das Einlösen von TAN gegen PoPP-Token sind zwei unterschiedliche Typen von TAN vorgesehen. Für Anwendungsfälle mit einem Bezug zu einer konkreten Telematik-ID und somit einer LEI wird eine "kurze" menschenlesbare TAN generiert.

Für Anwendungsfälle, wo es zum Zeitpunkt der TAN-Erstellung keinen Bezug zu einer konkreten Telematik-ID und somit einer LEI gibt, wird ein TAN-Set mit "langer" TAN generiert.

A_26567 - PoPP-Service - Erstellung einer TAN bzw. eines TAN-Sets

Der PoPP-Service MUSS sicherstellen, dass auf Anfrage eines PoPP-Moduls ein TAN-Set erstellt und zum TANSet-Records gespeichert wird. Sendet das PoPP-Modul im Anfrage-Request die Telematik-ID einer LEI als Parameter mit, so MUSS der PoPP-Service sicherstellen, dass eine "kurze" TAN mit eindeutigem Bezug zur Telematik-ID erzeugt und im TANSet-Record gespeichert wird. Sendet das PoPP-Modul im Anfrage-Request keine Telematik-ID einer LEI mit, so MUSS der PoPP-Service sicherstellen, dass ein TAN-Set bestehend aus einer Anzahl von "langen" TANs erzeugt und im TANSet-Record gespeichert wird. Die Anzahl der zu generierenden TANs MUSS ein Konfigurationsparameter des PoPP-Service sein.

Der PoPP-Service MUSS sicherstellen, dass TAN bzw. TAN-Set an das aufrufende PoPP-Modul in Form eines JWT zurückgegeben wird. [≤]

Hinweis: Der Defaultwert für die Anzahl der "langen" TAN eines TAN-Sets beträgt drei.

A_27136 - PoPP-Service - Anforderung an die Generierung einer "langen" TAN

Der PoPP-Service MUSS sicherstellen, dass eine "lange" TAN eine zufällig generierte 40-stellige numerische Zeichenkette ist, deren Wert in keiner anderen, aktuell gültigen "langen" TAN entspricht. [≤]

Hinweis 1: Dezimal numerische Zeichenketten lassen sich leicht in QR-Codes umwandeln.

Hinweis 2: 40 dezimale Ziffern entsprechen rund 132,9 bit Entropie.

A_27137 - PoPP-Service - Löschung von "langen" TAN

Der PoPP-Service MUSS sicherstellen, dass ungültige "lange" TAN unmittelbar aus dem System gelöscht werden. TAN sind ungültig, wenn sie bereits zur Erstellung eines PoPP-Token verwendet wurden oder wenn der Gültigkeitsdauer expirationTime des TANSet-Record überschritten ist. [≤]

A_27372 - PoPP-Service - Gültigkeitsdauer einer TAN bzw. eines TAN-Set

Der PoPP-Service MUSS sicherstellen, dass der Gültigkeitszeitraum einer TAN bzw. eines TAN-Sets dem Gültigkeitszeitraum des zugeordneten TANSet-Record entspricht. [≤]

Hinweis: Die Anforderungen an den Gültigkeitszeitraum des TANSet-Record sind in A_27328 festgelegt.*

A_27134 - PoPP-Service - Anforderung an die Generierung einer "kurzen" TAN

Der PoPP-Service MUSS sicherstellen, dass eine "kurze" TAN eine zufällige generierte 6-stellige dezimal numerische Zeichenkette ist. Der PoPP-Service MUSS dabei sicherstellen, dass die "kurze" TAN einer konkreten Leistungserbringerinstitution (Telematik-ID) zugeordnet und eindeutig über alle ausgegebenen aktuell gültigen TAN zu dieser Leistungserbringerinstitution ist. [≤]

A_27135 - PoPP-Service - Löschung einer "kurzen" TAN

Der PoPP-Service MUSS sicherstellen, dass eine abgelaufene oder eingelöste "kurze" TAN für eine Leistungserbringerinstitution unmittelbar im PoPP-Service gelöscht wird. [≤]

6.2.2.3 TANSet-Record

A_26571 - PoPP-Service - Erstellung eines TANSet-Record

Der PoPP-Service MUSS sicherstellen, dass nach Nachweiserbringung mit eGK oder GesundheitsID ein TANSet-Record Datensatz mit folgenden Daten erstellt und gespeichert wird:

Tabelle 19: Dateninhalte TANSet-Record

Datenfeld	Beschreibung
tanSet	Das TANSet wird in Abhängigkeit der Eingangsparameter generiert und kann die folgenden Ausprägungen haben: <ol style="list-style-type: none"> genau eine "lange" TAN, wenn die Telematik-ID gesetzt ist und keine "kurze" TAN vom PoPP-Modul angefordert wurde, genau eine "kurze" TAN, wenn die Telematik-ID gesetzt ist und eine "kurze" TAN vom PoPP-Modul angefordert wurde, ein festgelegte Anzahl von "langen" TAN, wenn keine Telematik-ID gesetzt ist.
patientId	KVNR - Kassenversichertennummer des Patienten
insurerId	IK-Nummer der Krankenversicherung
telematikID	Telematik-ID einer LEI, für welche das TAN-Set ausgestellt ist (optional).
patientProofTime	Zeitpunkt des Nachweises der Anwesenheit des Patienten
expirationTime	Zeitpunkt Ablauf der Gültigkeit des TANSet-Records.
proofMethod	Methode mit der die Anwesenheit des Patienten nachgewiesen wurde. Die zulässigen Werte für GesundheitsID und eGK(mobil) sind in [I_PoPP_Token_Generation.yaml] spezifiziert.

