

Telematikinfrastruktur 2.0

Feature: PoPP Stufe 2 - Online Check-in

Version: 1.0.0 CC
Revision: 1495788
Stand: 26.01.2026
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemF_PoPP_Online_Check-in

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	26.01.2026		initiale Einarbeitung	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments.....	6
1.1 Zielsetzung.....	6
1.2 Zielgruppe.....	6
1.3 Abgrenzungen.....	6
1.4 Methodik.....	7
1.4.1 Epic und User Story.....	7
1.4.2 Anforderungen.....	7
2 Konzept.....	8
2.1 Komponenten und Rollen.....	9
2.1.1 Apps/Anwendungen.....	9
2.1.2 Authentifizierung.....	10
2.1.3 Auswahl der LEI.....	10
2.1.4 PoPP-Modul.....	10
2.1.5 Informationen zur LEI: QR-Code / WorkplaceID.....	11
2.1.6 PoPP-Client.....	11
2.1.7 PoPP-Service.....	12
2.2 Abläufe (Workflows).....	12
2.2.1 Vor-Ort in Versorgungseinrichtung.....	13
2.2.2 Mobile Versorgung (beispielsweise Haus-/Heimbefuch).....	14
2.2.3 Fernversorgung (beispielsweise Videosprechstunde).....	14
2.2.3.1 Online-Check-in über eine Drittanbieter-App (voll integriert):.....	14
2.2.3.2 Online-Check-in über eine Drittanbieter-App mit Nutzung der Krankenversicherungs-App (App2App).....	15
2.3 Sicherheit.....	15
2.4 Technischer Workflow: Verarbeitung von LEI-Daten.....	16
2.4.1 Verarbeitung Telematik-ID.....	16
2.4.2 Verarbeitung WorkplaceID.....	17
2.5 Nicht Bestandteil des Dokuments.....	17
3 Einordnung in die Telematikinfrastruktur.....	18
4 Spezifikation.....	19
4.1 Änderungen in [gemSpec_Popp_Service].....	19
4.1.1 [gemSpec_PoPP_Service#2.1]: Überblick zum Ablauf eGK und GesundheitsID aus Versichertensicht.....	19
4.1.2 [gemSpec_PoPP_Service#2.2]: Überblick der Anwendungsfälle für die Ausstellung von PoPP-Token.....	19
4.1.3 [gemSpec_PoPP_Service#2.3]: Akteure und Rollen.....	22
4.1.3.1 [gemSpec_PoPP_Service#2.3.1.6]: Hersteller PoPP-Modul.....	23
4.1.3.2 [gemSpec_PoPP_Service#2.3.1.7]: Hersteller App.....	23
4.1.4 [gemSpec_PoPP_Service#3]: Systemkontext PoPP-Service.....	24
4.1.5 [gemSpec_PoPP_Service#3.1]: Produktzerlegung und Außenschnittstellen.....	24
4.1.6 [gemSpec_PoPP_Service#3.2]: Systemkontext.....	25

