Telematikinfrastruktur 2.0

Technisches Konzept Proof of Patient Presence (PoPP)

Version:	1.0.0_CC
Revision:	933118
Stand:	06.06.2024
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemKPT_PoPP

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um eine Erstveröffentlichung.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0_CC	06.06.2024		initiale Erstellung	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

1.1 Zielsetzung

Das vorliegende Dokument versteht sich als Grobkonzeption und dient der Einleitung einer aktiven Abstimmung mit den Gesellschaftern der gematik. Es bietet einen Überblick über die geplante technische Architektur, die Nutzungsszenarien sowie die benötigten Komponenten und Dienste zur Umsetzung der Proof of Patient Presence (PoPP)-Lösung für einen Einsatz ab 2026.

Dabei ist das Ziel, die Gesellschafter über die strategische Ausrichtung und die technischen Anforderungen zu informieren und durch eine detaillierte Darstellung der benötigten Komponenten und Dienste zum einen die Ressourcenanforderungen frühzeitig transparent zu machen und zum anderen potenzielle Herausforderungen rechtzeitig zu identifizieren. Damit soll eine fundierte Basis geschaffen werden, auf der die Gesellschafter ihre Zustimmung und Unterstützung für die nächsten Schritte geben können.

1.2 Gesetzliche Rahmenbedingungen

(siehe Kapitel 2.1- Impliziter Auftrag)

1.3 Zielgruppe

- Gesellschafter der gematik, die als Entscheider über die Umsetzung der Lösung sowie Leistungsumfang und Kosten entscheiden
- Mitarbeiter der gematik, die auf Basis des Konzepts die weiteren Unterlagen wie Schnittstellenbeschreibungen, Spezifikationen, Ausschreibungsunterlagen etc. erstellen

1.4 Geltungsbereich

Wichtiger 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.

1.5 Abgrenzung des Dokuments

Dieses Dokument beschreibt das Grob-Konzept für die PoPP-Lösung, die im Kontext der TI2.0 ab 2026 für neue Anwendungen, wie VSDM2, benötigt wird. Es grenzt sich von bisherigen Konzepten und Vorabveröffentlichungen zum PoPP ab, die es bereits Ende 2022 / Anfang 2023 gegeben hat und im Zusammenhang mit einer Umsetzung im Konnektor standen.

1.6 Methodik

Dieses Konzept-Papier enthält keine Anforderungen.

1.6.1 Hinweis auf offene Punkte

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

2 Auftragslage und Rahmenbedingungen

2.1 Impliziter Auftrag

Gemäß §291b Abs. 1, SGB V, haben die Krankenkassen ab 01.01.2026 Dienste zur Verfügung zu stellen, mit denen die an der vertragsärztlichen Versorgung teilnehmenden Leistungserbringer und Einrichtungen die Gültigkeit und die Aktualität der Angaben nach § 291a Absatz 2 und 3 bei den Krankenkassen online überprüfen und diese Angaben aktualisieren können. Nach einer Übergangszeit von drei Monaten ist das bisherige Verfahren mit dem Onlineabgleich und der Onlineaktualisierung der gespeicherten Daten auf der elektronischen Gesundheitskarte nach §291b Abs. 2, SGB V, nicht mehr zulässig.

Neben dem Versicherungsnachweis hat sich das Verfahren, bei dem auch ein VSDM-Prüfungsnachweis erzeugt wird, für das Einlösen eines E-Rezeptes durch eine authentifizierte Apotheke etabliert. Ab 2025 wird der Prüfungsnachweis auch den Zugriff eines authentifizierten Leistungserbringers auf die "ePA für alle" ermöglichen. Sofern die mit dem gesetzlichen Auftrag verbundenen Systeme der Kassen ab dem 31.03.2026 abgeschaltet werden, wird mit der PoPP-Lösung eine Nachfolgetechnologie ermöglicht, die eine geeignete Basis für die TI2.0 Architektur bietet, d.h. weitestgehend ohne Konnektor auskommt und auf Basisfunktionalitäten der Zero Trust Architektur baut.

Weiterhin soll die digitale Identität für Versicherte ab dem 01.01.2026, neben der eGK, auch als Versicherungsnachweis dienen. Dies muss eine Lösung im Zusammenspiel mit den Kassen und ihrer betriebenen Identitätsprovider ermöglichen. Daneben wird mindestens jeder gesetzlich Versicherter über eine elektronische Gesundheitskarte verfügen. Mit beiden Identitätstypen müssen die TI-Versorgungsszenarien weiterhin möglich sein.

2.2 Versorgungskontext

Der mit der hier beschriebenen Lösung ausgestellte Nachweis ist ein Nachweis über einen Versorgungskontext zwischen einem Versicherten und einer Leistungserbringerinstitution.

Dafür muss zu einem bestimmten Zeitpunkt ein Zusammenhang zwischen einem berechtigten Versicherten und der ihn behandelnden oder anderweitig versorgenden authentifizierten Leistungserbringerinstitution hergestellt werden. Berechtigt ist ein Versicherter, wenn er mit seiner digitalen Identität authentifiziert oder seine eGK auf Echtheit und Gültigkeit erfolgreich überprüft wurde.
Der Nachweis des Versorgungskontextes soll sicher, kryptografisch belegt und damit nicht kompromittierbar erfolgen, sodass er ausschließlich die in diesem Kontext versorgende und authentifizierte Leistungserbringerinstitution zum Zugriff auf anwendungsbezogene Versicherungsdaten über die TI-Anwendungen autorisiert. Diese Verbindung wird hier als "Versorgungskontext" bezeichnet.

Da bei einem Versorgungskontext in den meisten Fällen die physische Anwesenheit von Leistungserbringer und Versichertem vorliegt und diese Anwesenheit auch im Fokus vergangener Konzeptionsaktivitäten der gematik lag, ist der Nachweis dieses Kontextes unter dem Namen PoPP als "Proof of Patient Presence" bekannt. Diese Abkürzung wird im Dokument häufig verwendet, inkludiert aber beispielsweise auch telemedizinische Use Cases ohne physische Präsenz.

192 Das Artefakt der PoPP-Lösung ist ein kryptografisch gesichertes Token, das als PoPP-
193 Token bezeichnet wird.

3 Anwendungsumfeld

Dieser Abschnitt befasst sich mit den beteiligten Nutzergruppen und listet beispielhaft Nutzungsszenarien der TI-Anwendungen VSDM2, E-Rezept und "ePA für alle" auf.

3.1 Personen und Rollen

3.1.1 Versicherte

Im Fokus des PoPP-Konzeptes sind folgende Versichertengruppen in Deutschland:

1. gesetzlich Versicherte mit eGK
2. gesetzlich Versicherte mit GesundheitsID
3. Privatversicherte mit GesundheitsID

Explizit ausgeschlossen werden Privatversicherte, die nur über eine Speicherkarte (KVK) verfügen. Sie besitzen keine Identität im Gesundheitswesen, die eine Authentizität gewährleistet.

3.1.2 Leistungserbringerinstitution (LEI)

Bei TI-Fachdienstzugriffen ist die Institutionsidentität maßgeblich, bspw. beim Zugriff auf den E-Rezept-Fachdienst oder der "ePA für alle". Daher muss der Behandlungsnachweis Merkmale der nutzenden Institution, bspw. die Telematik-ID, beinhalten. Für diesen Teil ist die Verfügbarkeit einer Identität - kartengebunden (SMC-B) bzw. kartenlos (SM-B) - zwingend erforderlich.

3.1.3 Leistungserbringer (LE)

Mit Blick auf den vorherigen Absatz wird der Ablauf zum Versorgungskontext - möglichst als "Hintergrundjob" - vom medizinischen Fachpersonal initiiert. Der Ablauf in der Praxis soll sich nach Möglichkeit vom heutigen Ablauf (bspw. Stecken einer eGK in ein Kartenterminal) nicht unterscheiden. Für die Nutzung der GesundheitsID als Versicherungsnachweis sind hingegen andere Abläufe durch eine geänderte Technologie nicht auszuschließen.

Die Nutzung eines Heilberufsausweises, d.h. personenbezogene Vorgänge, werden in diesem Konzept nicht betrachtet.

3.1.4 Primärsystem-Hersteller

Hersteller und Anbieter von Primärsystemen (PS) nehmen eine entscheidende Rolle in der Entwicklung und Migration zur Verwendung von PoPP ein. Ein Teil der Funktionalität der Herstellung eines Versorgungskontextes wird zwingend als Bestandteil des Primärsystems benötigt ("PoPP-Client"). Darüber hinaus ist es in Hinblick auf eine Migration entscheidend, neben einer neuen Lösung zeitweise auch die bisherigen Autorisierungswege an TI-Fachdiensten parallel abzubilden. Demnach muss ein Primärsystem zum Rollout des PoPP alle bisherigen und die neuen Abläufe unterstützen und darüber hinaus noch eine einfache Umschaltung zur Migration integrieren.

3.1.5 IT-Servicedienstleister

Die IT-Servicedienstleister sind für den Rollout der angepassten Primärsysteme sowie als Kommunikationsmittel für das medizinische Fachpersonal von entscheidender Bedeutung.

3.1.6 gematik

Die gematik stellt für den PoPP-Client Spezifikationen in Form eines Implementierungsleitfadens sowie eine Beispielimplementierung des PoPP-Clients als Open Source zur Verfügung. Darüber hinaus wird die Test-Instanz des PoPP-Services in der RU genutzt, um die Integration des PoPP-Clients zu testen.
Weiterhin ist die gematik für die Spezifikation, Ausschreibung und Vertragsgestaltung des zentralen PoPP-Services verantwortlich.

3.2 Ortskontext

Behandlungen mit physischer Präsenz von Leistungserbringern und Leistungsempfängern können:

1. in einer LEI vor Ort
2. mobil (LE beim Versicherten vor Ort)
3. mobil in einer LEI vor Ort

erfolgen. Letzteres meint beispielhaft einen Versicherten mit GesundheitsID in einem Krankenhaus, der keine Möglichkeit hat, für einen Check-in mit bisher zugelassenen TI-Komponenten zu interagieren. Auch dieser Fall muss mitgedacht und über den PoPP-Nachweis adressiert werden.

Darüber hinaus kann es Behandlungssituationen ohne physische Präsenz, wie beispielsweise in der Telemedizin geben. Auch hier müssen die Versorgungskontexte über den PoPP sicher nachgewiesen werden.

3.3 Zeitkontext

Die Erstellung des kryptografisch gesicherten PoPP-Nachweises erfolgt weitestgehend synchron zur Behandlung / Versorgung.
Da der PoPP Service über keine Verbindung zur TI 1.0 verfügt, besorgt er sich die Uhrzeit im Internet. Um die Vertrauenswürdigkeit zu erhöhen, empfiehlt es sich, dass sich der PoPP Service mit einem vertrauenswürdigen Zeitdienstanbieter synchronisiert (qualifizierter Zeitstempel).

3.4 Ableitung von Nutzungsszenarien

In diesem Abschnitt werden Versorgungsszenarien als Beispiele für die Nutzung des PoPP-Tokens beschrieben, um die Vielfalt der Anforderungen darzulegen.

In der folgenden Tabelle sind zunächst die möglichen Konstellationen von verschiedenen Aufenthaltsorten des Leistungserbringers und des Versicherten in einem Versorgungsszenario dargestellt und einer Szenarien-ID zugeordnet. Die anschließende

Auflistung exemplarischer Use Cases in den darauf folgenden Tabellen zu den unterschiedlichen Szenarien fokussiert die Sicht eines Versicherten, der ein Szenario bei oder mit einem Leistungserbringer durchlaufen möchte.

Tabelle 1: Übersicht der möglichen Versorgungsszenarien in Bezug auf den Ort des Leistungserbringers bzw. des Versicherten (innerhalb / außerhalb der LEI)

Versorgungsszenario-ID	01	02	03a*	03b**	04
Versicherter in LEI	x				x
Versicherter außerhalb der LEI		x	x	x	
Leistungserbringer in LEI	x	x			
Leistungserbringer außerhalb der LEI			x	x	x

* Versicherter und Leistungserbringer am selben Ort

** Versicherter und Leistungserbringer an unterschiedlichen Orten

Im Folgenden wird auf Use Cases zu den Versorgungsszenarien für die relevantesten TI-Anwendungen VSDM2, E-Rezept und "ePA für alle" eingegangen. Für alle Szenarien benötigt eine authentifizierte LEI einen kryptografisch gesicherten Nachweis des Versorgungskontextes (PoPP-Token), um auf den entsprechenden Fachdienst zugreifen zu können. In den unterschiedlichen Szenarien wird unterschieden, ob für den PoPP-Token die "eGK ohne PIN" und / oder die "GesundheitsID" des Versicherten verwendet werden kann.
Nicht betrachtet wird, ob ein PoPP-Token für eine Anwendung ausreichend ist oder ob darüber hinaus noch weitere anwendungsspezifische Nachweise erforderlich sind.

Die notwendigen Hardware-Anforderungen bei der Verwendung der eGK G2.1 ohne PIN bzw. der GesundheitsID in dem jeweiligen Versorgungszenario finden sich in Kap. **4.2- PoPP mit eGK** bzw. Kap. **4.3- PoPP mit GesundheitsID**

3.4.1 Versorgungsszenario 01

Der Versicherte und der LE befinden sich in der LEI.

