Proof of Patient Presence (PoPP)

Der Proof of Patient Presence (PoPP) ist ein Anwesenheitsbeleg mittels TI-Dienst als zukünftige Nachfolgeversion der derzeit beim Abruf von E-Rezepten mit der eGK eingeführten VSDM++-Lösung, der auch als Nachweis eines bestehenden Behandlungskontextes dient.

Die Spezifikation und Umsetzung erfolgt in **zwei Stufen**.

Stufe 1 umfasst folgende Anwendungsfälle:

- Nutzung der eGK in Versorgungseinrichtungen
- Nutzung der eGK in mobilen Szenarien

⇒ Keine Nutzung der GesundheitsID!

Die Nutzung der eGK soll bei den Leistungserbringenden auch mit Standardkartenlesern bzw. Smartphones möglich sein, was aktuell noch zu Sicherheitsdiskussionen führt.

Stufe 2 (Online-Check-In) umfasst folgende Anwendungsfälle:

- Nutzung der eGK auch in der Fernversorgung (bspw. Videosprechstunde oder Online-Diensten von Apotheken)
- Nutzung der GesundheitsID in allen Versorgungsszenarien:
  - in Versorgungseinrichtungen
  - in mobilen Szenarien
  - in der Fernversorgung

Grober Ablauf Stufe 1:

- eGK wird in den Versorgungseinrichtungen in ein Kartenterminal gesteckt.
- eGK wird in mobilen Szenarien an die NFC-Schnittstelle des Smartphones gehalten.

Grober Ablauf Stufe 2 (Online-Check-in):
Ziel ist es, den Zugang zu Versichertendaten auch in diesen Versorgungsszenarien für die LEI zu ermöglichen und zusätzlich den VER mit der GesundheitsID eine virtuelle Alternative zum Stecken der physischen eGK in vor-Ort-Szenarien anzubieten. Das Ergebnis des Prozesses ist auch hier ein PoPP-Token, der gemäß der Spezifiktion [gemSpec_PoPP_Service] generiert wird und berechtigten LEI den Zugriff auf die Versichertendaten in den Fachdiensten ermöglicht.

Der Prozess für den Online-Check-in wird vom VER initiiert und erfordert unter anderem folgende weitere Komponenten im Vergleich zur ersten Stufe:

- eine App, die den Online-Check-in via PoPP unterstützt,
- eine Auswahl der LEI via App bei dem sich der VER einchecken möchte,
- zum Ausweisen eine GesundheitsID oder wie bisher die eGK des VER.

Der Prozess startet mit der Auswahl der LEI, bei der der VER einchecken möchte.

- Dies erfolgt in der Regel durch das Scannen eines statischen QR-Codes (beinhaltet die Telematik-ID der LEI) aus einer App für den Online-Check-in heraus.
- Danach weist sich der VER mithilfe seiner GesundheitsID oder eGK an seinem Smartphone aus.
- Abschließend wird der PoPP-Token im PoPP-Service erstellt und über diesen der LEI für en Zugrif auf die Versichertendaten in den Fachdiensten zur Verfügung gestellt.

Status

Am **28.11.2025** erhält **RISE** den Zuschlag für die Umsetzung des PoPP Service[1)], nachdem die Ausschreibung am 4.4.2025 veröffentlicht wurde. Die Umsetzung basiert auf einem vorabveröffentlichten Stand der PoPP-Spezifikation. Die **Umsetzung** läuft **seit 1.12.2025**. Eine Veröffentlichung der **finalen Spezifikationen** ist für **30.01.2026** geplant. Die **Umsetzung der Stufe 1** des PoPP-Service ist für den **30.06.2026** geplant. Die **Umsetzung der Stufe 2** müsste dann **spätestens in Q4/2026** erfolgen, damit sie nach Abschluss der Migration von VSDM 1 auf VSDM 2 zur Verfügung steht.

Umsetzungen

- gesund.de plant PoPP-Entwicklung als Nachfolger von CardLink ein.[2)]

Spezifikation

Spezifikation der Stufe 2 als Prerelease PoPP_26_1 (26.01.2026) veröffentlicht

Technisches Konzept: Proof of Patient Presence (PoPP),Version 1.0.0 (20.08.2024)
⇒ Dient der Information von Gesellschaftern und Öffentlichkeit über geplante Architekturänderungen; Diskussionsgrundlage auf deren Basis die Spezifikationen erstellt werden.