81	4.1.7 [gemSpec_PoPP_Service#3.3]: Nachbarsysteme.....	29
82	4.1.8 [gemSpec_PoPP_Service#4]: Funktionale Anwendungsfälle des PoPP-Service..	30
83	4.1.9 [gemSpec_PoPP_Service#4.1]: Übersicht der Systemanwendungsfälle für die	
84	Ausstellung des PoPP-Token.....	30
85	4.1.10 Neues Kapitel 4.5: Online-Check-in und Ausgabe des PoPP-Token.....	33
86	4.1.11 Neues Kapitel 4.5.1: Auswahl einer LEI für den Online-Check-in.....	35
87	4.1.11.1 Zugang zum FHIR-VZD.....	36
88	4.1.11.2 Ermittlung von Informationen zu einer LEI.....	36
89	4.1.12 Neues Kapitel 4.5.2: Online-Check-in mit GesundheitsID.....	36
90	4.1.13 Neues Kapitel 4.5.3: Online-Check-in mit eGK-in-Fernversorgung.....	42
91	4.1.14 Neues Kapitel 4.5.4: PoPP-Token bei Online-Check-in.....	49
92	4.1.15 Neues Kapitel 4.5.5: Status der PoPP-Token-Erstellung nach Online-Check-in	
93	ermitteln.....	52
94	4.1.16 Änderungen [gemSpec_PoPP_Service#5.3.4] PoPP-Service Signaturen.....	55
95	4.1.17 Änderungen [gemSpec_PoPP_Service#5.4]: ZETA Guard im PoPP-Service.....	55
96	4.1.18 Änderungen [gemSpec_PoPP_Service#5.6]: Federation Entity Statement.....	56
97	4.1.19 [gemSpec_PoPP_Service#6.1]- eGK-Handling.....	59
98	4.1.19.1 Ergänzung in Kap. 6.1.1 - eGK-Handling, Einführung.....	59
99	4.2 Änderungen in [gemILF_PoPP_Client].....	60
100	4.2.1 Erzeugung und Verwendung statischer QR-Codes für PoPP.....	60
101	4.2.2 WorkplaceID.....	61
102	4.2.3 Verbindung zum PoPP-Service herstellen und PoPP-Token abrufen.....	61
103	4.3 Änderungen in [gemSpec_PoPP_Modul].....	62
104	4.4 Änderungen in [api-popp].....	62
105	4.5 Änderungen in [gemSpec_ZETA].....	63
106	4.6 Änderungen in [gemSpec_IDP_Sek].....	63
107	4.7 Änderungen in [gemKPT_Test].....	64
108	4.7.1 Änderungen im Kapitel 7.4 Interoperabilität.....	65
109	4.8 Änderungen in [gemSpec_Perf].....	65
110	4.9 Änderungen in [gemKPT_Betr].....	68
111	5 Dokumentenhaushalt.....	69
112	6 Anhang A - Verzeichnisse.....	70
113	6.1 Abkürzungen.....	70
114	6.2 Glossar.....	70
115	6.3 Abbildungsverzeichnis.....	72
116	6.4 Tabellenverzeichnis.....	73
117	6.5 Referenzierte Dokumente.....	73
118	6.5.1 Dokumente der gematik.....	73
119	6.5.2 Weitere Dokumente.....	75
120	7 Anhang B - Anforderungshaushalt.....	77
121	7.1 Umsetzungsanforderungen.....	77
122	7.2 Blattanforderungen/ spezifische Festlegungen.....	77
123	8 Anhang C - Offene Punkte, Fragen.....	78

124	8.1 Offene Punkte.....	78
125		
126		

1 Einordnung des Dokuments

Dieses Feature-Dokument beschreibt das Konzept und die Anforderungen von PoPP Service Stufe 2: Online-Check-in. Neben dieser Feature-Dokument ist auch die neue Spezifikation [gemSpec_PoPP_Modul] relevant.

1.1 Zielsetzung

Diese Feature-Dokument dient Herstellern, Anbietern und Umsetzenden des PoPP-Services als Orientierung und bietet eine konsolidierte Übersicht über die neuen Anforderungen für den Online-Check-in bei PoPP. Dies betrifft alle Szenarien, in denen der Versicherte sein mobiles Endgerät für einen Online-Check-in verwendet.

Hierzu zählen alle Versorgungsszenarien, bei denen die Versicherten ihre GesundheitsID nutzen; und zwar sowohl in Versorgungseinrichtungen (Vor-Ort-Besuch), in der mobilen Versorgung (bspw. Hausbesuch) oder in der Fernversorgung (bspw. Videosprechstunde). Zudem umfasst dies alle Versorgungsszenarien, in denen die Versicherten ihre eGK in der Fernversorgung nutzen.

1.2 Zielgruppe

Dieses Dokument richtet sich an:

- den Hersteller und Anbieter des PoPP-Service,
- Hersteller von Produkttypen oder Komponenten, die eine Schnittstelle zum PoPP-Service besitzen (insbesondere PoPP-Modul- und Primärsystem-Hersteller),
- Hersteller und Anbieter von FD, die einen PoPP-Token nutzen.

1.3 Abgrenzungen

Dieses Feature-Dokument enthält Konzepte und Anforderungen, die für den PoPP-Service Stufe 2 relevant sind. Für Stufe 1 des PoPP-Services gilt die aktuelle Spezifikation [gemSpec_PoPP_Service].

Nach erfolgter Freigabe dieses Features (sowie [gemSpec_PoPP_Modul]) werden die entsprechenden Anteile aus dem Kapitel 4 "Spezifikation" in die [gemSpec_PoPP_Service], bzw. die anderen betroffenen Dokumente überführt. Die [gemSpec_PoPP_Service] wird dann für Stufe 1 und Stufe 2 gelten.