[≤]

A_27328 - PoPP-Service - Gültigkeitsdauer eines TANSet-Record

Die Gültigkeitsdauer eines TANSet-Record berechnet sich aus dem Zeitpunkt des Nachweises der Anwesenheit des Patienten (patientProofTime) und dem Zeitpunkt

Ablauf der Gültigkeit des TANSet-Records (expirationTime). Die Gültigkeitsdauer eines TANSet-Record MUSS ein Konfigurationsparameter des PoPP-Service sein. [≤]

Hinweis: Der Defaultwert für die expirationTime **beträgt 48h**.

A_27314 - PoPP-Service - Schnittstellen des PoPP-Service Resource Server

Für Client-Systeme, deren Zugriff auf den PoPP-Service via Internet erfolgt, MUSS der PoPP-Service Resource Server die Anwendungsfälle:

- PoPP-Service - Datenübernahme aus "eHealthID-check" Access Token und Speicherung in einem TANSet-Record ,
- PoPP-Service - Datenübernahme aus "card-check" Access Token und Speicherung in einem TANSet-Record ,
- PoPP-Service - Validierung der Access Token ,
- PoPP-Service - Anforderung an die Generierung einer "langen" TAN ,
- PoPP-Service - Löschung von "langen" TANs ,
- PoPP-Service - Anforderung an die Generierung einer "kurzen" TAN ,
- PoPP-Service - Löschung einer "kurzen" TAN ,
- PoPP-Service - Erstellung einer TAN bzw. eines TAN-Sets ,
- PoPP-Service - Erstellung eines TANSet-Record ,

unterstützen und dabei für die Client Anfrage nach TAN die Operationen zum Erhalt dieser TAN gemäß [I_PoPP_Checkin_ResourceServer.yaml] bereitstellen.

[≤]

6.2.3 Schnittstelle für Token Abrufe

Die technische Spezifikation der Schnittstelle I_PoPP_Token_Generation zum Abruf von PoPP-Token durch Clientsysteme veröffentlicht die gematik auf GitHub im OpenAPI-Format.

Zusätzlich gelten die folgenden Anforderungen.

A_26345 - PoPP-Service - WebSocket Interface zur PoPP-Token-Erstellung EHC

Der PoPP-Service MUSS sicherstellen, dass die Schnittstellen I_PoPP_Token_Generation zum Abruf von PoPP-Token bei Nutzung der eGK in einer LEI als WebSocket-Interface mit den Endpunkten gemäß der Schnittstellen-Spezifikation in [I_PoPP_Token_Generation.yaml] umgesetzt ist. [≤]

A_27376 - PoPP-Service -REST Interface zur PoPP-Token-Erstellung TAN

Der PoPP-Service MUSS sicherstellen, dass die Schnittstellen I_PoPP_Token_Generation zum Abruf von PoPP-Token bei Nutzung einer TAN in einer LEI als REST-Interface mit den Endpunkten gemäß der Schnittstellen-Spezifikation in [I_PoPP_Token_Generation.yaml] umgesetzt ist. [≤]

A_26361 - PoPP-Service - Zero Trust Schutz des PoPP-Interfaces

Der PoPP-Service MUSS sicherstellen, dass der Zugang zu den Schnittstellen I_PoPP_Token_Generation zum Abruf von PoPP-Token mittels des ZETA Guard [gemSpec_ZETA] vor unberechtigten Zugriffen geschützt ist. [≤]

A_26362 - PoPP-Service - Status Code im WebSocket-Interface

Der PoPP-Service MUSS sicherstellen, dass in der Beantwortung eingehender Requests an den Schnittstellen I_PoPP_Token_Generation zum Abruf von PoPP-Token ausschließlich

die http-Status Code gemäß der OpenAPI-Spezifikation auf [I_PoPP_Token_Generation.yaml] verwendet werden. [≤]

A_26364 - PoPP-Service - VSDM-PN in PoPP-Token Nachricht aufnehmen

Der PoPP-Service MUSS sicherstellen, dass wenn addPN2TokenResponse = 1 konfiguriert ist, zusätzlich zu einem PoPP-Token ein VSDM-PN gemäß [A_26368*] erstellt und mit derselben Antwort-Nachricht wie das PoPP-Token an die aufrufende LEI gesendet wird. [≤]

Hinweis:

Das Erstellen und Versenden des zusätzlichen VSDM-PN wird über den PoPP-Service konfiguriert. Zu Beginn des PoPP-Service Betriebes ist der Schalter aktiviert. Sobald alle betroffenen Fachanwendungen und PS umgestellt sind, wird der Schalter deaktiviert. Die gematik wird den Betreiber des PoPP-Service dem entsprechend informieren und beauftragen.

A_26831 - PoPP-Service - Schalter für das Einbinden von VSDM-PN

Der PoPP-Service MUSS einen konfigurierbaren Schalter addPN2TokenResponse(int) implementieren, welcher das Einbinden vom VSDM-PN in die PoPP-Token Response Nachricht (Antwort-Nachricht) steuert.