Im Nachgang wurde das Konzept in mehreren vorabveröffentlichten Releases konkretisiert/aktualisiert:

- Prerelease Draft_Smartcards_24_3 (20.01.2025)
- Prerelease Draft_PoPP_25_1 (16.06.2025)
- Prerelease Draft_PoPP_25_2 (21.11.2025)
- Prerelease Draft_PoPP_26_1 (26.01.2026)

Ursprünglich war eine Lösung für den CheckIn mit FdV vorgesehen, bei der der Versicherte den CheckIn anstößt, indem er sich am PoPP-Service authentisiert und anschließend eine TAN als One-Time-Passwort (OTP) erhält, mit der er im Folgenden in der Leistungserbringerinstitution (LEI) den Versorgungskontext herstellen kann. In der LEI wird das OTP entweder als Barcode eingescannt (Scanner notwendig!) oder in einer kurzen Version manuell eingegeben (wenn die LEI vorab bekannt war). Mittels dieses OTP holt sich die LEI, dann den Versorgungskontext als PoPP-Token vom PoPP-Service.

Nach Gesellschafterbeschluss wurde diese Lösung überarbeitet. Die alternative Lösung sieht vor, dass

der Versicherte einen statischen QR-Code in der Praxis (oder beim Hausbesuch einen mitgebrachten QR-Code) mit seiner App scannt und sich darüber eincheckt. Bei der Fernversorgung muss dann die Drittanbieter App ein PoPP-Modul anbieten, über das dann eingecheckt werden kann oder ein QR-Code zum CheckIn im Browser eingeblendet oder per E-Mail zugesendet werden, mit dem dann der CheckIn stattfinden kann. Auch in diesen Fällen wird aber ein PoPP-Modul benötigt. Die Ausschreibung wurde auf Basis einer Grobkonzeption der Lösung in Q3/2025 angepasst.

Denkbar, aber nicht realisiert wäre auch eine Lösung ohne PoPP-Modul, bei der der Versicherte nur auf Anforderung der LEI tatsächlich reagiert in seiner App. Der LEI fordert ein PoPP-Token für den Versicherten an und der IdP fordert daraufhin vom Versicherten eine Authentifizierung an. Die Daten des Versicherten könnte der LEI bspw. über einen von der App generierten QR-Code oder NFC-Übertragung als vCard erhalten (Scanner in Praxis benötigt!).

Ältere Lösungsansätze

Eine erste Ende 2022 entwickelte Grobkonzeption und ein darauf aufbauendes Featuredokument fanden ihren Niederschlag im Nachgang als Arbeitsstand einer PoPP-Lösung in der veröffentlichten Version 1.1.1 eines Featuredokuments zum „Abruf der E-Rezepte in der Apotheke nach Autorisierung“. Der Stand ist gekennzeichnet als nicht normativ, da er sich noch in Abstimmung befindet.

Lösung in [gemF_eRp_Autorisierung_Apo]

Die Lösung steht ganz im Kontext des E-Rezept-Abrufs mittels eGK und berücksichtigt auch nur diesen Fall, lässt also die GesundheitsID außen vor. Es geht lediglich um die Ablösung der VSDM++-basierten Lösung.

Der konzipierte PoPP-Dienst ist ein Dienst im zentralen Netz der TI, welcher einen kryptographisch gesicherten Nachweis ausstellt, dass eine eGK in einer LEI gesteckt wurde. Eine **PIN-Eingabe** des Versicherten ist hierzu **nicht notwendig**. Die Kommunikation vom Primärsystem zum PoPP-Dienst erfolgt über ein **Modul im Konnektor**.

Beim Abruf der E-Rezepte in einer Apotheke nach Autorisierung wird die eGK des Versicherten als Mittel für die Autorisierung verwendet. Andere Mittel für die Autorisierung als die eGK werden nicht unterstützt.

Das Primärsystem (PS) ruft die Operation für den Anwesenheitsnachweis am Konnektor auf. Das Modul PoPP des Konnektors liefert einen durch den PoPP-Dienst signierten Token, welcher belegt, dass die eGK im eHealth-Kartenterminal der LEI gesteckt ist. Im Rahmen dieser Operation wird geprüft, ob die eGK nicht gesperrt und das Authentisierungszertifikat auf der eGK gültig ist.