Die konzeptionellen Anteile dieses Feature-Dokuments (Fachliches Konzept und Technisches Konzept) verbleiben in [gemF_PoPP_Online_Check-in]. Diese wird dann ebenfalls veröffentlicht.

1.4 Methodik

1.4.1 Epic und User Story

<Methodik von Epic und User Story erläutern>

Epics und zugeordnete User Stories werden durch eine eindeutige ID gekennzeichnet.

Epic und UserStory werden im Dokument wie folgt dargestellt:

<Jira-ID> - <Zusammenfassung des Jira-Issue>

Text / Beschreibung

[<=]

Dabei umfasst die Anforderung sämtliche zwischen Jira-ID und Textmarke [<=]
angeführten Inhalte.

1.4.2 Anforderungen

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

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

Anforderungen werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke [<=]
angeführten Inhalte.

Hinweis auf offene Punkte

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

2 Konzept

Die Stufe 2 des PoPP-Services erweitert die Möglichkeiten zur Herstellung eines Versorgungskontexts zwischen einer Leistungserbringerinstitution (LEI) und Versicherten (VER). Neu eingeführt wird mit Stufe 2 der Online-Check-in für PoPP, der direkt am Smartphone des VER erfolgt. Dieser ermöglicht

- die Nutzung einer elektronischen Gesundheitskarte (eGK) ergänzend zur ersten Stufe auch in der Fernversorgung, beispielsweise bei Videosprechstunden oder Online-Diensten von Apotheken,
- die Nutzung einer GesundheitsID in allen Versorgungsszenarien, also auch vor-Ort in einer Versorgungseinrichtung.

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 Spezifikation [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 einer 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 den Zugriff auf die Versichertendaten in den Fachdiensten zur Verfügung gestellt.

Die App erhält durch den Online-Check-in keinen Zugriff auf die Versichertendaten im Fachdienst. Dieser Zugriff ist weiterhin, wie auch in Stufe 1, ausschließlich der berechtigten LEI vorbehalten, die zuvor durch den VER ausgewählt wurde.

Die Anwendungsfälle der Stufe 1, bei denen VER ihre eGK in Versorgungseinrichtungen vor Ort oder in mobilen Versorgungsszenarien, wie Heim- oder Hausbesuchen, nutzen, bleiben unverändert und sind in [gemSpec_PoPP_Service] dokumentiert.

Das folgende Kapitel enthält die fachliche Beschreibung des Online-Check-ins mit eGK und GesundheitsID in verschiedenen Versorgungsszenarien sowie in unterschiedlichen Apps (Krankenversicherungs-Apps und Drittanbieter-Apps). Zudem werden Möglichkeiten aufgezeigt, den Online-Check-in in (größeren) Einrichtungen einzelnen Arbeitsplätzen zuzuordnen und neben dem Scannen eines QR-Codes auch alternative Verfahren zur Auswahl der LEI bzw. zur Erfassung der Telematik-ID zu nutzen.

Die Abläufe werden lediglich skizziert und sind teilweise verkürzt oder vereinfacht dargestellt. Zur besseren Lesbarkeit ist im Folgenden von Apps und Smartphones die Rede; es sind jedoch ebenso Web-Anwendungen sowie die Nutzung an einem Desktop-PC

mit einem Standard-Kartenleser vorgesehen. Die vollständigen Abläufe sowie die detaillierten Anforderungen sind in [gemSpec_PoPP_Service] und [gemSpec_PoPP_Modul] beschrieben.

2.1 Komponenten und Rollen

Zunächst werden die Komponenten und Rollen für den Online-Check-in beschrieben, bevor im Anschluss der zugehörige Workflow dargestellt wird.

2.1.1 Apps/Anwendungen

Der Online-Check-in kann über verschiedene Arten von Anwendungen erfolgen sowie unterschiedlich durch Hersteller implementiert werden.

Es können sowohl Krankenversicherungen als auch Drittanbieter den Online-Check-in in Apps oder in (Web-)Anwendungen implementieren.

- **iOS-/Android-Apps der Krankenversicherungen:** Beispielsweise zur Nutzung des Online-Check-in für eine Praxis vor Ort am Smartphone mit GesundheitsID. Der Online-Check-in muss nicht zwingend im ePA FdV sein, es kann sich auch um eine separate Krankenversicherungs-App handeln.
- **iOS-/Android-Apps von Drittanbietern:** Beispielsweise Apotheken-App oder Videosprechstunden-App zur Nutzung des Online-Check-in am Smartphone für eine (Online-)Apotheke oder Praxis.
- **Webanwendungen von Drittanbietern:** Beispielsweise Patientenportal oder Videosprechstunden-Lösungen zur Nutzung des Online-Check-in am Desktop-PC oder Smartphone für ein Krankenhaus oder eine Praxis.