PoPP-Token über	Nutzung möglich
eGK G2.1 ohne Pin	ja
GesundheitsID	ja

288 **Tabelle 2 : Exemplarische Use Cases zum Versorgungsszenario 01**

Anw_1.x	Beschreibung des Uses Cases	Anmerkungen / Erläuterung
VSD_1.1	Ein Versicherter möchte in der Praxis eine Leistung empfangen. Dazu benötigt der behandelnde LE aktuelle Stammdaten und einen Versicherungsnachweis (VSDM2) für die Abrechnung.	
ePA_1.1	Ein Versicherter in der Praxis möchte dem ihn behandelnden LE Zugriff auf seine "ePA für alle" gewähren.	
eRX_1.1	Ein Versicherter möchte verordnete E-Rezepte in der Apotheke einlösen.	
eRX_1.2	Ein Versicherter möchte bei einem Hilfsmittel-LE/ Heilberufler oder stationärer Pflegeeinrichtung eVerordnungen einlösen.	
eRX_1.3	Ein Versicherter möchte nach Erfassung seiner Antragsdaten, die im PS des LEs erfassten Angaben bestätigen. Zuvor hat ein Hilfsmittel-LE / Pflegekraft bei der Erfassung dieser Antragsdaten in Vorbereitung auf die Genehmigung einer Leistung durch die Krankenkasse unterstützt.	Wie bereits in Kap. 3.4-Ableitung von Nutzungsszenarien erwähnt, wird nicht betrachtet, ob der PoPP-Token für diesen Use Case ausreichend ist.

289 ### 3.4.2 Versorgungsszenario 02

290 Der Versicherte befindet sich außerhalb und der LE in der LEI

PoPP-Token über	Nutzung möglich
eGK G2.1 ohne Pin	**nein**
GesundheitsID	ja

291

292 **Tabelle 3: Exemplarische Use Cases zum Versorgungsszenario 02**

Anw_2.x	Beschreibung des Uses Cases	Anmerkungen / Erläuterung
VSD_2.1	Ein Versicherter möchte via Telemedizin eine Leistung empfangen. Dazu benötigt der behandelnde LE aktuelle Stammdaten und einen Versicherungsnachweis (VSDM2) für die Abrechnung.	
ePA_2.1	Ein Versicherter möchte während einer Videosprechstunde dem behandelnden Leistungserbringer Zugriff auf seine "ePA für alle" gewähren.	
eRX_2.1	Ein Versicherter möchte mobil mit seinem Smartphone über eine Apotheken-App verordnete E-Rezepte zum Abholen oder Versand einlösen.	⚠ Use Case wird nicht unterstützt (s. Kap. 3.4.6- Nicht unterstützte Use Cases)
eRX_2.2	Ein Versicherter möchte während einer Videosprechstunde ein E-Rezepte verordnet bekommen.	

293 ## 3.4.3 Versorgungsszenario 03a

294 Der Versicherte und der LE befinden sich außerhalb der LEI am selben Ort.

PoPP-Token über	Nutzung möglich
eGK G2.1 ohne Pin	ja
GesundheitsID	ja

295

296 **Tabelle 4: Exemplarische Use Cases zum Versorgungsszenario 03a**

Anw_3a.x	Beschreibung des Uses Cases	Anmerkungen / Erläuterung
VSD_3a.1	Ein Versicherter möchte zuhause eine Leistung empfangen (LE beim Versicherten). Dazu benötigt der behandelnde LE aktuelle Stammdaten und einen Versicherungsnachweis (VSDM2) für die Abrechnung.	

Anw_3a.x	Beschreibung des Uses Cases	Anmerkungen / Erläuterung
ePA_3a.2	Ein Versicherter möchte dem LE zuhause Zugriff auf seine "ePA für alle" gewähren (LE beim Versicherten zuhause).	
ePA_3a.3	Ein Bewusstloser oder eine nicht ansprechbare Person möchte, dass der behandelnde LE beim Auffinden auf der Straße auf seine Notfalldaten in der "ePA für alle" zugreifen kann.	⚠ Use Case kann nur mit eGK umgesetzt werden. Die GesundheitsID kann nicht verwendet werden, da eine Interaktion des Versicherten mit seinem VE-Endgerät ausgeschlossen ist.
eRX_3a.1	Ein Versicherter möchte bei einem ambulanten Pflegedienst eine durch einen Arzt verordnete eVerordnung einlösen.	
eRX_3a.2	Ein Versicherter möchte ein E-Rezept an der Haustür beim Apothekenmitarbeiter (Bote) einlösen. Ein Apothekenmitarbeiter (Bote) möchte dazu mit seiner "Apo-Botendienst-Smartphone-App" das verordnete E-Rezept abrufen und für die Dispensierung der eigenen Apotheke zuweisen, sodass beim Beliefern auch das E-Rezept in die Hoheit der Apotheke gelangt.	Voraussetzung ist, dass die "Apo-Botendienst-Smartphone-App" die Funktion eines PS mit PoPP-Client übernimmt.
eRX_3a.3	Ein pflegebedürftiger Versicherter ohne eigenes Smartphone möchte in der Pflege zuhause verordnete eVerordnungen für häusliche Krankenpflegeleistungen einlösen.	⚠ Use Case kann nur mit der eGK umgesetzt werden, da kein VE-Endgerät vorhanden.
eRX_3a.4	Ein Versicherter ohne eigenes Smartphone möchte die von der Pflegekraft erbrachte Leistung abzeichnen. Die Pflegekraft benötigt den Nachweis, den Versicherten zuhause versorgt zu haben.	⚠ Use Case kann nur mit der eGK umgesetzt werden, da kein VE-Endgerät vorhanden. Wie bereits in Kap. 3.4-Ableitung von Nutzungsszenarien erwähnt, wird nicht betrachtet, ob der PoPP-Token für diesen Use Case ausreichend ist.

Anw_3a.x	Beschreibung des Uses Cases	Anmerkungen / Erläuterung
eRX_3a.5	Ein Versicherter möchte die vom Heilmittel-LE (Logopäde, Physiotherapeut, ...) erbrachte Leistung abzeichnen. Der Heilmittel-LE mit eigenem LE-Smartphone benötigt den Nachweis, den Versicherten versorgt zu haben.	⚠ da ein mobiles LE-Endgerät verwendet wird, entspricht der Use Case Versorgungsszenario 3a und nicht Versorgungsszenario 1 Voraussetzung ist, dass eine App auf dem LE-Smartphone die Funktion eines PS mit PoPP-Client übernimmt. Wie bereits in Kap. 3.4-Ableitung von Nutzungsszenarien erwähnt, wird nicht betrachtet, ob der PoPP-Token für diesen Use Case ausreichend ist.
eRX_3a.6	Ein Versicherter möchte die vom Hilfsmittel-LE (Sanitätshaus, Augenoptiker, Hörakustiker, ...) erbrachte Leistung abzeichnen. Der Hilfsmittel-LE mit eigenem LE-Smartphone benötigt den Nachweis, den Versicherten versorgt zu haben.	⚠ da ein mobiles LE-Endgerät verwendet wird, entspricht der Use Case Versorgungsszenario 3a und nicht Versorgungsszenario 1 Voraussetzung ist, dass eine App auf dem LE-Smartphone die Funktion eines PS mit PoPP-Client übernimmt. Wie bereits in Kap. 3.4-Ableitung von Nutzungsszenarien erwähnt, wird nicht betrachtet, ob der PoPP-Token für diesen Use Case ausreichend ist.

297 ### 3.4.4 Versorgungsszenario 03b

298 Der Versicherte und der LE befinden sich außerhalb der LEI an unterschiedlichen Orten.

PoPP-Token über	Nutzung möglich
eGK G2.1 ohne Pin	**nein**
GesundheitsID	ja

299 Aktuell wurden keine Use Cases identifiziert.

300

3.4.5 Versorgungsszenario 04

Der Versicherte befindet sich in und der LE außerhalb der LEI.

PoPP-Token über	Nutzung möglich
eGK G2.1 ohne Pin	ja
GesundheitsID	ja

Aktuell wurden keine Use Cases identifiziert.

3.4.6 Nicht unterstützte Use Cases

Bei den zum Zeitpunkt der Initialerstellung des Konzeptes nicht unterstützten Use Cases (RX_2.1) handelt es sich um Fälle, bei denen der Versicherte eine eGK über sein eigenes Gerät (mit "VE-Endgerät" bezeichnet) per NFC anbindet. Es kann bei der Kontaktloskommunikation mit den eGK G2.1 im Gegensatz zum kontaktbehafteten Ansprechen nicht sichergestellt werden, dass die Daten "authentisch" aus der eGK ausgelesen werden. Eine Änderung dieser Zugriffsregeln lassen sich erst für eine neue Kartengeneration, z.B. eGK G3, ändern. Bei der Verfügbarkeit der PoPP-Lösung zum 1.1.2026 sind jedoch zu 100% G2.1 Karten im Feld verfügbar.

Beim CardLink-Verfahren konnten die aus der eGK ausgelesenen Informationen über die Informationssysteme der Krankenkassen (VSDM-Fachdienste) wieder zusammengeführt und abgeglichen werden. Mit der Annahme, dass dies mit VSDM2 nicht mehr in der Form zur Verfügung steht, ist eine sichere mobile Nutzung der eGK G2.1 ohne PIN in einem Versorgungskontext nicht möglich.

Offener Punkt:
Die gematik arbeitet weiterhin an entsprechenden Lösungsvorschlägen, um die kontaktlose Nutzung der eGK G2.1 ohne PIN zukünftig im Kontext PoPP zu ermöglichen und somit die bisher nicht erfüllten Use Cases zu unterstützen.

3.5 Nachnutzende TI-Anwendungen und Dienste

Das PoPP-Token weist nach, welcher Versicherte und welche Leistungserbringerinstitution sich zu einem bestimmten Zeitpunkt in einem Versorgungskontext befunden haben. Er dient der LEI nach der Authentifizierung an einer TI-Fachanwendung als Autorisierungsnachweis, um an die notwendigen Daten des behandelten Versicherten zu gelangen.
Die jeweilige TI-Anwendung entscheidet, in welchem Zeitraum nach Ausstellung das PoPP-Token als Nachweis akzeptiert wird. Jede TI-Anwendung hat damit die Möglichkeit eigene Regularien um- und durchzusetzen.

4 Technische Konzeption

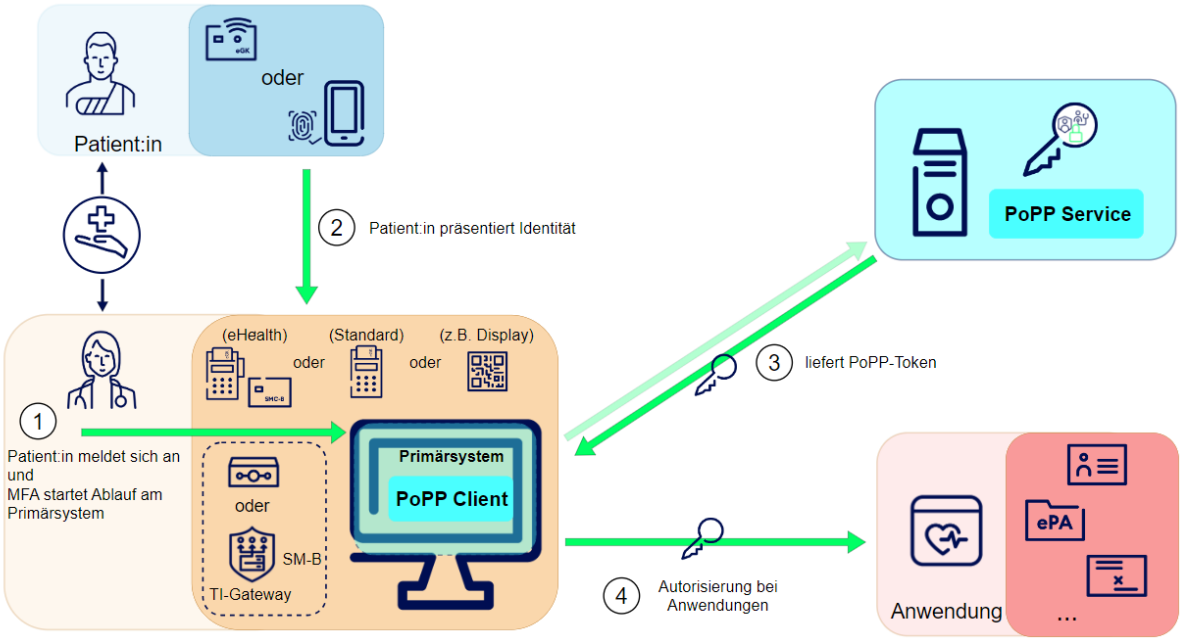

Abbildung 1 Überblick PoPP-Lösung

PoPP ("Proof of Patient Presence") ist wie bereits beschrieben ein Nachweis, der belegt, dass ein Versicherter sich zu einem bestimmten Zeitpunkt in einem Versorgungskontext mit einer bestimmten Leistungserbringerinstitution befindet. Dabei ist es die Aufgabe der PoPP-Lösung, die Authentifizierung der Leistungserbringerinstitution durchzuführen und durch Authentifizierung per GesundheitsID oder Verifikation des Vorhandenseins der gültigen eGK die Bestätigung des Versorgungskontexts durch den Versicherten einzuholen. Das Ergebnis ist ein Token, der ausschließlich dem Leistungserbringer zur Autorisierung für den Zugriff auf die Daten des Versicherten bei einer Anwendung dient.