Der Token beinhaltet u.a. die Information der KVNR der eGK, die Telematik-ID der Leistungserbringerinstitution und den Zeitpunkt der Erstellung des Token. Der Token ist durch den PoPP-Dienst signiert.

Der E-Rezept-Fachdienst prüft beim Abruf der E-Rezepte den Token. Es wird geprüft, dass die Signatur gültig ist, dass der Token innerhalb eines bestimmten Zeitfensters vor dem Aufruf der Operation erstellt wurde und dass die Telematik-ID im Token mit der Telematik-ID der aufrufenden Apotheke übereinstimmt. Wenn diese Prüfungen positiv ausfallen, dann werden im Response für den Aufruf die

E-Rezepte zur KVNR aus dem Token zurückgeliefert.

Lösung in [gemKPT_PoPP]

Diese Lösung abstrahiert nun vom E-Rezept-Kontext und dient als Grobkonzeption einer Lösung ohne Konnektor und mit GesundheitsID und eGK.[3)]. Es handelt sich also um eine **TI-2.0-kompatible** Lösung. Eine PIN für Versicherte kommt dabei nicht zum Einsatz.

Ermöglicht werden sollen mit der Lösung somit eine Autorisierung bzw. Etablierung eines Behandlungskontextes[4)]

- zum Abruf VSD mit eGK und GesundheitsID als Versicherungsnachweis,
- zum Abruf E-Rezepte in Apotheke,
- zum Zugriff auf die ePA.

Ein legitimer Behandlungskontext ist ein nachgewiesener Zusammenhang zwischen einem berechtigten Versicherten und der ihn behandelnden oder anderweitig versorgenden authentifizierten Leistungserbringerinstitution zu einem bestimmten Zeitpunkt. Berechtigt ist ein Versicherter, wenn er mit seiner digitalen Identität authentifiziert oder seine eGK auf Echtheit und Gültigkeit erfolgreich überprüft wurde. Der Nachweis des Behandlungskontext erfolgt kryptografisch belegt und damit nicht kompromittierbar erfolgen. Das kryptographische Artefakt der PoPP-Lösung ist ein kryptografisch gesichertes Token, das als **PoPP-Token** bezeichnet wird.

Betrachtete Versorgungsszenarien

- **Versorgungsszenario 1**: Versicherter und LE befinden sich beide in der LEI
  - Ein Versicherter möchte in der Praxis eine Leistung empfangen. Dazu benötigt der behandelnde LE aktuelle Stammdaten und einen Versicherungsnachwei
  - Ein Versicherter in der Praxis möchte dem ihn behandelnden LE-Zugriff auf seine „ePA für alle“ gewähren.s (VSDM2) für die Abrechnung.
  - Ein Versicherter möchte verordnete E-Rezepte in der Apotheke einlösen.
  - Ein Versicherter möchte bei einem Hilfsmittel-LE/ Heilberufler oder stationärer Pflegeeinrichtung eVerordnungen einlösen.
  - Ein Versicherter möchte nach Erfassung seiner Antragsdaten, die im PS des LEs erfassten Angaben bestätigen. Der Versicherte stellt den Antrag, zuvor hat ein Hilfsmittel-LE / Pflegekraft bei der Erfassung dieser Antragsdaten in Vorbereitung auf die Genehmigung einer Leistung durch die Krankenkasse unterstützt.
- **Versorgungsszenario 2:** Versicherter befindet sich außerhalb der LEI und der LEI in der LEI
  - Ein Versicherter möchte via Telemedizin eine Leistung empfangen. Dazu benötigt der behandelnde LE aktuelle Stammdaten und einen Versicherungsnachweis (VSDM2) für die Abrechnung.
  - Ein Versicherter möchte während einer Videosprechstunde dem behandelnden Leistungserbringer Zugriff auf seine „ePA für alle“ gewähren.
  - Ein Versicherter möchte mobil mit seinem Smartphone ein verordnetes E-Rezept mit seiner eGK und ohne PIN zum Abholen oder Versand einlösen. **(nicht unterstützt!)**
  - Ein Versicherter möchte während einer Videosprechstunde ein E-Rezepte verordnet bekommen.
- **Versorgungsszenario 3a:** Versicherter und LE befinden sich außerhalb der LEI am selben Ort
  - Ein Versicherter möchte zuhause eine Leistung empfangen (LE beim Versicherten). Dazu