Die Funktion des Online-Check-ins kann durch Hersteller bzw. Dienstleister direkt implementiert werden oder von einer Krankenversicherungs-App nachgenutzt werden.

- **Online-Check-in über eine Drittanbieter-App (voll integriert):** Drittanbieter-Apps implementieren den Online-Check-in mit der Komponente PoPP-Modul. Der Vorteil bei Nutzung der eGK besteht darin, dass der komplette Online-Check-in innerhalb derselben App erfolgen kann. Bei Verwendung der GesundheitsID ist für die Authentifizierung hingegen ein Wechsel in die Krankenversicherungs-App mit integriertem Authenticator-Modul erforderlich. Der Schritt "Auswahl der LEI" kann für den VER entfallen, sofern die Telematik-ID bereits in der App hinterlegt ist.
- **Online-Check-in über eine Drittanbieter-App mit Nutzung einer Krankenversicherungs-App (App2App):** Drittanbieter-Apps implementieren nur den App-Sprung in die Krankenversicherungs-App, also ohne die Komponente PoPP-Modul. Es ist entsprechend immer ein Wechsel in die Krankenversicherungs-App mit PoPP-Modul erforderlich. Der Schritt "Auswahl der LEI" kann für den VER entfallen, sofern die Telematik-ID bereits hinterlegt ist.
- **Online-Check-in ausschließlich über eine Krankenversicherungs-App mit manueller Auswahl der LEI:** Krankenversicherungs-Apps mit PoPP-Modul werden verwendet, es ist kein App-Wechsel erforderlich, auch nicht bei Nutzung der GesundheitsID. Es ist immer die manuelle Auswahl der LEI durch die VER notwendig.

2.1.2 Authentifizierung

Die Authentifizierung kann auf unterschiedliche Weise für den Online-Check-in erfolgen:

- **GesundheitsID auf dem Smartphone:**Die GesundheitsID auf dem Smartphone der VER wird verwendet.Technisch erfolgt die Authentifizierung der VER bei der GesundheitsID stets über das Authenticator-Modul, das in derselben Krankenversicherungs-App integriert sein muss, in der auch das PoPP-Modul vorhanden ist.
- **eGK über NFC-Schnittstelle:**Die elektronische Gesundheitskarte (eGK) wird nach der CAN-Eingabe durch die VER über die NFC-Schnittstelle eingelesen, insbesondere auch bei der Nutzung am Smartphone der VER.
Technisch erfolgt die Authentifizierung der eGK durch den PoPP-Service über Card-to-Card-Authentisierung. Anders als bei der GesundheitsID wird nur die Karte authentifiziert, nicht jedoch die VER selbst.
- **eGK über Standardkartenleser:**Die eGK wird über einen Standardkartenleser eingelesen, insbesondere bei Nutzung an einem Desktop-Rechner der VER.
Technisch erfolgt die Authentifizierung der eGK durch den PoPP-Service über Card-to-Card-Authentisierung. Anders als bei der GesundheitsID wird auch hier nur die Karte authentifiziert, nicht jedoch die VER selbst.

2.1.3 Auswahl der LEI

VER müssen die LEI auswählen, bei der sie online einchecken wollen. Dafür wird die Telematik-ID der LEI benötigt. Diese kann auf verschiedene Weise durch die VER erfasst werden:

- **Scannen eines QR-Codes:**Ein statischer QR-Code, der die Telematik-ID beinhaltet und von der LEI als Aufsteller am Empfang bereitgestellt wird.
- **Hinterlegung in Apps:**Die Telematik-ID wird von der LEI direkt in der Drittanbieter-App hinterlegt, beispielsweise in einem Patientenportal oder einer Apotheken-App.
- **Manuelle Ermittlung über VZD-Suche in der App:**Die LEI mit der notwendigen Telematik-ID wird durch eine manuelle Suche im Verzeichnisdienst (VZD) ermittelt.
- **Historie oder Favoriten in der App:**Die Telematik-ID wird durch Auswahl der LEI über einen Eintrag aus der Historie der letzten Online-Check-ins oder aus angelegten Favoriten ermittelt.