- Versicherte, die sich mit ihrer eGK oder ihrer GesundheitsID repräsentieren, und Leistungserbringer (repräsentiert durch die SM(C)-B ihrer LEI) befinden sich zu dem dedizierten Zeitpunkt in einem Versorgungskontext.
- Der Beweis, dass Versicherte und Leistungserbringer zusammentreffen, wird mittels eines zentralen Dienstes vertrauenswürdig attestiert (PoPP-Service).
- Der PoPP-Service erstellt ein positives Ergebnis (PoPP-Token), wenn die Authentisierung der LEI und die Authentisierung bzw. Verifikation des Versicherten vertrauenswürdig bestätigt wird.
- Bei Versicherten, die sich mit ihrer eGK repräsentieren, reicht der Besitz der Karte aus. Der PoPP-Service stellt sicher, dass die Daten von der eGK auf Gültigkeit und Echtheit geprüft werden. Eine Verifizierung des Versicherten über eine PIN-Eingabe findet nicht statt.
- Bei Versicherten, die sich mit ihrer GesundheitsID repräsentieren, findet eine Authentifizierung statt.

Um eine zukunftssichere Lösung zu erhalten, wird die Entkopplung von Authentisierung ("wer bin ich?") und Autorisierung ("was darf ich?") gefordert. Aus diesem Prinzip leiten sich Anforderungen an die PoPP-Lösung ab, während es sich verbietet, anwendungsspezifische Anforderungen aufzunehmen.

Der PoPP-Service erzeugt ein authentisches PoPP-Token; es müssen also die verwendeten Informationen authentisch zum PoPP-Service gelangen bzw. müssen diese für den PoPP-Service so überprüfbar sein, dass er seinerseits die Authentizität verifizieren kann.
Zur Erstellung des PoPP-Token müssen

- seitens der Versicherten ihre KVNR hinsichtlich Authentizität geprüft im PoPP-Service vorliegen.
- seitens der LEI die Telematik-ID hinsichtlich Authentizität geprüft im PoPP-Service vorliegen.

4.1 PoPP-Token

Der PoPP-Service erstellt den PoPP-Token als Nachweis für den Versorgungskontext und signiert ihn. Das signierte PoPP-Token wird als Antwort auf den Request von PoPP-Client/ Primärsystem über den sicheren Kanal zurückgesendet.

Der Versorgungsnachweis (PoPP-Token) wird umgesetzt durch ein Token mit den Inhalten (1)-(6).

1. KVNR als Identität des Versicherten - inkl. der Information, ob die Quelle die eGK oder die GesundheitsID ist
2. IK-Nummer als Kassenzugehörigkeit des Versicherten
3. Telematik-ID als Identität der Institution
4. Zeitstempel der Token-Erstellung
5. Signatur über die Daten (1)-(4)
6. Zertifikat (mit Public Key) zur Verifikation der Signatur

Für die Signatur des PoPP-Tokens verwaltet der PoPP-Betreiber die Signing Keys. Alle PoPP-Token Signing Keys werden über die Komponenten PKI zertifiziert. Entsprechende X.509 Zertifikate werden in den PoPP-Token aufgenommen, damit die Fachdienste die Signatur als authentisch verifizieren können.

4.1.1 Unterstützung für die Migration von Fachanwendungen

Zusätzlich zum eigenständigen PoPP-Token wird durch den PoPP-Service zur Abwärtskompatibilität ein Prüfnachweis nach VSDM 1.0 Spezifikation bereitgestellt. Ein so erstellter Prüfnachweis ist technisch identisch zum aktuellen Prüfnachweis, welcher im Rahmen von VSDM+ verwendet wird.
Dadurch wird für die Übergangszeit mehr Flexibilität bei der Migration der ePA und des E-Rezeptes sichergestellt. Das Primärsystem kann wahlweise den PoPP-Token oder den Prüfnachweis verwenden, um einen Versorgungskontext nachzuweisen.
Hierfür wird der HMAC-Schlüssel des PoPP-Services über die vorhandenen betrieblichen Prozesse an die E-Rezept und ePA Fachdienste verteilt, sodass die vom PoPP-Service ausgestellten Nachweise verifiziert werden können.
Eine Verwendung dieser Prüfnachweise für die Abrechnung muss ausgeschlossen sein, da keine online-Überprüfung des Versicherungsstatus stattgefunden hat.

4.2 PoPP mit eGK

Die Erstellung des PoPP-Token erfolgt nach Authentifizierung der LEI beim PoPP-Service mittels einer SM-B Identität (Karte oder HSM) und dem Nachweis der Anwesenheit der eGK. Der dazu verwendete PoPP-Client wird als Funktionsteil innerhalb des Primärsystems umgesetzt. In der Architektur sind stationäre und mobile Szenarien sehr ähnlich.

4.2.1 Architektur in der LEI

Es wird angenommen, dass die folgende Ausstattung bei der LEI bereits vorliegt:

- 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 HSM des HSK,
- Primärsystem (PS) in der Rolle des PoPP-Clients,
- Möglichkeit der kontaktbehafteten Anbindung der eGK entweder A) über einen Standard-Kartenleser oder B) über eH-KT und Konnektor.

In der folgenden Darstellung ist die Architektur der PoPP-Lösung für ein Vor-Ort-Szenario mit vorhandener TI-Infrastruktur dargestellt.

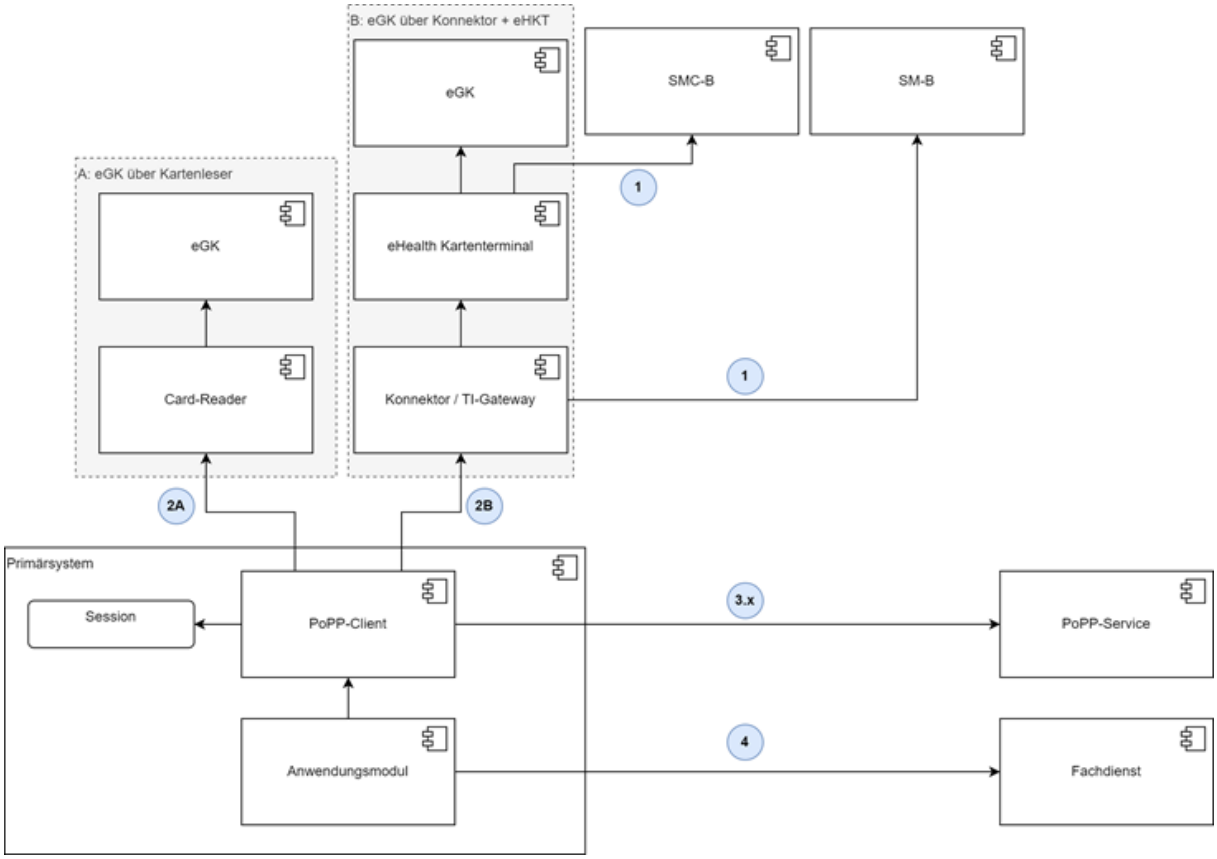

Abbildung 2 LEI-Architektur PoPP mit eGK

420 Die grundsätzliche Idee zur Erstellung des PoPP-Tokens wird anhand des Konzepts wie
421 folgt erläutert:

#	Ablauf
1	Die LEI (PoPP-Client) authentifiziert sich gegenüber dem PoPP-Service über eine freigeschaltete SM-B. Hierfür wird eine vorhandene Konnektor-Schnittstelle "externalAuthenticate" verwendet. Die Authentifizierung erfolgt direkt zwischen Client und Service im Challenge-Response Verfahren. Der PoPP-Client erhält einen Access-Token, den sogenannten PoPP-Service Access-Token, der zur authentifizierten Kommunikation mit dem PoPP-Service im Rahmen einer Session verwendet wird. Der PoPP-Service bestimmt in welchen Zeitabständen sich der PoPP-Client re-authentifizieren muss.
2A	**Option A:** Die eGK wird in ein Standard-Kartenlesegerät gesteckt Der PoPP-Client bekommt das Stecken der eGK mit (z.B. über PC/SC oder WinCard API). Der PoPP-Client kann jetzt auf Anfrage des PoPP-Services die APDU-Sequenzen an die eGK schicken und die Antworten lesen.
2B	**Option B**: Die eGK wird in ein eH-KT gesteckt Das Primärsystem bekommt das Stecken der eGK mit (z.B. über Konnektor CETP Event) und kann den CardHandle zur nachfolgenden Kommunikation mit dem Konnektor an den PoPP-Client übergeben. Der PoPP-Client ist jetzt in der Lage über eine Konnektor-Schnittstelle die APDU-Sequenzen an die eGK zu schicken und die Antworten zu lesen.
3	Der PoPP-Client öffnet eine bidirektionale WebSocket Verbindung zum PoPP-Service. Die Verbindung wird über den PoPP-Service Access-Token authentifiziert. Der PoPP-Service beginnt diesen Ablauf. Der PoPP-Client vermittelt die Kommunikation zwischen PoPP-Service und eGK. Die APDU-Sequenzen vom PoPP-Service werden durch den PoPP Client 1:1 an die eGK weitergeleitet. Die Antworten der eGK werden vom PoPP-Client 1:1 an den PoPP-Service weitergeleitet.
3.1	Card-to-Card-Authentisierung (C2C) zwischen eGK und PoPP-Service (CVC mit Null-Flaglist) - der PoPP-Service überprüft die Echtheit der eGK, und dass diese zum aktuellen Zeitpunkt bei der LEI vorliegt.
3.2	Etablierung eines Trusted Channel zwischen PoPP-Service und eGK durch Aushandlung von Session-Keys beim C2C
3.3	Authentisches Lesen des CH.AUT X.509 Zertifikats (enthält u.a. die KVNR und IK-Nummer)
3.4	Prüfung des 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.

#	Ablauf
3.5	Der PoPP-Service erstellt und signiert den PoPP-Token und übermittelt diesen an den PoPP-Client als letzte Nachricht der WebSocket Kommunikation mit dem PoPP-Client. Die Informationen über den Versicherten werden aus dem Zertifikat entnommen. Informationen über die LEI werden aus der PoPP-Client Authentifizierungs-Session (PoPP-Service Access-Token) entnommen.
4	Anschließend kann ein Anwendungsmodul innerhalb des Primärsystems den PoPP-Token als Autorisierung verwenden, z.B. zum Abruf der Versichertenstammdaten.

Die Besonderheit des Vor-Ort-Architekturkonzepts ist die Möglichkeit eine entsprechende Lösung mit einem Standard-Kartenleser (Option A) und mit einem eH-KT (Option B) durchzuführen.

Die Option A ermöglicht eine kostengünstige Beschaffung und mehr Wahlfreiheit bei den Endgeräten. Zudem funktioniert diese Option ohne Konnektor.

Hinweis: Für die Interaktion mit der eGK selbst ist keine Sicherheitsleistung des Lesegerätes (Kartenterminal) erforderlich. Die Sicherheitsleistung wird durch die eGK und den PoPP-Service erbracht. Bei der Card-to-Card-Freischaltung mit dem PoPP-Service wird durch das 0-flag-CV-Zertifikat serverseitig sichergestellt, dass die eGK keine schützenswerten Daten freischaltet. Darüber hinaus ist für das authentische Auslesen der KVNR aus der eGK keine PIN-Eingabe des Versicherten erforderlich, wodurch ein zertifiziertes Gerät auf Seiten des Leistungserbringers nicht erforderlich scheint. Mit dem Start der "ePA für alle" sind alle TI-Anwendungen so umgestellt, dass eine PIN-Eingabe für den Versorgungskontext beim Leistungserbringer nicht mehr erforderlich ist, also nun vielmehr der Besitz einer eGK ausreicht. Zusätzliche Sicherheit über den rechtmäßigen Besitz der Karte, gerade im Kontext VSDM oder ePA, bietet das auf der eGK verpflichtend aufzudruckende Bild des Versicherten, das im Zweifel mit der Person vom LEI-Personal abgeglichen werden kann.