Wert	Bedeutung
1	VSDM-PN in PoPP-Token-Antwort zufügen
0	VSDM-PN nicht PoPP-Token-Antwort zufügen

[≤]

A_26832 - PoPP-Service - Einbinden von VSDM-PN konfigurieren

Der PoPP-Service MUSS sicherstellen, dass der Schalter addPN2TokenResponse vom PoPP-Service Betreiber im laufenden Betrieb (mit einer Latenz von einer Stunde) umgestellt werden kann. [≤]

Hinweis: Entsprechend [A_26595] werden die Anwendungskontexte stündlich neu gestartet.*

A_26833 - PoPP-Service - Einbinden von VSDM-PN initial eingeschaltet

Der PoPP-Service MUSS sicherstellen, dass der Schalter addPN2TokenResponse bei Betriebsbeginn des PoPP-Service eingeschaltet ist. [≤]

6.3 PoPP-Modul

Die Anforderungen an eine Frontendkomponente für Versicherte sind erfasst in [gemSpec_PoPP_Modul]. Ein PoPP-Modul, welches in eine App integriert wird, muss diese Anforderungen erfüllen.

6.4 PoPP-Client

Die Beschreibung des PoPP-Client

https://pet-gematikde.msapproxy.net/polarion/#/project/Mainline_OPB1/wiki/Spezifikation/gemILF_PoPP_Client

6.5 Fehlerbehandlung

Error Code (HTTP Status Code, ergänzt um operationsspezifische Ergebnisse) werden in den jeweiligen Schnittstellen Dateien (Yaml-Files) erfasst und dokumentiert. In der PoPP-Service Spezifikation gibt es keine Auflistung von Error-Code.

A_26500 - PoPP-Service - externe Fehlercodes

Der PoPP-Service MUSS Fehlercodes gemäß der Schnittstellenbeschreibung umsetzen:

- [I_PoPP_CheckIn_AuthorizationServer.yaml],
- [I_PoPP_CheckIn_ResourceServer.yaml],
- [I_PoPP_Token_Generation.yaml] und
- [pip-pap-service.yaml].

[<=]

A_27317 - PoPP-Service - interne Fehlercodes

Der PoPP-Service MUSS folgende interne Fehlercodes verwenden:

Tabelle 20 : Tab_PoPP_Service_interne_Fehlercodes

BDE-Code	Errorcode Referenz	Beschreibung	Fehler-adressat
79010	POPP_INVALID_IK	Invalid health insurer mark <ik>.	Clientsystem
79011	POPP_INVALID_KVNR	Invalid health insured person number <kvnr>.	Clientsystem
79030	POPP_MISSING_OR_INVALID_HEADER	The required header <header> is missing or invalid.	Clientsystem
79031	POPP_UNSUPPORTED_MEDIATYPE	The clientsystem asked for an unsupported media type <media type>.	Clientsystem
79032	POPP_UNSUPPORTED_ENCODING	The clientsystem asked for an unsupported encoding scheme <encoding scheme>.	Clientsystem

79040	POPP_INVALID_HTTP_OPERATION	ERROR	Clientsystem
79041	POPP_INVALID_ENDPOINT	ERROR	Clientsystem
79100	POPP_SERVICE_INTERNAL_SERVER_ERROR	Unexpected internal server error.	Clientsystem
79112	POPP_OCSP_NOTREACHABLE		Clientsystem
79113	POPP_OCSP_TIMEOUT		Clientsystem
79205	-	Header ZTA-Client-Data fehlt.	HTTP-Proxy
79206	-	Header ZTA-User-Info fehlt.	HTTP-Proxy
79400	-	Client-Data Daten können nicht verarbeitet werden.	HTTP-Proxy
79401	-	User-Info Daten können nicht verarbeitet werden.	HTTP-Proxy
79402	-	PoPP-Info Daten können nicht verarbeitet werden. (?)	HTTP-Proxy

【<=】

7 Testanforderungen

Anforderungen an Test und Testbarkeit des PoPP-Service finden sich in [gemKPT_Test].

<< Die neuen Test-Festlegungen für PoPP sind im Änderungsantrag C_12019
zusammengeführt. >>
C_12019 -

8 Betrieb

In diesem Kapitel werden übergreifende, betriebliche Anforderungen getroffen oder auf Kapitel mit speziellen Ausprägungen für den Anbieter PoPP-Service in normativen Querschnittsdokumenten verwiesen.

<<Die Festlegungen werden im Änderungseintrag C_11939 zusammengeführt.>>

< siehe C_11939 >

A_27390 - Performance - PoPP-Service - Zugriff für den Nutzer

Der Anbieter PoPP-Service MUSS den Zugriff auf den Dienst über einer einzigen URL ermöglichen. Die Nutzung von diensteigenen Redundanzmechanismen zur Aufrechterhaltung der Verfügbarkeit im Falle eines Teilausfalls darf keine Nutzerinteraktion erfordern.【<=】

8.1 Schnittstellen und Anwendungsfälle

Die vom PoPP-Service zur Verfügung gestellten Schnittstellen und Anwendungsfälle werden im entsprechenden Kapitel von [gemKPT_Betr] dargestellt.

8.2 Leistungsanforderungen und Performance

Die vom PoPP-Service zu leistenden Performancevorgaben werden im entsprechenden Kapitel von [gemSpec_Perf] dargestellt. Dazu gehören insbesondere Vorgaben zur Verfügbarkeit, eingesetzten Redundanz und der Leistungsfähigkeit der Schnittstellenabrufe. Darüber hinaus werden Vorgaben zur Verarbeitung der eingesetzten Datenliefermodelle gemacht, die sich sowohl auf den Fachdienst, als auch organisatorisch auf den entsprechenden Anbieter beziehen, welcher diese Datenlieferungen gewährleisten muss.