2.1.4 PoPP-Modul

Das PoPP-Modul ist eine neue Komponente in den Apps, die für den Online-Check-in erforderlich sind und ermöglicht die notwendige Kommunikation mit dem PoPP-Service.

Das PoPP-Modul muss nicht zwingend in die App, die den Online-Check-in nutzen möchte, integriert werden. Vielmehr kann eine Drittanbieter-App ein PoPP-Modul einer Krankenversicherungs-App via App2App nachnutzen.

Im Gegensatz zum PoPP-Client, der eine Komponente des Primärsystems (PS) ist und von LEI-Personal genutzt wird, ist das PoPP-Modul für Apps vorgesehen, die von VER verwendet werden.

Technisch erfolgt die sichere Kommunikation für den Online-Check-in immer über die Komponenten der Zero-Trust-Architektur, das heißt, die App mit PoPP-Modul benötigt zusätzlich einen ZETA-Client, der mit ZETA Guard im PoPP-Service kommuniziert.

2.1.5 Informationen zur LEI: QR-Code / WorkplacelD

Der QR-Code erleichtert insbesondere vor Ort in Versorgungseinrichtungen oder in mobilen Versorgungsszenarien (zum Beispiel Heim- oder Hausbesuch) die LEI-Auswahl zur Erfassung der Telematik-ID. Dies erfolgt, indem der QR-Code aus der App, in der der Online-Check-in integriert ist, von der VER abgescannt wird.

Zusätzlich kann der QR-Code weitere Informationen enthalten, nämlich eine optionale WorkplacelD, die verschiedenen Aufgaben übernehmen kann.

- **Arbeitsplatzzuordnung:**Die WorkplacelD kann in Einrichtungen mit mehreren Arbeitsplätzen am Empfang zur besseren Organisation dienen. Sie ermöglicht es, QR-Codes gezielt einem Arbeitsplatz zuzuordnen, sodass der Online-Check-in einer VER direkt dem richtigen Arbeitsplatz zugeordnet werden kann.
- **SessionID:**Die WorkplacelD kann zusammen mit der Telematik-ID auch in Drittanbieter-Apps hinterlegt werden, um als SessionID eine richtige Zuordnung zwischen Aktionen in einer App der VER und dem PoPP-Token nach dem erfolgreichen Online-Check-in im PS der LEI zu gewährleisten.

Die LEI muss dazu einmalig einen QR-Code im Praxisverwaltungssystem (PS) generieren. Optional kann für jeden Arbeitsplatz ein separater QR-Code mit einer spezifischen WorkplacelD erstellt werden. Diese QR-Codes können entweder am Empfang als Zettel oder auf einem Bildschirm platziert oder bei mobilen Versorgungsszenarien mitgebracht werden.

Erfolgt die Auswahl der LEI in der Krankenversicherungs-App jedoch aus dem Verzeichnisdienst (VZD), den Favoriten oder der Historie, wird keine WorkplacelD übermittelt und entsprechend nicht verarbeitet.

2.1.6 PoPP-Client

Die grundlegende Aufgabe des PoPP-Clients bleibt im Vergleich zur Stufe 1 unverändert, nämlich die Verarbeitung und Verwaltung von PoPP-Token zum Zugriff einer LEI auf die Versichertendaten.

In Stufe 2 erweitert sich die Funktionalität des PS. Es muss zusätzlich einen QR-Code für den Online-Check-in erstellen und in der Lage sein, arbeitsplatzbezogene Check-ins zu verarbeiten. Darüber hinaus wird es erforderlich, PoPP-Token beispielsweise nach einer Offline-Phase abrufen zu können.

Die sichere Kommunikation beim Online-Check-in erfolgt technisch stets über die Komponenten der Zero-Trust-Architektur. Das bedeutet, ein Primärsystem mit PoPP-Client benötigt einen ZETA-Client, der mit ZETA Guard innerhalb des PoPP-Services kommuniziert.

2.1.7 PoPP-Service

Die grundlegende Aufgabe des PoPP-Services bleibt im Vergleich zu Stufe 2 unverändert. Im PoPP-Service werden PoPP-Token erzeugt und nach erfolgreicher Authentifizierung der LEI sowie nach dem Ausweisen der VER an die LEI übermittelt.