Über die Option A können sich perspektivisch neue Leistungserbringergruppen an die TI anschließen, die durch die Verwendung eines TI-Gateways und SM-B teilweise auch vollständig auf ein eH-KT verzichten können. Ein anderer Vorteil kann das kostengünstigere Aufsetzen mehrerer Arbeitsplätze mit Standard-Kartenterminals sein, bspw. in einer größeren Apotheke.

Für die Unterstützung der Option B ist eine entsprechende Modifizierung der Konnektoren vorgesehen, die derzeit (06/2024) spezifiziert, vorabveröffentlicht und für ein PTV6-Release aufgeplant ist. Diese Variante mit der aktuellen PoPP-Lösung umzusetzen ist aus mehreren Gründen sinnvoll:

- Bestandshardware (eH-KT) kann weiterverwendet werden (Investitionsschutz)
- Es gibt auch ab 1.1.2026 noch immer Use Cases mit der eGK in denen ein zertifiziertes eH-KT am Konnektor zum Einsatz kommen muss (Bsp: Notfalldaten müssen nach SGB V noch immer auf der eGK gespeichert werden können).

Über den Transport der APDU-Sequenzen zwischen PoPP-Client (in Vertretung des PoPP-Services) und eGK unterscheiden sich die beiden Optionen nicht. Durch technische Maßnahmen des COS ist die Manipulation der Kommunikation in beiden Optionen ausgeschlossen.

4.2.2 Architektur mobil

Die Sicherheitsleistung der PoPP-Lösung für eGK baut auf dem Prinzip des authentischen Auslesens relevanter Informationen aus der eGK auf. In mobilen Szenarien ist davon auszugehen, dass Versicherte die eGK häufiger über die Kontaktlosschnittstelle ansprechen möchten. Die Kontaktloskommunikation mit eGK nutzt nach Eingabe der CAN das PACE-Protokoll. Die Zugriffsregeln der eGK verhindern den zusätzlichen Aufbau eines Trusted Channels zum PoPP-Service (zusätzlich zum PACE-Kanal). Für die PoPP-Lösung scheint es jedoch auch vor allem für Versicherte nicht zumutbar, einen kontaktbehafteten Kartenleser zu beschaffen und diesen in ihre Geräteinfrastruktur einzubinden.

Aufgrund dieser technischen Rahmenbedingungen sind die Nutzungsszenarien mit eGK ohne PIN mit dem Versicherten-Smartphone zumindest in der Initialveröffentlichung des PoPP-Konzepts nicht umsetzbar. Siehe dazu auch den Hinweis in 3.4.6- Nicht unterstützte Use Cases .

Dennoch können künftig mobile TI-Online-Nutzungsszenarien mit der PoPP-Lösung adressiert werden, sofern die behandelnden Leistungserbringer ein Kartenterminal mit kontaktbehafteter Kartenschnittstelle mit sich führen. Eine Einbindung in die Architektur nach Abschnitt 4.2.1 Option A (Standard-Kartenterminal) ist somit auch für mobile Anwendungen denkbar. Dabei ist es für die sichere Umsetzung unerheblich, ob das Kartenterminal selbst kontaktlos (bspw. via Bluetooth, WiFi) mit dem Endgerät des Leistungserbringers verbunden ist. Für das sichere Auslesen des CH.AUT Zertifikats von der eGK ist nur Voraussetzung, dass der direkte Zugriff auf die eGK mittels kontaktbehafteter Schnittstelle stattfindet.

Das Primärsystem (und damit der vermittelnde PoPP-Client) kann damit entweder auf dem mobilen Endgerät des Leistungserbringers mit einer Anbindung an die Praxis oder direkt zum TI-Gateway operieren oder das Kartenterminal ist über das Internet mit der eigenen Praxis und dem Praxissystem verbunden.

Hinweis: Mit der Weiterentwicklung der eGK (G3) soll die authentische kontaktlose Anbindung der Karte in der Zukunft sichergestellt werden. Inwieweit dann der Besitz der Karte bei den unterschiedlichen Nutzungsszenarien ausreichend ist, ist noch zu bewerten.

4.2.3 Telemedizin

Dieser Anwendungsfall wird nicht betrachtet, da eine Anbindung der eGK lediglich über die IT des Versicherten möglich wäre und dahingehend gelten die Aussagen im vorhergehenden Absatz.

4.2.4 Einordnung in die TI 2.0

Der generelle Umgang mit kartenbasierten Identitäten (eGKs) und entsprechenden Zertifikaten ist in dieser Form unverändert zur bestehenden TI und kann daher nicht direkt in der TI2.0 verortet werden. Eine bedeutsame Änderung zum Status quo ist jedoch, dass das sichere Auslesen der eGK weder vom Konnektor orchestriert noch über ein zertifiziertes eH-KT erfolgen muss. Zwei wesentliche Bestandteile der bisher notwendigen Basisinfrastruktur werden für diese Funktionalität damit nicht mehr benötigt. Zusätzlich ergibt sich der eigentliche "TI2.0"-Kontext aus der zukünftigen Nutzbarkeit der GesundheitsID der Versicherten im Versorgungskontext mit Leistungserbringern. (siehe auch 4.6- TI2.0 und Zero Trust)

4.3 PoPP mit GesundheitsID

Als Voraussetzung für den Einsatz der GesundheitsID muss der Versicherte diese bei seiner Krankenkasse bereits eingerichtet haben.

4.3.1 Architektur in der LEI

Wie auch bei der eGK-Lösung wird die folgende Ausstattung in der LEI angenommen:

- Einboxkonnektor mit eH-KT und SMC-B
- oder TI-Gateway mit Highspeed-Konnektor und SMC-B als Karte im eH-KT oder als SM-B im HSM des HSK,
- Primärsystem (PS) in der Rolle des PoPP-Clients,

Darüber hinaus muss die LEI über einen Bildschirm / Tablet verfügen, in dem ein individueller QR-Code angezeigt werden kann. Der individuelle QR-Code wird durch den PoPP-Service generiert und kann durch einen Versicherten nur einmalig verwendet werden, damit ein PoPP-Token nur unmittelbar mit dieser Behandlungs- bzw. Versorgungssituation zusammenhängen kann.

In der folgenden Darstellung ist die Architektur der PoPP-Lösung für ein Vor-Ort-Szenario mit vorhandener TI-Infrastruktur dargestellt.

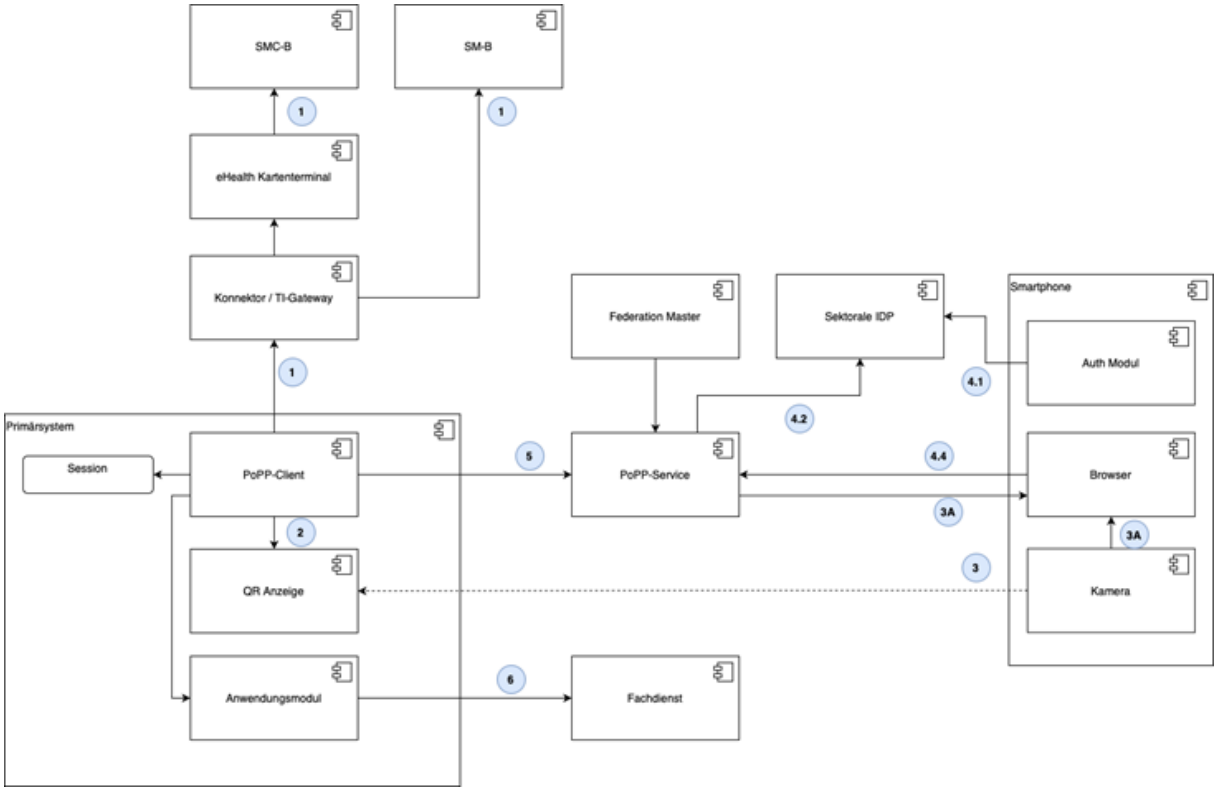

Abbildung 3 LEI-Architektur PoPP mit GesundheitsID

520 Die grundsätzliche Idee zur Erstellung des PoPP-Tokens wird anhand der Konzept-Skizze
521 wie folgt erläutert:

#	Ablauf
1	PoPP-Client authentifiziert sich gegenüber PoPP-Service mit einer freigeschalteten SM-B (Karte oder HSM). Es entsteht eine Session zwischen Client und Server, abgebildet über PoPP-Service Access-Token analog zum eGK Ablauf (s. oben).
2	PoPP-Client besorgt sich vom PoPP-Service einen an die LEI gebundenen Consent-Code. Der Consent-Code wird in Form eines Hyperlinks zum Scannen durch den Versicherten auf der QR-Anzeige dargestellt.
3A	Der Versicherte scannt den QR-Code mit der Smartphone-Kamera. Dabei öffnet sich über den Hyperlink der Browser mit der Web-Oberfläche des PoPP-Services. Der Versicherte wird informiert, dass für die Übermittlung der GesundheitsID-Daten an die LEI eine Anmeldung erforderlich ist. Es wird die Liste der unterstützten Sektoralen IDPs dargestellt, aus welcher der Versicherte seine Versicherung auswählen muss. Die Auswahl wird für zukünftige Abfragen im Browser gespeichert (LocalStorage oder Cookie). Beim nächsten Arztbesuch entfällt dieser Schritt.
3B	Alternativ kann das Scannen direkt in einer Versicherungs-App bzw. in GesundheitsID Authenticator App erfolgen. Dadurch wird die Wahl der Versicherung aus der Liste überflüssig und der gesamte Ablauf kann in einer App erfolgen.
4.1	Der Versicherte authentifiziert sich mit seiner GesundheitsID über den Sektoralen IDP gegenüber dem PoPP-Service.
4.2	Der PoPP-Service erhält vom Sektoralen IDP einen ID-Token, welcher unter anderem den Namen, die KVNR des Versicherten und die IK-Nummer der Versicherung enthält.
4.3	In der Web-Oberfläche des PoPP-Services oder direkt in der Versicherungs-App wird ein Consent-Screen angezeigt mit der Aufforderung der Bestätigung, dass die GesundheitsID-Daten an die LEI übertragen werden.
4.4	Versicherte bestätigt die Übermittlung der GesundheitsID-Daten an angegebene LEI. Über den eindeutigen Consent-Code wird die Bestätigung der laufenden Session zugeordnet und die LEI kann den PoPP-Token über Primärsystem abrufen. PoPP-Service vermerkt die Entscheidung und die Daten serverseitig.
5	PoPP-Service erstellt einen PoPP-Token anhand der Daten aus dem ID-Token und aus der über Consent-Code identifizierten LEI. Der PoPP-Client kann über die authentifizierte Session und den Consent-Code die erteilte Genehmigungen (Consents) abrufen. Dabei wird geprüft, dass der Consent-Code im zulässigen Zeitraum ausgestellt wurde ("Freshness"). Es muss berücksichtigt werden, dass nach dem Scannen des QR-Codes dem Versicherten genug Zeit für die Anmeldung bleibt.

#	Ablauf
6	Anschließend kann ein Anwendungsmodul innerhalb des Primärsystems den PoPP-Token als Autorisierung verwenden, z.B. zum Abruf der Versichertenstammdaten.