9 Anhang A - Verzeichnisse

9.1 Abkürzungen

Tabelle 21: Im Dokument verwendete Abkürzungen

Kürzel	Erläuterung
APDU	Application Protocol Data Units
ASN.1	Abstract Syntax Notation 1, eine Variante zur Spezifikation von Datenaustauschformaten
AuthZ	Autorisierung
BDE	Betriebsdatenerfassung
CID	Change, Integration, Deletion
CSR	Certificate Signing Request
CVC	Card Verifiable Certificate
CVE	Common Vulnerabilities and Exposures
DiGA	Digitale Gesundheitsanwendungen
DPoP	Demonstrating Proof of Possession
ECIES	Elliptic Curve Integrated Encryption Scheme
eGK	elektronische Gesundheitskarte
eH-KT	eHealth-Kartenterminal
eIDAS	electronic Identification, Authentication and trust Services
FD	Fachdienst
FIPS	Federal Information Processing Standard
HMAC	Hash-based Message Authentication Code
HSM	Hardware-Sicherheitsmodul

HSM-B	Hardware Security Module Typ B
HW	Hardware
IANA	Internet Assigned Numbers Authority
IDP	Identity Provider
IK	Institutionskennzeichen
ITSEC	Information Technology Security Evaluation Criteria
JSON	JavaScript Object Notation
JWK	JSON Web Key
JWKS	JSON Web Key Set
JWT	JSON Web Token
KTR	Kostenträger
KVNR	Krankenversichertennummer
LE	Leistungserbringer
LEI	Leistungserbringerinstitution
MFA	Medizinische Fachangestellte
NFC	Near Field Communication
NFD	Notfalldatensatz
OAuth	Open Authorization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
P-256	elliptische Kurve mit Domainparametern gemäß [SP800-186#3.2.1.3]
PACE	Password Authenticated Connection Establishment
PAP	Policy Administration Point
PAR	Pushed Authorization Request

PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PKI	Public Key Infrastructure
PoPP	Proof of Patient Presence
PS	Primärsystem
SIEM	Security Information and Event Management
SM-B	Security Module Typ B
SMC-B	Security Module Card Typ B
TAN	Transaktionsnummer
TI	Telematikinfrastruktur
TSL	Trust Service Status List
UX	User Experience
VAU	Vertrauenswürdige Ausführungsumgebung
VK	Verarbeitungskontext
VSDM	Versichertenstammdatenmanagement
VSDM-PN	Prüfungsnachweis VSDM
ZETA	Zero Trust Access

9.2 Glossar

Tabelle 22: Glossar der explizit im Dokument verwendeten Begriffe

Begriff	Erläuterung
Authenticator-Modul	Die Komponente, durch die der Nutzer die Authentifizierung gegenüber dem Identity Provider (IDP) durchführt, ist ein wesentlicher Bestandteil des Sicherheitssystems.
Authorization Server	Ein Server, der Zugriffstoken ausgibt, nachdem er die

	Identität eines Benutzers authentifiziert und die Berechtigungen überprüft hat. In OAuth 2.0-basierten Systemen ist der Authorization Server eine zentrale Komponente zur Verwaltung von Zugriffsrechten.
Card Access Number (CAN)	Wird verwendet um eine vertrauenswürdige, kontaktlose Kommunikation zu einer Smartcard aufzubauen
CVC-Root	Die CVC-Root ist die zentrale Root-CA der PKI für CV-Zertifikate in der TI. Die CVC-Root ist ein Produkttyp.
DiGA	
Distinguished Encoding Rules (DER)	Eine Variante zur Codierung von ASN.1 Objekten als Bytestring.
Drittanbieter-App	Eine App, die ein Versicherter zum mobilen Check-in nutzt, wird im Gegensatz zur Kassen-App von beliebigen Stellen herausgegeben. Drittanbieter-App können für beliebige Smartphone-Betriebssysteme wie Android oder iOS sowie für unterschiedliche Desktop Betriebssysteme wie Windows oder Linux verfügbar sein. Zudem ist es möglich, dass Drittanbieter-Apps innerhalb beliebiger Internetbrowser laufen.
GesundheitsID	Die GesundheitsID ist die digitale Identität im Gesundheitswesen für Versicherte, welche durch die eigene Krankenversicherung bereitgestellt wird. Sie dient zur Anmeldung an TI-Anwendungen und weiteren versorgungsrelevanten Fachanwendungen und kann perspektivisch auch als Versicherungsnachweis - analog zur elektronischen Gesundheitskarte - verwendet werden.
Kassen-App	Eine App, die ein Versicherter zum mobilen Check-in nutzt, wird im Gegensatz zur Drittanbieter-App von seiner Krankenkasse herausgegeben.
Leistungserbringer (LE)	Ein Leistungserbringer gehört zu einem zugriffsberechtigten Personenkreis nach § 352 SGB V und erbringt Leistungen des Gesundheitswesens für Versicherte. Nach § 339 SGB V darf er auf Versichertendaten in Anwendungen der TI zugreifen.
Leistungserbringerinstitution (LEI)	Die in organisatorischen Einheiten oder juristischen Personen zusammengefassten Leistungserbringer (bspw. Arztpraxen, Krankenhäuser).
Mobiles PS	Mobiles Endgerät, auf dem ein PS-Client des installiert. Ein LE nutzt den mobilen PS-Client bei Anwendungsfällen außerhalb der LEI.