Neu ist, dass der PoPP-Service auch mit dem PoPP-Modul kommuniziert. Dadurch kann sich eine VER direkt über ihr Smartphone für den Online-Check-in ausweisen, eine LEI auswählen und deren Telematik-ID an den PoPP-Service übermitteln. Zusätzlich wird die Verarbeitung von VZD-Anfragen integriert.

2.2 Abläufe (Workflows)

Zunächst wird als Happy Path der Online-Check-in mittels Krankenversicherungs-App mit PoPP-Modul und GesundheitsID vor Ort in einer Versorgungseinrichtung tabellarisch beschrieben. Ergänzend werden exemplarisch einzelne Alternativen mit aufgeführt.

Anschließend folgt die Beschreibung der einzelnen Workflows in folgenden Versorgungsszenarien:

- vor Ort in einer Versorgungseinrichtung,
- mobiles Versorgungsszenario (zum Beispiel Haus- oder Heimbefuch),
- Fernversorgung (zum Beispiel Online-Dienst einer Apotheke oder Videosprechstunde).

Bereits in Stufe 1 umgesetzte Versorgungsszenarien, eGK in vor-Ort-Versorgungseinrichtungen und in der mobilen Versorgung (beispielsweise Haus- und Heimbefuch) werden nicht noch einmal aufgeführt.

Die Reihenfolge der Schritte bleibt beim Online-Check-in dabei stets gleich, unabhängig vom Versorgungsszenario, wobei einzelne Schritte je nach Anwendungsfall entfallen oder im Inhalt variieren können.

Der Ablauf des Happy Path ist visuell als Click-Dummy aufrufbar: [Link](#)

ID	Beschreibung
Einstieg	<p>VER öffnet seine Krankenversicherungs-App auf seinem Smartphone beim Betreten der Versorgungseinrichtung.</p> <p>Alternativ VER checkt über eine Drittanbieter-App ein, zum Beispiel zuhause mit einer Videosprechstunden-App.</p>
Check-in	<p>VER wählt die Funktion "Online-Check-in" in der App mit PoPP-Modul aus.</p>
Auswahl der LEI	<p>LEI stellt einen statischen QR-Code (Zettel, Bildschirm) am Empfang sichtbar bereit. Dieser enthält die Telematik-ID. VER scannt am Empfang den QR-Code</p> <p>Alternativ, wenn beispielsweise in der Fernversorgung kein QR-Code gescannt werden kann VER wählt manuell die LEI über die App aus über eine Historie-/Favoritenfunktion oder durch eine Suche im Verzeichnisdienst (VZD). Die Auswahl kann auch entfallen, wenn die LEI mit der Telematik-ID bereits in der Drittanbieter-App hinterlegt ist, beispielsweise bei einer Apotheken-App.</p>
Einwilligungen	<p>VER wird in der App der Name der LEI inkl. Adresse angezeigt, welche zur ausgewählten Telematik-ID gehört; via VZD-Abruf</p> <p>VER bestätigt nach der Kontrolle den Online-Check-in.</p>

Authentifizierung	<p>VER weist sich mit seiner GesundheitsID auf seinem Smartphone aus; via Authenticator-Modul in der Krankenversicherungs-App</p> <p>Alternativ VER weist sich mittels eGK ohne PIN (mit CAN) über die NFC-Schnittstelle am Smartphone aus. <i>Dies erfolgt via Card-to-Card-Authentisierung mit PoPP-Service</i></p>
Anfrage an PoPP-Service	Nach erfolgreicher Authentifizierung übermittelt das PoPP-Modul die relevanten Daten, insbesondere die Telematik-ID, und sofern vorhanden die WorkplaceID sowie den Authentifizierungsnachweis, an den PoPP-Service.
PoPP-Token-Erstellung	PoPP-Service prüft die Daten, generiert ein PoPP-Token und übermittelt dieses an das Primärsystem der LEI.
Statusinformation	<p>VER wird nach erfolgreicher Authentifizierung in der App eine Statusmeldung vom PoPP-Service angezeigt, die den erfolgreichen Online-Check-in bei der ausgewählten LEI bestätigt.</p> <p>Alternativ VER kann auch angezeigt werden, dass der Online-Check-in noch ausstehend ist, beispielsweise wenn die LEI bei einer Fernversorgung noch nicht online ist. In diesem Fall kann eine Statusänderung auch nachträglich übermittelt und der VER angezeigt werden.</p>
Abschluss	LEI erhält das PoPP-Token und kann damit, sofern diese berechtigt ist, auf die Versichertendaten in den Fachdiensten zugreifen

2.2.1 Vor-Ort in Versorgungseinrichtung

VER nutzt eGK (UC_PoPP_1a)

Bereits mit der ersten Stufe umgesetzt/keine Änderung. Beschreibung siehe [gemSpec_PoPP_Service].