4.3.2 Architektur mobil

Da sich ein Versicherter mittels eigenem Smartphone authentifiziert, bedarf es bei mobilen Szenarien lediglich der Möglichkeit einen QR-Code zwischen Versicherten und Leistungserbringer anzeigen zu können. Der QR-Code wiederum ist ein Link, der auch über andere Wege übertragen werden kann. In telemedizinischen Szenarien ist die Übermittlung eines Links in einem Chat denkbar, der bei Öffnen mittels Smartphone oder PC den entsprechenden Authentifizierungsworkflow über den sektoralen IDP startet. Der dem Versicherten übermittelte Link repräsentiert eine individuelle, einmalig nutzbare Einladung, die im Auslösen einer Autorisierungsanfrage resultiert.

4.3.3 Telemedizin

Der Ablauf ist identisch. Lediglich das Anzeigen des QR-Codes bzw. die Übermittlung des Links zum Start des Authentisierung-Flow findet passend über das jeweils genutzte Telemedizin-Medium statt, also bspw. über einen Link als Text im Chat (wenn seitens Versicherten bereits das Smartphone genutzt wird) oder die Anzeige eines QR-Codes in einer Video-Konferenz (wenn seitens Versicherten der PC oder eine andere Video-Konferenz-Technik genutzt wird).

4.4 Anpassungsbedarf bestehender Produkte

Um PoPP zu unterstützen müssen folgende bestehende Komponenten und Dienste der TI angepasst werden:

- **Primärsysteme** - zur Unterstützung der Funktionalität "PoPP-Client" für Abläufe mit eGK und GesundheitsID
- **Konnektor** - zur Unterstützung bei Verwendung von eH-KTs bei PoPP mit eGK in der LEI
- **Fachdienste** - zur Nutzung des PoPP-Tokens
- **Frontend des Versicherten (FdV)** - optional um den Ablauf mit eGK oder GesundheitsID direkt innerhalb der Versicherungs-App umsetzen zu können

4.4.1 Primärsysteme (PS)

Das PS fordert das PoPP-Token an, vermittelt zwischen PoPP-Service und Authentisierungsmittel (eGK oder GesundheitsID) und sendet den PoPP-Token an die nutzenden Fachdienste. Der PoPP-Client ist dabei als Erweiterung der bestehenden Primärsysteme zu betrachten und muss im Rahmen eines PS-Updates auf den Rechnern der LEI ausgerollt werden.

Der Funktionsumfang des PoPP-Clients ist im Kapitel 7- PoPP-Client beschrieben.

4.4.2 Konnektor

Für eine Nachnutzung von bereits beschafften und finanzierten eH-KTs (siehe dazu 4.2.1-Architektur in der LEI Option A) muss eine neue Funktionalität für das Auslesen von eGK Daten durch den PoPP-Service über den Konnektor spezifiziert und ausgerollt werden. Dazu wird das SOAP-Interface des Konnektors zum PS erweitert.

Der Konnektor erhält eine neue Schnittstellen-Operation, mit der ein Client (PoPP-Client, bzw. Primärsystem) einen sicheren Kanal zwischen einer eGK und dem PoPP-Service vermitteln kann.
In diesem sicheren Kanal werden Zertifikats-Daten sicher von der eGK gelesen und an den PoPP-Service übertragen.
Anschließend wird der sichere Kanal wieder abgebaut und die eGK zur anderweitigen Verwendung freigegeben.
Der vom PoPP-Client angefragtes PoPP-Token wird nicht über diesen Kanal verschickt.

Diese Änderung am Konnektor ist für Konnektor PTV6 geplant. Inhalt und Umfang der Änderung sind durch einen PoC der gematik gestützt und wurden im Rahmen eines Impulsvortrags im TI-Ausschuss bereits vorgestellt.

4.4.3 Fachdienste

Der Fachdienst prüft die Signatur des PoPP-Token und verwendet dessen Informationen im Rahmen der Zugangsberechtigung ergänzend zur Authentifizierung der anmeldenden LEI. Hierfür muss eine entsprechende Schnittstellen-Erweiterung vorgesehen werden. Die Verantwortung zu den Autorisierungsprozessen in den TI-Anwendungen liegt ebenfalls in der gematik. Alle Teams der Anwendungen sind eng bei der PoPP-Konzeption eingebunden. Explizit genannt werden: VSDM2, ePA für alle, E-Rezept.

Während die Anwendung VSDM2 ausschließlich mit dem PoPP-Token funktionieren wird, sind die Anwendungen ePA für alle und E-Rezept angewiesen einen Parallelbetrieb bei der Akzeptanz von VSDM-Prüfungsnachweis und PoPP-Token zu gewährleisten.

4.4.4 Frontend des Versicherten (FdV)/ Kassen-Apps

Das Frontend des Versicherten (FdV) muss in der Lage sein, einen individuellen Registration-Code/ Consent-Code, beispielsweise in Form eines QR-Codes zu verarbeiten, um so eine Authentifizierungssession mit einem Versicherten mit GesundheitsID zu starten.
Es ist möglich, dass von so einer Anpassung auch die Integration des Authenticator Moduls in einem FdV betroffen ist.
Dabei ist auch zu berücksichtigen, dass nicht alle Kassen-App Nutzer, die die GesundheitsID verwenden, auch eine ePA und damit ein ePA-FdV haben.

4.5 Neue Produkte

4.5.1 PoPP-Service

Für die Umsetzung der PoPP-Lösung ist im Vergleich zur heutigen Infrastruktur ein zusätzlicher zentraler Dienst erforderlich, der eine sichere Datenverarbeitung (Vermeidung Profilbildung) und unter anderem die Sicherheitsleistung des authentischen sicheren Auslesens der eGK übernimmt. Dieser Dienst, der PoPP-Service, wird durch die

gematik ausgeschrieben und vergeben. Weiteres ist in Kapitel 6- PoPP-Service dargelegt.

4.5.2 Hardware in LEI

Ein USB-, LAN- oder kontaktlos verbundener Kartenleser, mit mindestens einem kontaktbehafteten Slot zum Stecken der eGK, übernimmt die Kommunikation mit der eGK und kann ab dem 1.1.2026 in einer LEI für die Erfüllung der PoPP-Lösung mittels eGK eingesetzt werden, sofern eH-KT und Konnektor nicht vorhanden sind bzw. diese nicht genutzt werden sollen. Diese neue Komponente muss in der LEI installiert und am Primärsystem konfiguriert werden. Darüber hinaus sind selbige oder zusätzliche Geräte für die Nutzung im mobilen Kontext möglich.

Sofern noch nicht vorhanden, muss den Nutzern der GesundheitsID ein Bildschirm für das Anzeigen eines individuellen QR-Codes für den Start des PoPP-Workflows zur Verfügung stehen.

4.6 TI2.0 und Zero Trust

Die Architektur der PoPP-Lösung basiert maßgeblich auf Prinzipien von TI2.0, insbesondere:

- Universelle Erreichbarkeit des PoPP-Services über das Internet
- Verwendung der OAuth2 und OpenID Connect Protokollfamilie
- Kommunikation zwischen PoPP-Client und PoPP-Service wird über Zero Trust Mechanismen abgesichert (siehe auch gemF_Zero-Trust).
- Weitgehende Unabhängigkeit vom Konnektor mit den Ausnahmen, dass
  - derzeit die SM(C)-B als Authentisierungsmittel benötigt wird, die nur über Konnektor oder TI-Gateway ansprechbar ist.
  - für die Abwärtskompatibilität (Option B mit eGK) eine Konnektor Anpassung durchgeführt wird, um bestehende Komponenten besser nachnutzen zu können.

Die Einführung der TI2.0 Funktionalitäten erfolgt bedarfsgerecht und unter der Berücksichtigung aktueller technischer Möglichkeiten. Ebenso wird darauf geachtet, dass die Komplexität den reibungslosen Betrieb und die engen Zeiträume nicht gefährdet. Als ersten Schritt werden folgende Mechanismen vorgesehen:

- Client-Authentisierung des Primärsystems erfolgt über die freigeschaltete SM(C)-B. Durch direktes Challenge-Response Verfahren zwischen Primärsystem (PoPP-Client) und PoPP-Service wird eine Hardware-basierte Vertrauensbeziehung zwischen Primärsystem und PoPP-Service hergestellt.
- Primärsysteme müssen die Selbstauskunft über sich selbst und ihre Umgebung bereitstellen. Dies erfolgt im Rahmen des Session Aufbaus zwischen Primärsystem und PoPP-Service. Hierbei handelt es sich nicht um eine Attestierung der Primärsystemsoftware per se, bietet jedoch eine gute Möglichkeit im Laude der Zeit auf die Änderungen (oder nicht Änderungen) der Umgebungen zu reagieren.
- PoPP-Service erhält einen Policy Enforcement und Policy Decision Point, die zwei Basiskomponenten von Zero Trust. Dadurch kann die gematik die Zugriffsregeln

auf den PoPP-Service dynamisch kontrollieren und die Voraussetzungen für das Ausstellen des PoPP-Tokens festlegen.

Die Zero Trust Basiskomponenten übernehmen die wesentlichen Sicherheitsleistungen für den Zugang zum PoPP-Service:

- Client Authentifizierung mittels SM(C)-B
- OAuth2 Authorization Server zum Ausstellen der PoPP-Token
- Relying Party gegenüber GesundheitsID
- Session Management
- Policy basierte Zugriffskontrolle

Das von PoPP-Service ausgestellte PoPP-Token wird kryptographisch abgesichert. Zudem wird das PoPP-Token über die in Zero Trust definierten Token-Binding Mechanismen an die konkrete Instanz des Primärsystems bzw. die Session zwischen PoPP-Client und PoPP-Service gebunden (DPoP, [RFC9449]).

Das PoPP-Token wird als ein self-contained JWT OAuth2 Access-Token abgebildet, der standardkonform für die Autorisierung des Zugriffs auf einen Fachdienst verwendet werden kann. Die Prüfung des PoPP-Tokens kann durch die Fachdienste autark erfolgen (insb. auch im HSM bei ePA für alle) und hat keine nennenswerte Auswirkung auf Performance oder Verfügbarkeit des Fachdienstes.

Die Backendkomponenten unterstützen Monitoring (Healthcheck), Betriebsdatenerfassung und Security Monitoring über die SIEM Systeme.

5 Datenschutz und Informationssicherheit

Die PoPP-Lösung muss auf zwei wesentliche Bedrohungen mit entsprechenden Maßnahmen reagieren: a) Erhalt von PoPP-Token durch Unberechtigte und b) Profilbildung über Versicherte (insbesondere welche Leistungserbringer sie aufsuchen).

Zu berücksichtigen ist der Betreiber des PoPP-Service, der sowohl Zugriff auf den Token-Signaturschlüssel hat und sich beliebige PoPP-Token ausstellen kann, als auch Zugriff auf die verarbeiteten Daten hat, wodurch die genannte Profilbildung möglich wird. Daher wird für den PoPP-Service eine VAU sowie ein sicherer Schlüsselspeicher (HSM) gefordert, die den Betreiber mit Hilfe von technischen und organisatorischen Maßnahmen vom Zugriff auf den Signaturschlüssel und die verarbeiteten Daten ausschließt.

Um sicherzugehen, dass nur Leistungserbringerinstitutionen PoPP-Token anfragen und abrufen können, findet eine Authentifizierung der LEI mittels der SMC-B (inkl. Prüfung auf Besitz des privaten Schlüssels) statt. Aus dieser Authentifizierung kann zugleich die Telematik-ID authentisch ermittelt werden, sodass sichergestellt ist, dass das PoPP-Token auch für die korrekte LEI ausgestellt wird.

Damit gewährleistet ist, dass nur für Versicherte, die in einem Versorgungskontext mit der LEI stehen, ein PoPP-Token ausgestellt wird, verifiziert der PoPP-Service die Identität des Versicherten, indem er entweder eine Authentifizierung über die GesundheitsID durchführt oder die Anwesenheit der eGK des Versicherten authentisch prüft. In beiden Fällen erhält der PoPP-Service im Zuge der Verifikation auf authentischem Wege die KVNR des Versicherten.

Die Prüfung auf Anwesenheit der eGK basiert auf einer logischen Verbindung direkt zwischen PoPP-Service und eGK (Card-to-Card-Authentication mit Aushandlung von Sessionkeys und anschließendem Secure Messaging). Dadurch wird die Sicherheit in den geprüften und zugelassenen Endpunkten (PoPP-Service und eGK) durchgesetzt und sämtliche Komponenten dazwischen sind nur für die Vermittlung der Kommunikation verantwortlich und liefern keine Sicherheitsleistung. Daher bedarf es weder geprüfter Kartenterminals noch eines geprüften Software-Clients. Entsprechend können für PoPP neben Konnektor und eH-KT auch Standard-Kartenleser verwendet werden und der PoPP-Client ist kein Zulassungsgegenstand, sondern Teil des PS.

Der Versorgungskontext wird vom PoPP-Service durch die technische Verknüpfung der Authentifizierung der LEI und der Verifikation der Versicherten-Identität innerhalb einer Session hergestellt, wodurch nur PoPP-Token erstellt werden, bei denen ein konkreter Zusammenhang von LEI und Versicherten Aktion besteht.

Sämtliche Kommunikation zum und vom PoPP-Service wird hinsichtlich Integrität und Vertraulichkeit geschützt (TLS). Dabei muss der PoPP-Client das TLS-Zertifikat des PoPP-Service prüfen. Dies ist eine Sicherheitsleistung, jedoch identisch mit der des E-Rezept-Clients und der zukünftigen Clients für ePA für alle, welche ebenso Teil des Primärsystems sind.