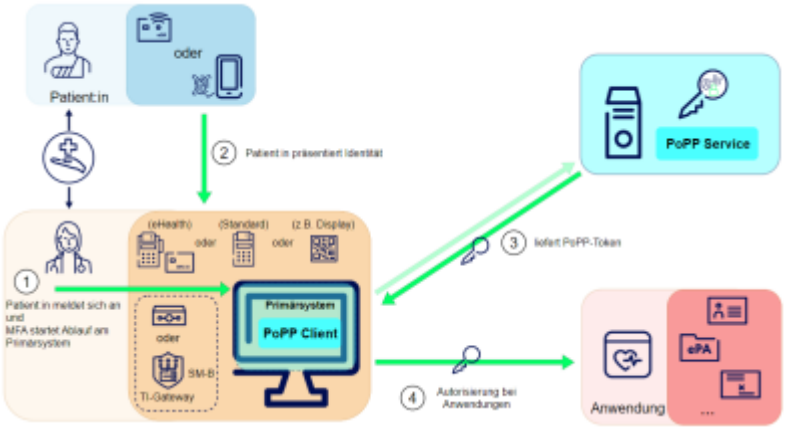
benötigt der behandelnde LE aktuelle Stammdaten und einen Versicherungsnachweis (VSDM2) für die Abrechnung.
    - Ein Versicherter möchte dem LE zuhause Zugriff auf seine „ePA für alle“ gewähren (LE beim Versicherten zuhause).
    - Ein Bewusstloser oder eine nicht ansprechbare Person möchte, dass der behandelnde LE beim Auffinden auf der Straße auf seine Notfalldaten in der „ePA für alle“ zugreifen kann. **(kann nur mit eGK umgesetzt werden!)**
    - Ein Versicherter möchte bei einem ambulanten Pflegedienst eine durch einen Arzt verordnete häusliche Krankenpflege einlösen.
    - Ein Versicherter ohne eigenes Smartphone möchte außerhalb der LEI verordnete eVerordnungen für häusliche Krankenpflegeleistungen einlösen. **(kann nur mit eGK umgesetzt werden!)**
    - Ein Versicherter ohne eigenes Smartphone möchte die von der Pflegekraft erbrachte Leistung abzeichnen. Die Pflegekraft benötigt den Nachweis, den Versicherten zuhause versorgt zu haben. **(kann nur mit eGK umgesetzt werden!)**
    - 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.
    - 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.
- **Versorgungsszenario 3b:** Versicherter und LE befinden sich außerhalb der LEI jeweils an einem anderen Ort
    - Ein Versicherter möchte während einer Videosprechstunde dem behandelnden, im HomeOffice befindlichen Leistungserbringer, Zugriff auf seine „ePA für alle„ gewähren
- **Versorgungsszenario 4:** Versicherter befindet in der LEI und der LEI außerhalb der LEI
    - keine Use Cases identifiziert

Nicht unterstützte Anwendungsfälle/Szenarien

Bei den nicht unterstützten Anwendungsfällen handelt es sich um Fälle, bei denen der Versicherte eine eGK über sein eigenes Gerät **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. ⇒ Nutzungsszenarien ohne PIN sind mit dem Versicherten-Smartphone zumindest initial nicht umsetzbar. Sicherstellung soll mit der Weiterentwicklung der eGK zur G3 erfolgen. Bei der voraussichtlichen Verfügbarkeit der PoPP-Lösung werden jedoch ausschließlich G2.1 Karten im Feld sein.

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.

Architektur



Zur Erstellung eines validen, signierten PoPP-Token müssen im PoPP-Service vorliegen:

- (authentizitätsgeprüfte) KVNR des Versicherten
- (authentizitätsgeprüfte) Telematik-ID der LEI.

In der Übergangszeit von VSDM 1.0 auf VSDM 2.0 wird zur Abwärtskompabilität vom PoPP-Service auch ein VSDM++-Prüfnachweis erstellt. Dabei muss eine Verwendung dieses Prüfnachweises für die Abrechnung ausgeschlossen werden, da keine Online-Prüfung des Versicherungsstatus stattgefunden hat.