mutual TLS (mTLS)	Eine TLS Verbindung, bei der sich beide Kommunikationspartner authentisieren
Policy Administration Point (PAP)	Eine Komponente, die Sicherheitsrichtlinien erstellt, verwaltet und verteilt. Der PAP definiert und verwaltet die Richtlinien, die von der PDP Policy Engine bei der Entscheidungsfindung verwendet werden.
Policy Decision Point (PDP)	Der PDP trifft die Entscheidung, ob ein Access Token ausgestellt werden darf, basierend auf den definierten Richtlinien und Informationen über den Anfragenden und den Client.
Policy Enforcement Point (PEP)	Ein Punkt in einem Netzwerk, an dem Sicherheitsrichtlinien durchgesetzt werden. Der PEP überwacht und kontrolliert den Zugriff auf Ressourcen basierend auf den Entscheidungen, die vom Policy Decision Point (PDP) getroffen werden.
Policy Information Point (PIP)	Eine Quelle von Attributen oder Kontextinformationen, die für die Entscheidungsfindung des Policy Decision Point (PDP) erforderlich sind. Der PIP stellt die notwendigen Daten zur Verfügung, um Zugriffsanfragen entsprechend den festgelegten Richtlinien zu bewerten.
PoPP-Client	Eine Komponente im Primärsystem, die für die sichere Kommunikation zum PoPP-Service verantwortlich ist.
PoPP-Modul	Eine Komponente von Kassen-App oder Drittanbieter-App, welche beim mobilen Check-in die Kommunikation mit dem PoPP-Service übernimmt. Das PoPP-Modul verwaltet TAN-Sets, die es vom PoPP-Service im Rahmen eines mobilen Check-ins erhält und hilft bei der Übertagung einer TAN an das Primärsystem.
PoPP-Service	Zentraler Dienst in der Telematikinfrastruktur 2.0 (TI 2.0), der PoPP-Token generiert und verwaltet.
PoPP-Service Authorization Server	Der Server, der für die Authentifizierung und Autorisierung im Rahmen des PoPP-Service zuständig ist.
PoPP-Service Resource Server	Der Server, der TAN oder TAN-Sets für Versicherte an PoPP-Module ausgibt und PoPP-Token für PoPP-Clients erzeugt.
PoPP-Token	Ein Token, das als Nachweis für einen Versorgungskontext dient.
Proof of Patient Presence (PoPP)	Ein Verfahren zur Bestätigung der physischen Präsenz eines Versicherten.
Security Information and	Technologien und Prozesse zur Sammlung, Analyse und

Event Management (SIEM)	Korrelation von Sicherheitsdaten aus verschiedenen Quellen, um Sicherheitsvorfälle zu erkennen und darauf zu reagieren.
Transport Layer Security (TLS)	Stand der Technik um eine vertrauenswürdige Verbindung zwischen zwei System aufzubauen.
Versorgungskontext	Ein Versorgungskontext besteht, wenn ein Leistungserbringer und ein Versicherter zum Zweck einer Versorgung zusammenkommen. Dabei kann die Versorgung eine medizinische Behandlung, eine pflegerische Leistung oder eine andere Versorgungsleistung sein, beispielsweise in einer Apotheke. Das Zusammentreffen kann lokal in einer Leistungserbringerumgebung, mobil, beispielsweise bei einem Hausbesuch oder virtuell, beispielsweise bei einer Telefon- oder Videosprechstunde sein.
VSDM-PN	Ersatz Prüfungsnachweis VSDM, der für eine begrenzte Übergangszeit zusätzlich zum PoPP-Token vom PoPP-Service erstellt wird und an die Primärsysteme übertragen wird. VSDM-PN ist strukturgleich mit VSDM+
ZETA Client	Zero Trust Client Komponente im Primärsystem; Client Komponente gegenüber der Zero Trust Server Komponente ZETA Guard.
ZETA Guard	Der beim Fachdienst einzubindende Zero Trust Cluster.

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

9.3 Abbildungsverzeichnis

Abbildung 1: Einfacher Systemüberblick.....	9
Abbildung 2: Rollen und Akteure bei Herstellung und Betrieb des PoPP-Service.....	15
Abbildung 3: Produkttypzerlegung.....	18
Abbildung 4: Systemkontext PoPP-Lösung.....	20
Abbildung 5: Anwendungsfälle zur Attestierung des Versorgungskontextes.....	25
Abbildung 6: Abläufe Check-in für unterschiedliche Konstellationen.....	30
Abbildung 7: Ausstellen und Einlösen eines "eHealth-ID-check" Access Token.....	31
Abbildung 8: Ausstellen und Einlösen eines "card-check" Access Token.....	35
Abbildung 9: Ausstellung PoPP-Token durch LEI über Einlösen einer TAN durch Versicherten am Ort der Leistungserbringung.....	41
Abbildung 10: Ausstellung PoPP-Token durch LEI über Einlösen einer TAN durch Versicherten mobil (Videosprechstunde, Apotheken).....	44