Da der PoPP-Service im Internet zu erreichen ist, werden die Schnittstellen entsprechend gegen Angriffe aus dem Internet abgesichert. Somit ist auch das Erlangen von PoPP-Token durch Hacking-Angriffe ausreichend abgewehrt.

Sollten Unberechtigte an ausgestellte PoPP-Token gelangen, sind diese durch eine Bindung an den berechtigten Token-Empfänger wertlos. Technisch ist dies durch DPoP umgesetzt, wodurch bei der Token-Abfrage ein Schlüsselpaar seitens des Clients verwendet wird, welches (inkl. Prüfung auf Besitz des privaten Schlüssels) auch bei der

Token-Nutzung verwendet werden muss. Somit kann nur der Client, der den Token abgerufen hat (und sich dabei authentisiert hat), den Token auch verwenden.

Die genannten Sicherheitsfunktionen müssen entsprechend detailliert und in Anforderungen überführt werden. Ebenso muss mit fortschreitender Spezifikation die Sicherheitsbetrachtung ebenso fortgeschrieben werden. Nach jetzigem Konzeptionsstand sind die angedachten Maßnahmen aber ausreichend, eine hinreichend sichere PoPP-Lösung zu gewährleisten.

Hinweis für nutzende Anwendungen: Trotz der im Rahmen von PoPP umgesetzten Sicherheitsmaßnahmen liegt es immer im Ermessen der jeweiligen Anwendung, ob diese einen PoPP-Token akzeptiert und welche ggf. weiteren Maßnahmen die Anwendung umsetzt, wie bspw. eine eigene Authentifizierung der zugreifenden LEI und einem Abgleich der Telematik-ID aus dieser Authentifizierung und jener aus dem PoPP-Token. Ebenso wird aus dem PoPP-Token ersichtlich, wie die Verifikation des Versicherten stattgefunden hat (eGK oder GesundheitsID), woran Anwendungen ggf. weitere Prüfungen / Entscheidungen knüpfen können.

6 PoPP-Service

Der PoPP-Service wird als ein zentraler Dienst der TI2.0 verstanden, dessen Umsetzung und Betrieb ausgeschrieben werden.

6.1 Systemarchitektur

Die Systemarchitektur für den PoPP-Service umfasst neben dem PoPP-Service selbst weitere Komponenten, die ebenfalls beim PoPP-Service Betreiber verortet sind.
Die PoPP-Service Betriebsumgebung umfasst neben dem eigentlichen PoPP-Service ein Zero Trust Cluster mit Policy Enforcement Point (PEP) und Policy Decision Point (PDP), der von der gematik als produktive Implementierung als Container-Images dem PoPP Service Betreiber zur Verfügung gestellt wird und von ihm in seiner Betriebsumgebung konfektioniert werden muss. Diese Zero Trust (ZT) Basiskomponenten PDP und PEP liefern Daten an einen Telemetrie Client. Der PDP bezieht die anzuwendenden Policies und Daten von Policy Information Point (PIP) und Policy Administration Point (PAP) der zentralen Betriebsüberwachung.
Die Telemetrie Komponente sammelt Telemetrie-Daten der PoPP-Clients der Primärsysteme, sowie von den ZT Komponenten PEP und PDP. Diese Daten werden ggf. aggregiert oder anders vorab verarbeitet und dann dem zentralen Betriebsdatenerfassungs(BDE)-Server über die BDE-upload Schnittstelle bereitgestellt.
Ebenso werden Plattform- und Infrastrukturdaten aus der PoPP-Service Betriebsumgebung überwacht (Monitoring-Komponente) und Monitoring-Daten ebenfalls dem BDE-Server übermittelt.
In der LE-Umgebung wird der PoPP-Client als Teil des Primärsystems (PS) benötigt (siehe Kapitel 7 - PoPP-Client). Daneben wird vorausgesetzt, dass die TI-Zugangskomponenten TI-Gateway/ Konnektor mit einem eH-KT und/ oder einem Standard-Kartenleser verwendet werden.
Die sektoralen IDP, die jeweils bei den betreibenden Kassen verortet sind, tragen für die Authentisierung der Versicherten mit der GesundheitsID bei.
Der Bereich "Zentrales Monitoring und Betriebsüberwachung" wird in der Verantwortung der gematik betrieben. Relevant sind hier die zentralen Zero Trust Komponenten PIP und PAP, die jeweils das aktuelle Regelwerk für den PoPP-Service Betreiber bereithalten. Der TI SIEM-Server nimmt Sicherheitsinformationen und Events vom PoPP-Service Betreiber entgegen. Der BDE-Server nimmt neben PoPP-Service spezifischen Telemetrie Daten auch Daten aus dem Betreiber-Plattform-Monitoring entgegen.

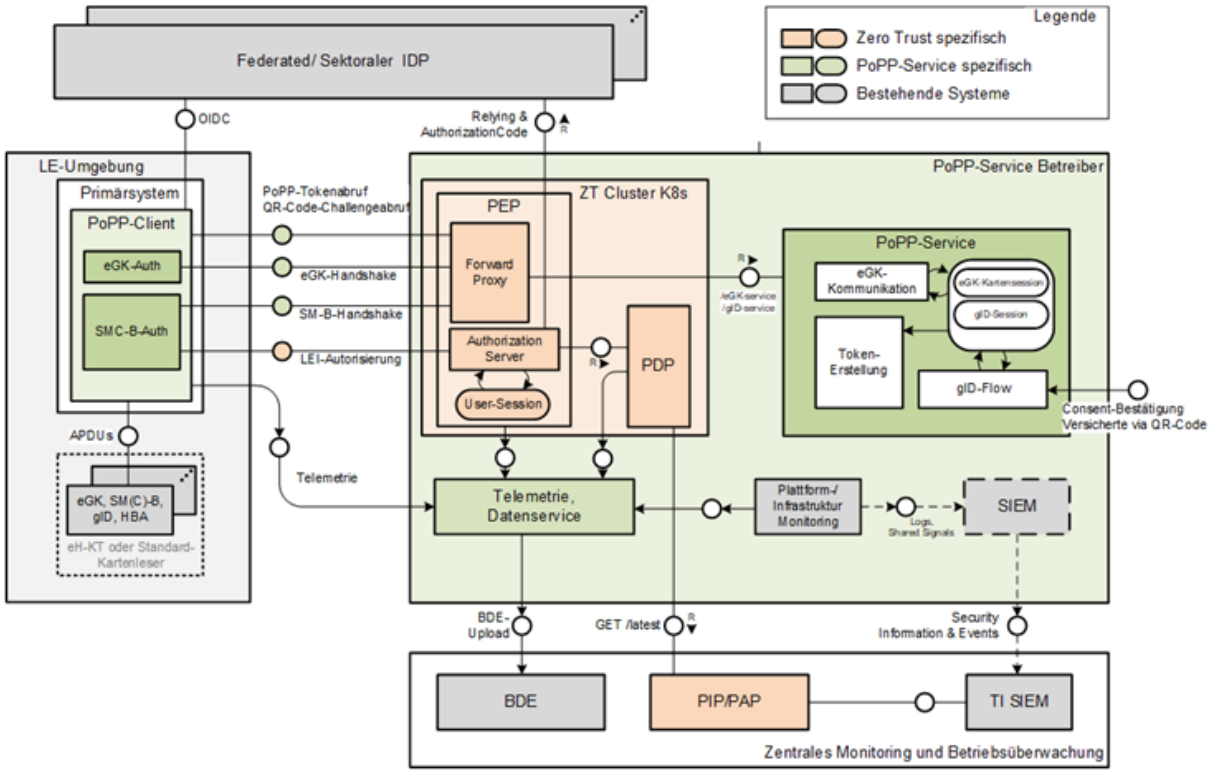

Abbildung 4 Systemarchitektur für die PoPP-Lösung

6.2 Komponentenzerlegung PoPP-Service

Der PoPP-Service ist ein zentraler Dienst in der TI2.0 mit folgenden Features / Funktionsblöcken:

- ZT Basiskomponente PEP hat einen:
  - Authorization Server, der die LEI-Autorisierung im Sinne einer Zugangsautorisierung des PoPP-Clients bei PoPP-Service über eine freigeschaltete SM(C)-B ermöglicht.
  - Forward Proxy, der nach erfolgter LEI-Autorisierung die Nachrichten eines PoPP-Clients für die Erstellung von PoPP-Token an den PoPP-Service weiterleitet.
- Modul zur Kommunikation mit der eGK im PoPP-Service (Session basierte Bearbeitung der eGK-Handshake Aufrufe , Zusammenführen von eGK Daten (KVNR) und SM(C)-B Daten (Telematik ID), Übergabe an Modul zur Token Erstellung
- dem Modul zur Behandlung des GesundheitsID-Flows im PoPP-Service und
- ein Modul zur Token-Erstellung
  - erstellt den PoPP-Token (siehe 4.1- PoPP-Token),
  - signiert den PoPP-Token mit einer nonQES Signatur mit der TI-Komponenten-Identität des PoPP-Service und gibt den signierten Token über die Schnittstelle eGK-Service/ gID-Service an den PoPP-Client zurück.

- stellt sicher, dass der im PoPP-Token enthaltene Zeitstempel vertrauenswürdig ist. Dazu synchronisiert sich der PoPP-Service mit einer vertrauenswürdigen Zeitquelle im Internet.

- der Telemetrie und Datenservice (siehe oben 6.1- Systemarchitektur)

6.3 Schnittstellen

6.3.1 Zugangsautorisierung des PoPP-Clients

Diese Schnittstelle ("LEI-Autorisierung" in Abbildung zur Systemarchitektur) dient der regelmäßigen Authentifizierung und Zugangsautorisierung der PoPP-Clients für den Zugang zu PoPP-Service Schnittstellen für die LE-Institutionen. Die Schnittstelle basiert auf dem OAuth2 Protokoll. Nach erfolgreicher Zugangsautorisierung wird dem PoPP-Client ein Access-Token ausgestellt, welcher als Autorisierung-Credential zum Zugriff auf weitere Schnittstellen des PoPP-Services dient, das PoPP-Service Access-Token. Für die Dauer der Gültigkeit des PoPP-Service Access-Tokens wird eine Session zwischen PoPP-Client und PoPP-Service aufgebaut; nach Ablauf des PoPP-Service Access-Tokens müssen die Clients sich erneut autorisieren lassen (und sich dabei authentisieren).

Die Zugangsautorisierung und das Session Management wird durch die Zero Trust Basiskomponenten übernommen, die entsprechend in der Betriebsumgebung des PoPP-Services konfiguriert und ausgeführt werden.

Für die Authentifizierung der LEI wird die SM(C)-B verwendet. Da die SM(C)-B in der LE-Umgebung freigeschaltet ist, kann die Authentifizierung automatisch durch den PoPP-Client erfolgen, d.h. insbesondere ohne Benutzerinteraktion. Die SM(C)-B dient gleichzeitig zur Authentifizierung des PoPP-Clients im Sinne von Zero Trust Client Authentifizierung. Auf eine separate Registrierung der PoPP-Clients und Client-Credentials-Management wird zunächst verzichtet, insbesondere aus betrieblichen Gründen und weil die Client-Authentifizierung und Attestation für Desktop-Betriebssysteme noch keinen ausreichenden Reifegrad hat. Durch die Verfügbarkeit der SM(C)-B können die PoPP-Clients sich ohne zusätzliche Komplexität als LEI-Softwaresysteme ausweisen, durch die im Zertifikat enthaltene Telematik-ID können die PoPP-Clients eindeutig der LEI zugeordnet werden.

Die Zugangsautorisierung erfolgt direkt zwischen den ZT-Basiskomponenten des PoPP-Services und der SM(C)-B (vermittelt über den PoPP-Client). Dadurch, dass die ZT-Basiskomponenten die Authentifizierung übernehmen, ist diese Funktion auch für andere Dienste nachnutzbar.

Die Zugangsautorisierung wird in folgenden Schritten durchgeführt:

- PoPP-Service stellt eine Nonce bereit (Abkürzung für "Number used once"). Wenn ein Nonce in einer Nachricht enthalten ist, kann diese Nachricht nicht wieder abgespielt werden, weil die Nonce einzigartig und nur einmal gültig ist (die beteiligten Systeme müssen die Nonce entsprechend abspeichern).
- Der PoPP-Service erwartet, dass die PoPP-Clients das DPoP-Verfahren gemäß [RFC9449] verwenden. Hierdurch wird sichergestellt, dass alle Requests aus derselben Umgebung kommen und nur einmal abgesetzt werden können.
- Der PoPP-Client erstellt eine JWT private key Client Assertion gemäß [RFC7523] (siehe Kapitel 7.1.1- Zugangsautorisierung beim PoPP-Service).
- Die Client Assertion wird mit SM(C)-B signiert und enthält das AUT-Zertifikat (C.HCI.AUT).