PoPP-Service: zentraler TI-Dienst ⇒ Vergabe
PoPP-Client: logische Komponente, die Teil des Primärsystems ist und vom jeweiligen Hersteller implementiert wird

PoPP-Token

Der PoPP-Service erstellt und signiert das PoPP-Token und liefert es in der Antwort auf einen Request des PoPP-Clients (im PS) mit folgenden Inhalten:

1. KVNR (als Identitätsattribut des Versicherten); inkl. der Info, ob die Quelle die eGK oder GesundheitsID des Versicherten ist
2. IK-Nummer (Kassenzugehörigkeit des Versicherten)
3. Telematik-ID (als Identitätsattribut der Institution)
4. ProfessionOID als weitere Qualifizierung der LEI
5. Zeitstempel der Token-Erstellung
6. Signatur über alle Daten (1-5)
7. X.509-Zertifikat (inkl. Public Key) zur Verifikation der Signatur

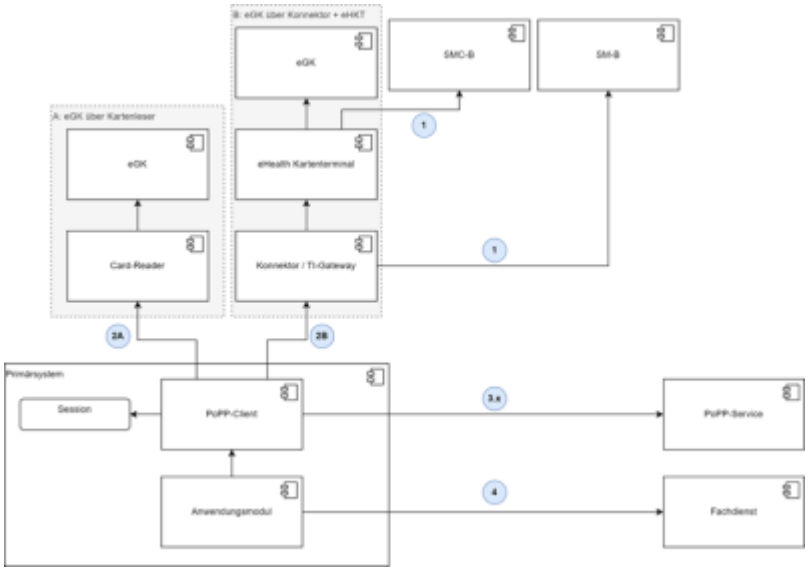
Das PoPP-Token ist kryptografisch abgesichert und über (die in Zero-Trust definierten) Token-Binding-Mechanismen an die konkrete Instanz des Primärsystems bzw. die Session zwischen PoPP-Client und PoPP-Service gebunden (DPoP[5)]).

Das PoPP-Token wird als ein self-contained JWT OAuth2 Access-Token abgebildet. Die Signatur erfolgt dann mit JSON Web Signature (JWS).

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.

Architektur in der LEI



Ablauf

1. LEI authentifiziert sich mit SM-B („externalAuthenticate“) gegenüber dem PoPP-Service
2. eGK wird in Standard- oder eHealth-KT gesteckt.
3. PoPP-Client initiiert bidirektionale WebSocket-Verbindung zum PoPP-Service und authentifiziert sich über den PoPP-Service-Access-Token. PoPP-Client ist der Vermittler zwischen eGK und PoPP-Service und leitet bidirektional die APDU-Sequenzen weiter.
    1. C2S-Authentisierung zwischen eGK und PoPP-Service (CVC mit Null-Flaglist) ⇒ Überprüfung des Vorliegens und der Echtheit der eGK
    2. Auslesen des CH.AUT-X509-Zertifikats (mit KVNR und IK-Nummer) durch PoPP-Service
    3. Zertifikatsprüfung auch gegen TSL und OCSP durch PoPP-Service
    4. Erstellung und Signierung des PoPP-Token durch den PoPP-Service
4. Übermittlung des PoPP-Tokens an den PoPP-Client

Es ist auch ein Standard-Kartenleser zulässig! Für die reine Kartenverifikation benötigt man dann auch keinen Konnektor.

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 ist. 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.

Für dieses Szenario ist eine Konnektoranpassung notwendig!