Abbildung 11: Ausstellung PoPP-Token nach Stecken der eGK in LEI.....	47
Abbildung 12: Komponentendiagramm PoPP-Service Authorization Server bei Authentifizierung mit GesundheitsID.....	93
Abbildung 13: Komponentendiagramm PoPP-Service Authorization Server bei Authentifizierung einer eGK mobil.....	94
Abbildung 14: Sequenzdiagramm Nutzer Authentisierung mit GesundheitsID oder eGK und die Erlangung einer TAN oder eines TAN-Sets über ein PoPP-Modul.....	101
Abbildung 15: Zustandsdiagramm für die Verarbeitung einer eGK.....	110
Abbildung 16: Anwendungsfälle des PoPP-Service Authorization Server bei der Zugriffsautorisierung eines in eine App integrierten PoPP-Moduls.....	127
Abbildung 17: Anwendungsfälle des PoPP-Service Resource Server beim Zugriff eines in eine App integrierten PoPP-Moduls.....	128

9.4 Tabellenverzeichnis

Tabelle 1: PoPP-Use Cases (Business Sicht).....	11
Tabelle 2: Kurzbeschreibung der Komponenten in der PoPP-Lösung.....	20
Tabelle 3: Zuordnung der Anwendungsfälle zu den Use Cases.....	26
Tabelle 4: PoPP-Token Claims (informativ).....	52
Tabelle 5: PoPP-Token Header (informativ).....	54
Tabelle 6: Übersicht über die im PoPP-Service verwendeten Schlüssel.....	81
Tabelle 7: Attribute im well-known document des PoPP-Service.....	88
Tabelle 8: Attribute des Metadatenblock <i>oauth_resource</i> im well-known document des PoPP-Service.....	89
Tabelle 9: Attribute des Metadatenblock <i>federation_entity</i> im well-known document des PoPP-Service.....	89
Tabelle 10: Attribute des Metadatenblock <i>oauth_authorization_server</i> im well-known document des PoPP-Service.....	90
Tabelle 11: Attribute zur Registrierung von Anwendungsfrontends.....	95
Tabelle 12: "ehealthId-check" Access Token nach Bestätigung durch einen sektoralen Identity Provider.....	96
Tabelle 13: "card-check" Access Token für die Prüfung der eGK(mobil).....	97
Tabelle 14: Kurzbeschreibung des Ablaufs der Nutzerauthentisierung mit GesundheitsID für die Erlangung einer TAN oder eines TAN-Sets über ein PoPP-Modul.....	101
Tabelle 15 : Kurzbeschreibung des Ablaufs der Authentifizierung der eGK für die Erlangung einer TAN oder eines TAN-Sets über ein PoPP-Modul.....	103
Tabelle 16 : Kurzbeschreibung des Ablaufs nach Authentifizierung mit GesundheitsID oder eGK für die Erstellung einer TAN oder eines TAN-Sets und Übergabe an das PoPP- Modul.....	104
Tabelle 17: Werte für spezifische Parameter im PAR.....	106
Tabelle 18: Fehlermeldungen eGK-Handling.....	122

Tabelle 19: Dateninhalte TANSet-Record.....	130
Tabelle 20 : Tab_PoPP_Service_interne_Fehlercodes.....	133
Tabelle 21: Im Dokument verwendete Abkürzungen.....	137
Tabelle 22: Glossar der explizit im Dokument verwendeten Begriffe.....	139
Tabelle 23: Referenzierte Dokumente der gematik.....	144
Tabelle 24 : Weitere Dokumente.....	147
Tabelle 25: Entity Statement des PoPP-Service.....	149

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.

Tabelle 23: Referenzierte Dokumente der gematik

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[VSDMPNSchema]	XML Schema VSDM Prüfungsnachweis v1.0 https://github.com/gematik/api-telematik/blob/OPB5/fa/vsds/Pruefungsnachweis.xsd
[TI-Föderation]	Fachanwendungen der TI-Föderation (aus der Wissensdatenbank der gematik, zuletzt abgerufen am 21.08.2024) https://wiki.gematik.de/pages/viewpage.action?pageId=523502009
[gemILF_PoPP_Client]	Implementierungsleitfaden Primärsystemfunktionalität PoPP-Client (Dokument noch in Erstellung)
[gemKPT_Betr]	Betriebskonzept Online-Produktivbetrieb https://gemspec.gematik.de/docs/gemKPT/gemKPT_Betr/
[gemKPT_Test]	Testkonzept der TI https://gemspec.gematik.de/docs/gemKPT/gemKPT_Test/
[gemSpec_IDP_Dienst]	Spezifikation Identity Provider-Dienst https://gemspec.gematik.de/docs/gemSpec/gemSpec_IDP_Dienst/