- Der PoPP-Service prüft die Client Assertion wie folgt
  - Request enthält validen DPoP-HeaderDPoP Proof und enthält die Nonce
  - Die Nonce wurde bisher noch nicht genutzt und ist nicht älter als ein im PoPP-Service konfigurierter Zeitraum (gewöhnlich 15 Minuten)
  - Der öffentliche DPoP-Schlüssel wird nicht bereits länger als ein noch zu definierender Zeitraum genutzt
    (Abgleich gegen eine Datenbank der Fingerprints der öffentlichen Schlüssel, welche beim PoPP-Service angelegt und mit jedem neuen Schlüssel erweitert werden muss)
  - Client Assertion JWT ist gebunden an DPoP Schlüssel und an die Nonce
  - Client Assertion SM(C)-B Signatur ist gültig. Es werden ausschließlich ECC-Signaturen und Zertifikate unterstützt.
  - AUT-Zertifikat der SM(C)-B (C.HCI.AUT) ist nicht gesperrt, bestätigt durch OCSP
  - Alle Eingangsparameter erfüllen die Policy-Vorgaben, bestätigt durch ZT Policy Decision Point

Nach erfolgreicher Prüfung stellt der ZT Authorization Server des PoPP-Dienstes einen Access-Token, den PoPP-Service Access-Token für den Zugriff auf weitere Schnittstellen des PoPP-Services aus.
Diese Zugangsautorisierung muss regelmäßig in noch zu definierenden Zeiträumen wiederholt werden.

6.3.2 eGK-Verarbeitung

Die Schnittstelle eGK Verarbeitung ("eGK Handshake" in Abbildung zur Systemarchitektur) ermöglicht die Prüfung, dass dem PoPP-Client eine gültige eGK vorliegt. Die Schnittstelle basiert auf dem WebSocket Protokoll, die gematik stellt die Beschreibung der Schnittstelle im Async API Format (https://www.asyncapi.com/) zur Verfügung.

Die eGK Verarbeitung erfolgt durch den Aufbau eines Trust Channels zwischen dem PoPP-Service und der eGK. Der PoPP-Client agiert dabei lediglich als Vermittler der Kommunikation. Für den Aufbau des Trusted Channels werden die CV-Zertifikate verwendet: bereits vorhandene CV-Zertifikate auf der eGK und ein neues CV-Zertifikat für den PoPP-Service. Das PoPP-Service CV-Zertifikat hat keine weiteren Berechtigungen (alle Flags sind auf 0 gestellt, damit ist kein Auslesen der medizinischen Daten möglich) und dient ausschließlich der Verifikation der Authentizität der eGK und dem Aufbau des Trusted Channels.

Die eGK Verarbeitung erfolgt in folgenden Schritten:

- PoPP-Client baut eine TLS gesicherte WebSocket Verbindung zum PoPP-Service auf (wss://). Client authentisiert sich mit PoPP-Service Access-Token und DPoP Proof.
- PoPP-Service authentifiziert den PoPP-Client durch Prüfung des PoPP-Service Access-Tokens und des DPoP Proofs.
- PoPP-Client und PoPP-Service verständigen sich über gegenseitige Hello Events.
- PoPP-Service erstellt APDU-Sequenzen und übermittelt diese an den PoPP-Client zur Weiterleitung an die eGK. Alle Antworten der eGK werden durch den PoPP-

Client an den PoPP-Service weitergeleitet. In diesem mehrfachen Ablauf werden insbesondere folgende Schritte durchgeführt:

- Prüfung ob es sich um eine eGK handelt.
- Bereitstellung der neuen CV-CA-Zertifikate, falls diese nicht bekannt sind.
- Gegenseitige Authentifizierung zwischen eGK und PoPP-Service. Hierdurch wird die Authentizität der eGK sichergestellt
- Etablierung eines Trusted Channels durch Aushandeln eines symmetrischen Session-Schlüssels
- Auslesen des eGK CH.AUT-Zertifikats über den vertrauenswürdigen Trusted Channel

Wenn alle Schritte erfolgreich waren, stellt der PoPP-Service einen PoPP-Token und einen abwärtskompatiblen Prüfnachweis aus. Die Informationen über die LEI werden über den PoPP-Service Access-Token bzw. über Zugangsautorisierung ermittelt. Die Informationen über den Versicherten werden aus dem eGK CH.AUT-Zertifikat entnommen, insbesondere die KVNR und IK-Nummer der Krankenversicherung.

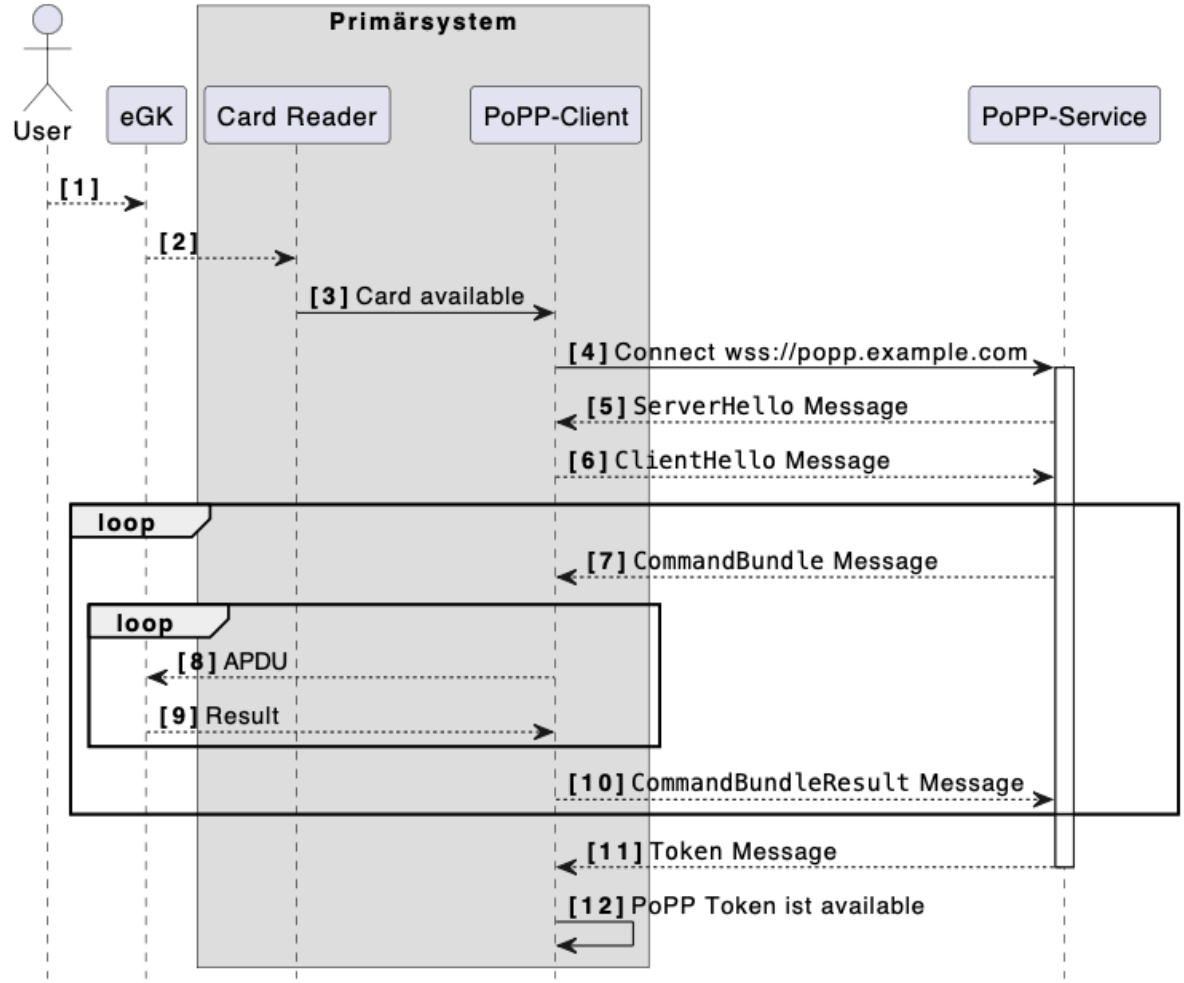

Abbildung 5 Schnittstelle eGK Verarbeitung (Sequenzdiagramm)

6.3.3 GesundheitsID-Verarbeitung

Die logische Schnittstelle zur GesundheitsID Verarbeitung ermöglicht die Prüfung, dass ein Versicherter mit gültiger GesundheitsID sich bei einer LEI anmeldet. Die Bestätigung erfolgt gegenüber dem PoPP-Service und umfasst folgende Schritte:

1. PoPP-Client initiiert die GesundheitsID-Prüfung durch eine Anfrage an den PoPP-Service.
   ("QR-Code Challenge Abruf")
2. PoPP-Service antwortet mit einem Hyperlink, für den Versicherten, der eine Anfrage zur Erstellung einer Anwesenheitsbestätigung enthält.
3. PoPP-Client zeigt den Hyperlink dem Versicherten beispielsweise in Form eines QR-Codes an.
4. Der Versicherte scannt den QR-Code mit seinem Smartphone.
5. Der Versicherte authentifiziert sich mit der GesundheitsID (OAuth2).
6. PoPP-Service erhält die Bestätigung der GesundheitsID-Prüfung ("Consent-Bestätigung Versicherte via QR-Code" in Systemarchitektur) und genehmigt die Ausstellung des PoPP-Tokens für den initiierenden PoPP-Client.

7. PoPP-Client ruft vom PoPP-Service den PoPP-Token ab ("PoPP-Tokenabruf" in Systemarchitektur).

Technisch sind im Ablauf mehrere Interfaces beteiligt. Die Kommunikation zwischen PoPP-Client und PoPP-Service basiert auf dem WebSocket Protokoll, die OAuth2 Anteile (Schritte 5 und 6) basieren auf HTTP.

6.3.4 PoPP-Token-Erstellung

Es ist vorgesehen, das PoPP-Token als JSON Web Token (JWT) zu realisieren, das mit JSON Web Signature (JWS) signiert wird.
Der PoPP-Token wird zudem an den DPoP Schlüssel des PoPP-Client gebunden, um bei Bedarf die Zero Trust Client-Bindung verifizieren zu können.

6.3.5 Telemetrie

Die Ansteuerung der TI-Dienste erfolgt in Zukunft verstärkt direkt über softwarebasierte Clients. Dadurch reduziert sich die Komplexität des Gesamtsystems maßgeblich. Die Verfügbarkeit und Performance der Backendsysteme werden für die Clients unmittelbar relevant. Um die Qualität der Dienste zu gewährleisten, ist es notwendig, die Performance und Verfügbarkeit der Backendsysteme zu überwachen und zu optimieren. Über das zentrale Monitoring hinaus, werden Telemetrie-Daten benötigt, die von den Clients an den PoPP-Service übermittelt werden. Die Telemetrie-Daten dienen dazu, Informationen über die Nutzung, Leistung und den Zustand der TI zu sammeln und zu überwachen. Insbesondere werden dadurch Erkenntnisse, die auf konkrete Implementierungen der Clients und die lokalen Umgebungen (z.B. Internetanbindung) zurückzuführen sind, gewonnen.

Diese Daten dienen folgenden Zwecken:

- Sind die notwendigen Dienste verfügbar?
- Wie ist die Performance der Dienste?
- Wie verhalten sich die Dienste unter Last und verteilt über die Zeit?
- Wie lange dauern die einzelnen Schritte der Dienste im Vergleich zum Gesamtdurchlauf aus Client Sicht?

Der PoPP-Service wird verpflichtet, Telemetrie-Daten zu erfassen und an den Betriebsdatenerfassungs-Server der gematik zu übermitteln. Dabei handelt es sich einerseits um Telemetrie-Daten, die von den PoPP-Clients erfasst und an den PoPP-Service übermittelt werden (siehe 7.1.7- Telemetrie).
Andererseits werden Telemetrie-Daten des PoPP-Service erfasst: zuliefernde interne Komponenten sind mindestens die ZT-Basiskomponenten PEP und PDP.

Konkrete Festlegungen zu den Telemetrie-Daten erfolgen in der Spezifikation. Es wird angestrebt moderne Technologien zur Übermittlung der Daten, wie z.B. OpenTelemetry, zu verwenden.

7 PoPP-Client

Der PoPP-Client wird als eine logische Komponente verstanden, die als Teil des Primärsystems durch den jeweiligen Hersteller implementiert wird.
Die gematik stellt eine Beispielimplementierung des PoPP-Clients als Open Source und einen Implementierungsleitfaden zur Verfügung. Darüber hinaus wird die Test-Instanz des PoPP-Services in der RU genutzt, um die Integration der PoPP-Clients zu testen.

7.1 Schnittstellen

7.1.1 Zugangsautorisierung beim PoPP-Service

Bevor der PoPP-Client auf den PoPP-Service zugreifen kann, muss eine Zugangsautorisierung erfolgen. Die Zugangsautorisierung wird durch die Zero Trust Basiskomponenten des PoPP-Services durchgeführt.

Die Zugangsautorisierung wird über OAuth2 Protokollfamilie realisiert. Zugangssession zwischen PoPP-Client und PoPP-Service wird durch ein Access-Token, den PoPP-Service Access-Token realisiert.