Bestandshardware (eH-KT) kann weiterverwendet werden (Investitionsschutz).
Es gibt voraussichtlich nach PoPP-Einführung 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)

Architektur mobil

Nicht über NFC unterstützt für eGK G2.1.

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.

Nach Eingabe der CAN nutzt die eGK das PACE-Protokoll
⇒ Die Zugriffsregeln der eGK verhindern dann den zusätzlichen Aufbau eines Trusted Channel zum PoPP (zusätzlich zum PACE-Kanal) bzw. das Einlesen des X.509-Zertifikat mit den benötigten Informationen zum Versicherten für den CheckIn aus dem bestehenden CV-Kanal.
⇒ Nutzungsszenarien ohne PIN sind mit dem Versicherten-Smartphone zumindest initial nicht umsetzbar. Sicherstellung soll mit der Weiterentwicklung der eGK zur G3 erfolgen.

Damit entfallen faktisch auch alle telemedizinischen Szenarien

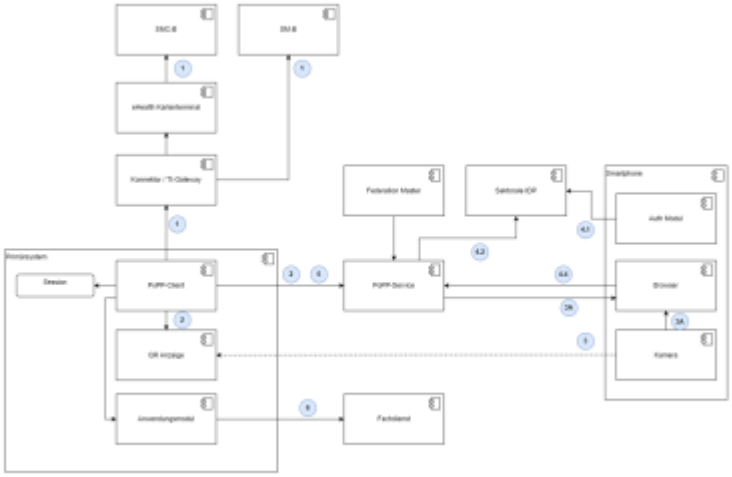
Ausblick

Über eine eGK-Hash-Datenbank (s. Kap. 9.1) wäre diese Szenario auch für eGK der Generation 2.1 möglich. Darüber kann man dann die Frage beantworten: Stammt ein vorgelegtes CV-Zertifikat und ein vorgelegtes X.509 Zertifikat aus ein und derselben eGK.

PoPP mit GesundheitsID

Lösung über dynamisch generierten QR-Code (Consent Code) und Authentifizierung des Versicherten ggü. dem PoPP-Service mittels GesundheitsID mit anschließender Bestätigung der an die LEI zu übermittelten Daten für das PoPP-Token.

Architektur in der LEI



Ablauf

1. LEI authentifiziert sich mit SM-B („externalAuthenticate“) gegenüber dem PoPP-Service
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 einem Gerät zur QR-Anzeige dargestellt**.
3. Der Versicherte scannt den QR-Code
    1. über den Browser
    2. über die Kassen-App
4. Authentifizierung des Versicherten und Übermittlung seiner Daten
    1. Der Versicherte authentifiziert sich mit seiner GesundheitsID über den sektoralen IdP gegenüber dem PoPP-Service
    2. Der PoPP-Service erhält vom sektoralen IdP einen ID-Token (inkl. Name, KVNr und IK-Nummer)
    3. Consent Screen wird in App oder Browser angezeigt
    4. Versicherter bestätigt über den Consent Screen die Übermittlung seiner Daten
5. PoPP-Service erstellt PoPP-Token. Das PS kann über die authentifizeirte Session und den Consent Code die erteilten genehmigungen abrufen. Dabei wird überprüft, dass der Consent Code im zulässigen Zeitraum erstellt wurde („Freshness“).
6. Anwendungsmodul des PS kann dann den PoPP-Token als Autorisierung am Fachdienst verwenden.

Architektur mobil

Ablauf wie in LEI, aber der Link des Consent Codes muss irgendwo angezeigt werden, so dass ihn der

Versicherte nutzen kann, um Authentisierung des Versicherten mittels Smartphone (via GesundheitsID) einzuleiten, sprich den entsprechenden Authentifizierungsworkflow über den sektoralen IdP zu starten.