[gemSpec_IDP_FD]	Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste https://gemspec.gematik.de/docs/gemSpec/gemSpec_IDP_FD/
[gemSpec_IDP_Sek]	Spezifikation Sektoraler Identity Provider https://gemspec.gematik.de/docs/gemSpec/gemSpec_IDP_Sek/
[gemSpec_ZETA]	Spezifikation Zero Trust Access (ZETA) (Dokument noch in Erstellung)
[gemSpec_PoPP_Modul]	Spezifikation PoPP-Modul (Dokument noch in Erstellung)
[gemSpec_DS_Anbieter]	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter https://gemspec.gematik.de/docs/gemSpec/gemSpec_DS_Anbieter/
[gemSpec_OID]	Spezifikation Festlegung von OIDs https://gemspec.gematik.de/docs/gemSpec/gemSpec_OID/
[gemSpec_Krypt]	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur https://gemspec.gematik.de/docs/gemSpec/gemSpec_Krypt/
[gemSpec_SST_FD_VSDM]	Schnittstellenspezifikation Fachdienste (UFS/VSDM/CMS) https://gemspec.gematik.de/docs/gemSpec/gemSpec_SST_FD_VSDM/
[gemAPI_ZT]	gematik: OpenAPI Schnittstellenspezifikation Zero Trust https://github.com/gematik/spec-t20r
[gemSpec_DS_Hersteller]	Spezifikation Datenschutz- u. Sicherheitsanforderungen der TI an Hersteller https://gemspec.gematik.de/docs/gemSpec/gemSpec_DS_Hersteller/
[gemSpec_TSL]	Spezifikation TSL-Dienst https://gemspec.gematik.de/docs/gemSpec/gemSpec_TSL/
[gemSpec_eGK_ObjSys_G2.1]	Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem https://gemspec.gematik.de/docs/gemSpec/gemSpec_eGK_ObjSys_G2_1/

[gemSpec_COS]	Spezifikation des Card Operating System (COS) https://gemspec.gematik.de/docs/gemSpec/gemSpec_COS/
[gemSpec_Kon]	Spezifikation Konnektor https://gemspec.gematik.de/docs/gemSpec/gemSpec_Kon/
[pip-pap-service.yaml]	OpenAPI Schnittstellenspezifikation für Policy Information Point und Policy Administration Point API https://raw.githubusercontent.com/gematik/spec-t20r/develop/src/openapi/pip-pap-api.yaml
[I_PoPP_CheckIn_AuthorizationServer.yaml]	OpenAPI Schnittstellenspezifikation des PoPP-Service Authorization Server für PoPP-Module: https://github.com/gematik/api-popp/blob/main/src/openapi/I_PoPP_CheckIn_AuthorizationServer.yaml
[I_PoPP_CheckIn_ResourceServer.yaml]	OpenAPI Schnittstellenspezifikation des PoPP-Service Resource Server für PoPP-Module: https://github.com/gematik/api-popp/blob/main/src/openapi/I_PoPP_CheckIn_ResourceServer.yaml
[I_PoPP_Token_Generation.yaml]	OpenAPI Schnittstellenspezifikation für PoPP-Service Resource Server für PoPP-Clients: https://github.com/gematik/api-popp/blob/main/src/openapi/I_PoPP_Token_Generation.yaml

9.5.2 Weitere Dokumente

Tabelle 24 : Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[AnbieterVZeitD]	Die Bundesnetzagentur listet unter https://www.elektronische-vertrauensdienste.de/EVD/DE/Uebersicht_eVD/Dienste/5_Zeitstempel.html?nn=691392 verschiedene Anbieter für qualifizierte Zeitstempel.
[FIPS PUB 180-4]	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Secure Hash Standard (SHS), August 2015 http://dx.doi.org/10.6028/NIST.FIPS.180-4
[OpenID Federation 1.0]	OpenID Federation 1.0 - draft 40 https://openid.net/specs/openid-federation-1_0.html#name-entity-statement
[RFC7519#Sect.2]	JSON Web Token (JWT)

	https://datatracker.ietf.org/doc/html/rfc7519#section-2
[OpenID Federation 1.0#draft 38]	OpenID Federation 1.0 - draft 38 https://openid.net/specs/openid-federation-1_0.html#section-3
[OpenID Connect Federation 1.0#section4.1]	OpenID Federation 1.0 - draft 40 https://openid.net/specs/openid-federation-1_0.html#section-4.1
[RFC1760]	The S/KEY One-Time Password System https://www.rfc-editor.org/rfc/rfc1760
[RFC2289]	A One-Time Password System https://www.rfc-editor.org/rfc/rfc2289
[RFC2119]	Key words for use in RFCs to Indicate Requirement Levels https://www.rfc-editor.org/rfc/rfc2119
[RFC 5639]	Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation https://www.rfc-editor.org/rfc/rfc5639
[RFC 6962]	Certificate Transparency https://www.rfc-editor.org/rfc/rfc6962
[RFC 9162]	Certificate Transparency Version 2.0 https://www.rfc-editor.org/rfc/rfc9162
[CAB Forum]	https://cabforum.org/
[RFC7518]	JSON Web Algorithms (JWA) https://www.rfc-editor.org/rfc/rfc7518
[RFC7517]	JSON Web Key (JWK) https://www.rfc-editor.org/rfc/rfc7517
[RFC7638]	JSON Web Key (JWK) Thumbprint https://www.rfc-editor.org/rfc/rfc7638
[RFC7519]	JSON Web Token (JWT) https://www.rfc-editor.org/rfc/rfc7519
[RFC7515]	JSON Web Signature (JWS) https://www.rfc-editor.org/rfc/rfc7515
[RFC6749]	The OAuth 2.0 Authorization Framework https://datatracker.ietf.org/doc/html/rfc6749
[RFC 6844]	DNS Certification Authority Authorization (CAA) Resource Record