PoPP-Client führt folgende Schritte durch:

- PoPP-Client sendet eine Anfrage an den PoPP-Service
- PoPP-Service antwortet mit einer Nonce
- PoPP-Client erzeugt eine Client Assertion inkl. Nonce in Form eines JWT und signiert diesen mit der vorher freigeschalteten SM(C)-B. Keine Benutzerinteraktion erforderlich.
- PoPP-Client übermittelt die Client Assertion an den PoPP-Service
- Nach erfolgreicher Autorisierung erhält der PoPP-Client ein Access-Token, den PoPP-Service Access-Token zum Zugriff auf den PoPP-Service
- PoPP-Client kann nun auf den PoPP-Service zugreifen

Der PoPP-Client muss die Zugangsautorisierung regelmäßig erneuern. Die Häufigkeit der Erneuerung wird durch den PoPP-Service über die Laufzeit des PoPP-Service Access-Tokens bestimmt. Auf die Nutzung von Refresh Token wird bewusst verzichtet, weil eine starke, regelmäßige Authentifizierung durch die freigeschaltete SM(C)-B vollautomatisch erfolgen kann.

Zusätzlich zur Client Authentifizierung über die SM(C)-B ermittelt der PoPP-Service die Identität der Institution, die den PoPP-Client betreibt. Aus diesem Grund wird zunächst auf eine explizite Registrierung des PoPP-Clients beim PoPP-Service verzichtet.

Die Client Assertion enthält folgende Informationen:

- Nonce vom PoPP-Service um Replay-Angriffe zu verhindern
- ClientID des PoPP-Clients (s. unten)
- Zeitstempel der Erstellung
- Gültigkeitsdauer
- Selbstauskunft des PoPP-Clients über sich selbst und die Laufzeitumgebung

- Signatur inkl. X.509 Zertifikat der SM-B

Die Software-Implementierungen der PoPP-Clients müssen bei der gematik durch die Hersteller registriert werden. Da die PoPP-Clients in die Primärsysteme integriert werden, ist nur eine Registrierung per Gesamtprodukt erforderlich. Es ist geplant, bereits erfolgte Registrierungen aus der Einführung von E-Rezept zu übernehmen.

Das PoPP-Service Access-Token ist über DPoP [RFC9449] an die PoPP-Client Instanz gebunden. Der PoPP-Client muss bei der Erstellung des PoPP-Service Access-Token die DPoP-Header mit übermitteln. Der PoPP-Service prüft die DPoP-Header bei jeder Anfrage und bindet den DPoP-Schlüssel an die Session.

Mit weiteren Ausbau der Telematikinfrastruktur und der Anwendungen ist damit zu rechnen, dass weitere Prüfungen bei der Zugangsautorisierung hinzukommen werden.

7.1.2 LEI Authentifizierung über Konnektor

Im Rahmen der Zugangsautorisierung wird die LEI Authentifizierung mittels SM(C)-B durchgeführt. Hierfür bieten die Konnektoren und TI-Gateways folgende relevante Schnittstellen an:

- ServiceDirectoryService (connector.sds) - zum Abruf der Konnektor-Informationen, vorhandenen Services und deren Versionen
- EventService - zum Abruf der vorhandenen SM(C)-Bs
- CardService - optional, für einmaliges Freischalten der SM(C)-B über PIN
- CertificateService - zum Abrufen des Zertifikats der SM(C)-B
- AuthSignatureService - zum Signieren der Client Assertion

Der PoPP-Client muss in der Lage sein diese Schnittstelle aufzurufen. Hierfür sind alle Voraussetzungen zum Zugriff auf Konnektorschnittstellen zu erfüllen:

- Client-Credentials, bspw. MTLS Zertifikat
- Für den PoPP-Client konfiguriertes Konnektor-Infomodell, welches den Zugriff auf gewünschte SM(C)-B erlaubt
- Infomodellparameter für die Client-Configuration: Mandanten-Id, Clientsystem-Id, Arbeitsplatz-Id

Da der PoPP-Client in die Primärsysteme integriert ist, ist nur eine gemeinsame Konfiguration des Konnektorzugriffs erforderlich.

Für die Signatur müssen ausschließlich ECC Schlüssel verwendet werden. Der PoPP-Client muss die Schnittstellen mit entsprechenden Parametern aufrufen.

7.1.3 eGK Prüfung durch PoPP-Service

Der PoPP-Client kann gegenüber dem PoPP-Service nachweisen, dass die eGK eines Versicherten vorliegt. Auf einer Seite verbindet sich der PoPP-Client mit der eGK. Hierfür sind zwei Optionen vorgesehen - über Kartenleser oder über Konnektor; die Anbindungsvariante der eGK in der LEI ist für den PoPP-Service transparent. Auf der anderen Seite verbindet sich der PoPP-Client mit dem PoPP-Service. Bei dem gesamten Ablauf agiert der PoPP-Client als Vermittler zwischen PoPP-Service und eGK und hat außer dem Transport der Daten und Fehlerhandling keine weiteren Funktionen.

PoPP-Client führt folgende Schritte durch:

1. PoPP-Client verbindet sich über eine bidirektionale WebSocket Verbindung mit dem PoPP-Service. Die Verbindung ist TLS geschützt (wss://) und über den PoPP-Service Access-Token mit DPoP Bindung authentifiziert.
2. PoPP-Client und PoPP-Service machen sich jeweils bekannt über Hello-Messages.
3. PoPP-Service übermittelt die APDU-Sequenzen an den PoPP-Client, der diese an die eGK weiterleiten muss.
4. PoPP-Client empfängt die APDU-Sequenzen vom PoPP-Service und leitet diese an die eGK weiter, entweder direkt über einen Kartenleser oder über Konnektor/eH-KT.
5. PoPP-Client empfängt die Antwort der eGK und leitet diese an den PoPP-Service weiter.
6. Schritte 3 bis 5 werden so lange wiederholt, bis die eGK die gewünschten Informationen an den PoPP-Service übermittelt oder ein Fehler auftritt.
7. PoPP-Service übermittelt den PoPP-Token an den PoPP-Client zusammen mit weiteren Informationen, die zur Verwendung des PoPP-Tokens erforderlich sind.

7.1.4 eGK über Kartenleser

Der PoPP-Client muss in der Lage sein, eine eGK über einen Kartenleser zu verbinden. Als Kartenleser ist ein beliebiges Gerät vorgesehen, das die eGK kontaktbehaftet auslesen kann und sich über Software ansteuern lässt. In Frage kommen zum Beispiel handelsübliche USB Kartenleser, die über eine PC/SC Schnittstelle angesprochen werden können. Es ist empfohlen die im Betriebssystem vorhandenen Treiber und Schnittstellen für den Kartenleser zu verwenden (z.B. Winscard für Windows, PCSC-Lite für Linux, CryptoTokenKit für Apple).

Dadurch, dass die Verbindung zwischen eGK und PoPP-Server Ende zu Ende abgesichert ist, ist es nicht erforderlich, dass der Kartenleser über eine Sicherheitszertifizierung verfügt. Die Verbindung zwischen einer eGK G2.1 - die aktuellste Version der eGK - und dem Kartenleser muss zwingend über eine kontaktbehaftete Schnittstelle erfolgen. Nur dann kann garantiert werden, dass die Verbindung zwischen eGK und PoPP-Service sicher ist. Ab der eGK G3.0 ist es geplant auch kontaktlose Schnittstellen mit dem gleichen Sicherheitsniveau zu unterstützen. Dadurch, dass die eGKs für die Nutzung der kontaktlosen Schnittstelle die Eingabe einer 6-stelligen CANs erfordern, ist es aus Nutzersicht ohnehin meistens praktischer, die eGK über die kontaktbehaftete Schnittstelle zu verwenden.

7.1.5 eGK über Konnektor

Der PoPP-Client kann eine eGK auch über den Konnektor verbinden. Hierfür ist eine Anpassung der Konnektorfirmware geplant, die es dem PoPP-Client ermöglicht die vom PoPP-Service übermittelten APDU-Sequenzen über den Konnektor an die eGK weiterzuleiten. Die Verbindung zwischen PoPP-Client und Konnektor erfolgt über die vorhandenen Konfigurationen, die bereits in der Zugangsautorisierung beschrieben sind. Die Verbindung zwischen Konnektor und eGK erfolgt über die vorhandenen Schnittstellen des Konnektors, die für die eGK-Kommunikation vorgesehen sind.

Darüber hinaus unterscheidet sich der Abflauf der eGK-Prüfung über Konnektor nicht von der eGK-Prüfung über Kartenleser. Der PoPP-Client leitet die APDU-Sequenzen vom PoPP-Service an die eGK weiter und leitet die Antwort der eGK an den PoPP-Service weiter.

7.1.6 GesundheitsID Prüfung

Der PoPP-Client kann mithilfe der GesundheitsID eine Bestätigung der Identität eines Versicherten gegenüber dem PoPP-Service erbringen und dadurch die Voraussetzung für die Ausstellung des PoPP-Tokens erfüllen.

PoPP-Client führt folgende Schritte durch:

1. PoPP-Client initiiert die GesundheitsID-Prüfung durch eine Anfrage an den PoPP-Service.
2. PoPP-Service antwortet mit einem Hyperlink, für den Versicherten, der eine Anfrage zur Erstellung einer Anwesenheitsbestätigung enthält.
3. PoPP-Client zeigt den Hyperlink dem Versicherten beispielsweise in Form eines QR-Codes an.
4. Der Versicherte scannt den QR-Code mit seinem Smartphone.
5. Der Versicherte authentifiziert sich mit der GesundheitsID.
6. PoPP-Service erhält die Bestätigung der GesundheitsID-Prüfung und genehmigt die Ausstellung des PoPP-Tokens für den initiierenden PoPP-Client.
7. PoPP-Client ruft vom PoPP-Service den PoPP-Token ab.

Hinweis: *Alternative (ohne QR-Display)*

1. *PoPP-Client initiiert die GesundheitsID-Prüfung durch eine Anfrage an den PoPP-Service.*
2. *PoPP-Service antwortet mit Code, der durch den Versicherten auf seinem Smartphone weiterverarbeitet werden muss, z.B. 4-stellige Zahl.*
3. *Der Versicherte scannt den statischen QR-Code, der in der LEI sichtbar angebracht ist.*
4. *Der Versicherte startet eine weitere Session zum PoPP-Service, authentisiert sich mit der GesundheitsID und gibt den Code aus Schritt 2 auf seinem Smartphone ein.*
5. *PoPP-Service erhält die Bestätigung der GesundheitsID-Prüfung und genehmigt die Ausstellung des PoPP-Tokens für den initiierenden PoPP-Client.*
6. *PoPP-Client ruft vom PoPP-Service den PoPP-Token ab.*

7.1.7 Telemetrie

Die PoPP-Clients bzw. Primärsysteme im Allgemeinen, werden verpflichtet, Telemetrie-Daten zu erfassen und an den PoPP-Service zu liefern. Dabei handelt es sich um anonymisierte, technische Messungen.

Der PoPP-Client muss auf Wunsch des Leistungserbringers die Telemetrie-Daten regelmäßig an den PoPP-Service übermitteln. Für den Leistungserbringer muss es transparent sein, welche Daten, im welchen Umfang und wie oft übermittelt werden (z.B. durch lokale Logs und Dokumentation).

Konkrete Festlegungen zu den Telemetrie-Daten erfolgen in der Spezifikation. Es wird angestrebt moderne Technologien zur Übermittlung der Daten, wie z.B. OpenTelemetry, zu verwenden.

8 Betriebskonzeption

Der PoPP-Service fungiert als notwendige zentrale Instanz bei der Ausstellung der PoPP-Token für Versicherte mit eGK oder Gesundheits-ID und wird nach der Vergabe von einem Auftragnehmer betrieben. Dieser Service muss hochverfügbar, redundant und sicher ausgelegt sein, damit ein kontinuierlicher und stabiler Betrieb des Dienstes und damit auch der Versorgungsprozesse gewährleistet werden kann.

Die im Rahmen der Spezifikations- und Vergabephase zu erfüllenden Anforderungen leiten sich im Wesentlichen aus den Erfahrungen bereits bestehender hochverfügbarer und sicherer TI-Dienste ab.

Da das vorliegende Konzeptdokument den Fokus auf die Nutzungsszenarien und die Architektur legt, werden betriebliche Einzelheiten hier nicht näher ausgeführt.

9 Anhang – Verzeichnisse

9.1 Abkürzungen

Kürzel	Erläuterung
PoPP	Proof of Patient Presence
DPoP	Demonstrated Proof of Possession
JWT	JSON Web Token
ECC	Elliptic Curve Cryptography
OCSP	Online Certificate Status Protocol
SM(C)-B	Instituts-Identität, die entweder auf einer Karte (SMC-B) oder in einem High Security Module (HSM) bereitgestellt wird.
LE	Leistungserbringer
ZT	Zero Trust
gID	GesundheitsID
HMAC	***h****ash-based* ***m****essage* ***a****uthentication* ***c****ode* (Hash-basierter Nachrichtenauthentifizierungscode), bei dem sich Seiten ein Secret kennen und sich so verifizieren können

9.2 Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

9.3 Abbildungsverzeichnis

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

9.4 Tabellenverzeichnis

9.5 Referenzierte Dokumente

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel

Weitere Referenzierungen:

[Quelle]	Herausgeber (Erscheinungsdatum): Titel

9.6 Offene Punkte / Klärungsbedarf

Kap.	Offener Punkt	Zuständig
3.4.6- Nicht unterstützte Use Cases	Es sollten Konzepte betrachtet werden, welche die kontaktlose Anbindung einer eGK der Generation 2 (bzw. 2.1) gestatten.	gematik