Telemedizinische Szenarien könnten bspw. über die Zurverfügungstellung eines Link im Chat ablaufen.

Alternatives Szenario falls kein QR-Display verfügbar:
PoPP-Service sendet statt eines Hyperlinks einen z.B. 4-stelligen Code. Der Versicherte scannt dann einen statischen Code, der in der LEI angebracht ist, startet eine weitere Session zum PoPP-Service und authentisiert sich mit der GesundheitsID und dem 4-stelligen Code auf seinem Smartphone.

Ausblick

Möglich wäre auch ein statischer QR-Code, um etablierte Verfahren wie eEB und OCI weiterverwenden zu können. Siehe dazu Kap. 9.2

Datenschutz und Informationssicherheit

Um zu verhindern, dass der Betreiber des PoPP-Service sich selbst Token ausstellt und zwecks Profilbildung Zugriff auf die Daten hat wird eine VAU genutzt sowie ein sicherer Schlüsselspeicher (HSM).

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.

Ausblick gesamt

Folgende Punkte wurden diskutiert und werden fortlaufend über Spezifikationsdokumente adressiert und ebenfalls zur Kommentierung und Diskussion vorgelegt.

Nutzung der eGK-Kontaktlosschnittstelle (NFC) für mobile Szenarien

Problem

Die Zugriffsregeln der eGK erfordern PACE als sicheres Übertragungsprotokoll für die kontaktlose Kommunikation. Dabei wird die Kommunikation zwischen der eGK und dem PACE-Endpunkt (i.d.R das Kartenlesegerät) verschlüsselt. Diese Art der Verschlüsselung würde nur dann sicher im PoPP-Service enden, wenn die CAN (Card Access Number) sicher übermittelt werden könnte, was mit der bestehenden Peripherie ausgeschlossen ist.

Das PoPP Konzept mit eGK basiert auf dem authentischen Auslesen des C.CH.AUT (KVNR und IK-Nummer) aus der eGK über ein C2C-initiiertes Secure Messaging zwischen eGK und PoPP-Service. Die Zugriffsregeln der eGK G2.1 lassen dies jedoch bei der Kontaktloskommunikation nicht zu. Demnach kann nicht sichergestellt werden, dass dem PoPP-Service nicht ein anderes C.CH.AUT Zertifikat zur Gültigkeitsprüfung vorgelegt wird.

Um dennoch sicherzustellen, dass das CV-Zertifikat (ICCSN) und X.509.AUT-Zertifikat (C.CH.AUT) von derselben eGK stammen, muss ein Datenabgleich ermöglicht werden. Da es keine gemeinsamen Eigenschaften der beiden Zertifikate gibt, muss der Auftragsdatensatz bekannt sein oder die Daten bereits mindestens einmal authentisch (über die kontaktbehaftete Schnittstelle und PoPP) eingelesen werden. 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**. Mit der Abschaltung der VSDM1-Fachdienste, steht das CardLink-Verfahren aufgrund seiner Abhängigkeit zu den VSDM1-Fachdiensten nicht mehr zur Verfügung.

Mögliche Lösung

Über eine eGK-Hash-Datenbank wäre diese Szenario auch für eGK der Generation 2.1 möglich. Darüber kann man dann die Frage beantworten: Stammt ein vorgelegtes CV-Zertifikat und ein vorgelegtes X.509 Zertifikat aus ein und derselben eGK. (s.o.)

Material

Über eine eGK-Hash-Datenbank (s. eGK-Hash-Datenbank, Kap. 6.2.1.9) wäre diese Szenario auch für eGK der Generation 2.1 möglich. Darüber kann man dann die Frage beantworten: Stammt ein vorgelegtes CV-Zertifikat und ein vorgelegtes X.509 Zertifikat aus ein und derselben eGK.

1) https://www.gematik.de/newsroom/news-detail/popp-dienst-startet-mit-umsetzungsstufe-1-zuschlag-geht-an-rise.

2) https://www.apotheke-adhoc.de/nachrichten/detail/e-rezept/gesundde-naechste-loesung-fuer-e-rezepte/#.

3) https://gemspec.gematik.de/docs/gemKPT/gemKPT_PoPP/latest/#1.5.

4) Im Dokument ist auch allgemeiner vom „Versorgungskontext“ die Rede.

5) RFC 9449