	https://www.rfc-editor.org/rfc/rfc6844
[RFC9396]	OAuth 2.0 Rich Authorization Requests https://www.rfc-editor.org/rfc/rfc9396.html
[RFC5639]	Elliptic Curve Cryptography (ECC) Brainpool Standard - Curves and Curve Generation https://datatracker.ietf.org/doc/html/rfc5639
[RFC 6066]	Transport Layer Security (TLS) Extensions: Extension Definitions https://datatracker.ietf.org/doc/html/rfc6066
[RFC5652]	Cryptographic Message Syntax (CMS) https://datatracker.ietf.org/doc/html/rfc5652
[RFC4122#3]	Namespace Registration Template https://datatracker.ietf.org/doc/html/rfc4122#section-3
[RFC 5280]	Validity https://www.rfc-editor.org/rfc/rfc5280#section-4.1.2.5
[SP800-186]	Chen L, Moody D, Regenscheid A, Robinson A, Randall K (2023) Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-186. https://doi.org/10.6028/NIST.SP.800-186
[jwk-set+jwt]	https://www.iana.org/assignments/media-types/ application/jwk-set+jwt
[BSI-QDDoS]	BSI: Qualifizierte DDoS-Mitigation Dienstleister, aktuelle Fassung https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/ Informationen-und-Empfehlungen/Informationen-und- weiterfuehrende-Angebote/Qualifizierte-Dienstleister/ qualifizierte-dienstleister_node.html (zuletzt aufgerufen am 28.11.2024)
[BSI ISI-LANA]	BSI: Standards zur Internet-Sicherheit (ISi-Reihe) https://www.bsi.bund.de/DE/Themen/Unternehmen-und- Organisationen/Informationen-und-Empfehlungen/ISI- Reihe/isi-reihe_node.html
[SP800-186#3.2.1.3]	Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters https://doi.org/10.6028/NIST.SP.800-186

[https://app.federationmaster.de/federation/list]	https://app.federationmaster.de/federation/list
---	---

9.6 Allgemeine Erläuterungen

9.6.1 Entity Statement des PoPP-Service

Tabelle 25: Entity Statement des PoPP-Service

Name	Werte	Beispiel	Anmerkungen
iss	URL	"https://popp-auth.de"	URL des PoPP-Service Authorization Server, Identifier in der Föderation
sub	URL	"https://popp-auth.de"	URL des PoPP-Service Authorization Server, (=iss)
iat	Alle time Werte in Sekunden seit 1970, [RFC7519]#Section.2	1645484401	2022-02-22 00:00:01
exp	Alle time Werte in Sekunden seit 1970, [RFC7519]#Section.2	1645570800	Gültigkeit von 24 Stunden
jwks	JWKS Objekt		Federation Entity Key für die Signatur des Entity Statements [OpenID Federation 1.0#draft 38]
authority_hints	[string]	"https://app.federationmaster.de"	iss Bezeichnung des Federation Masters
metadata {			

<i>openid_relying_party {</i>			
signed_jwks_uri	URL	"https://popp-rp.de/jws.json"	Schlüssel, welche die Relying Party für die Signatur und für die Verschlüsselung verwendet.
redirect_uris	[URLs]	"https://popp-rp.de/client"	Liste der registrierten redirect_uris
response_types	[code]	-	
client_registration_types	[automatic]	-	gemäß [https://openid.net/specs/openid-federation-1_0.html] _
grant_types	[authorization_code]	-	[https://openid.net/specs/openid-connect-registration-1_0.html#ClientMetadata] _
require_pushed_authorization_requests	true	-	[RFC 9126#section-6] _
token_endpoint_auth_method	self_signed_tls_client_auth	-	
default_acr_values	"gematik-ehealth-loa-high" "gematik-ehealth-loa-substantial"	"gematik-ehealth-loa-high"	[https://openid.net/specs/openid-connect-registration-1_0.html#ClientMetadata] _
id_token_signed_response_alg	ES256	-	Weitere Werte sind möglich.
id_token_encrypted_response_alg	ECDH-ES	-	Weitere Werte sind möglich.
id_token_encrypted_response_enc	A256GCM	-	Weitere Werte sind möglich.

scope	[string]	"openid urn:telematik:vers cherter"	String mit space- delimited scope values
}			
<i>federation_entity</i> {			
organization_name	String	Hersteller PoPP- Service	Optional: Name der Organisation die hinter dem Fachdienst steht
contacts	[strings]	"support@popp- hersteller.de", "info@popp- hersteller.de"	Optional
homepage_uri	URL	"https://popp- hersteller.de"	Optional
logo_uri	URL	"https://popp- hersteller.de/ logo.jpg"	Optional
}			
<i>oauth_authorization_server</i> {			
issuer	URL	"https://popp- auth.de"	Authorization Server issuer Identifizier
signed_jwks_uri	URL	"https://popp- auth.de/jws.json"	
authorization_endpoint	URL	"https://popp- auth.de/auth"	
token_endpoint	URL	"https://popp- auth.de/token"	
openid_providers_endpoint	URL	" https://idp.app.ti- dienste.de/director y/fed_idp_list "	
response_types_supported	<i>code</i>		
response_modes_supported	<i>query</i>		

grant_types_supported	authorization_code		
token_endpoint_auth_methods_supported	none		
token_endpoint_auth_signing_alg_values_supported	ES256		
code_challenge_methods_supported	S256		
}			
oauth_resource {			
signed_jwks_uri	URL	"https://popp.service.de/jwks.json"	Schlüssel welche die Protected Resource für die Signatur und für die Verschlüsselung verwendet.
authorization_server	URL	"https://popp.auth.de"	Identifizier (issuer) des PoPP-Service Authorization Server
}			
}			