VER nutzt GesundheitsID (UC_PoPP_1b)

Für das Einchecken vor Ort in einer Versorgungseinrichtung findet der Online-Check-in für gewöhnlich nur mit Nutzung der GesundheitsID Verwendung. Die eGK wird weiterhin für das Einchecken über ein eHealth-Kartenterminal oder einen Standardkartenleser der LEI eingelesen.

Der bevorzugte Weg in diesem Versorgungsszenario sollte das Einchecken über eine Krankenversicherungs-App und das Scannen eines QR-Codes durch den VER sein, es können jedoch auch Drittanbieter-Apps verwendet werden. Die Nutzung der GesundheitsID würde bei Verwendung von Drittanbieter-Apps jedoch stets einen Wechsel in die Krankenversicherungs-App mit Authentifizierungsmodul erfordern.

Im Anschluss übermittelt der PoPP-Service den PoPP-Token in das PS der LEI und ermöglicht der LEI den Zugriff auf die Versichertendaten in den Fachdiensten. Sofern die optionale WorkplaceID im QR-Code enthalten ist, kann eine arbeitsplatzbezogene Zuordnung über das PS erfolgen.

Entspricht dem Ablauf des Happy Path. Ablauf des Happy Path ist visuell als Click-Dummy aufrufbar: [Link](#)

2.2.2 Mobile Versorgung (beispielsweise Haus-/Heimbesuch)

VER nutzt eGK (UC_PoPP_2a)

Bereits mit der ersten Stufe umgesetzt/keine Änderung.

VER nutzt GesundheitsID (UC_PoPP_2b)

Der Online-Check-in in der mobilen Versorgung unterscheidet sich nicht von einem Online-Check-in vor Ort. Der einzige Unterschied besteht darin, dass die LEI den QR-Code mit zur VER nimmt.

2.2.3 Fernversorgung (beispielsweise Videosprechstunde)

LEI beziehungsweise deren Dienstleister können je nach Anwendungsfall den VER verschiedene Lösungen für den Online-Check-in in der Fernversorgung anbieten. VER können auch hier zwischen eGK und GesundheitsID wählen, sofern der Anwendungsfall nicht die Nutzung einer GesundheitsID zwingend voraussetzt.

Die verwendete Lösung hat Einfluss auf den Ablauf, also konkret darauf, ob eine oder zwei Apps für den Online-Check-in erforderlich sind und ob eine VER die LEI manuell auswählt oder dieser Schritt entfällt.

2.2.3.1 Online-Check-in über eine Drittanbieter-App (voll integriert):

VER nutzt GesundheitsID (UC_PoPP_3a) oder eGK (UC_PoPP_3c)

Bei Nutzung der eGK kann der Online-Check-in komplett über die Drittanbieter-App erfolgen. Diese Variante dient als Nachfolger u.a. für den Anwendungsfall, der derzeit noch über den eHealth-Cardlink umgesetzt, aber nach der Abschaltung von VSDM1 dann nicht mehr zur Verfügung stehen wird.

Bei Nutzung der GesundheitsID ist für den reinen Authentifizierungsvorgang zwingend ein App-Wechsel in die Krankenversicherungs-App mit Authentifizierungsmodul erforderlich, die anderen Schritte verbleiben in der Drittanbieter-App.

Im Anschluss übermittelt der PoPP-Service den PoPP-Token in das PS der LEI und ermöglicht der LEI den Zugriff auf die Versichertendaten in den Fachdiensten. Sofern die optionale WorkplaceID verwendet wurde, kann diese, als SessionID genutzt, die richtige Zuordnung zwischen Aktionen der VER in der App und dem PoPP-Token im PS der LEI ermöglichen (bspw. für Online-Dienste von Apotheken)

Der Implementierungsaufwand dieser Variante ist im Vergleich zu den folgenden Varianten höher, da sowohl ein Zero-Trust-Client als auch ein PoPP-Modul in der Drittanbieter-App implementiert werden müssen.

- Ablauf in einer Drittanbieter-App am Beispiel einer Apotheken-App und Nutzung der eGK ist visuell als Click-Dummy aufrufbar: [Link](#)

2.2.3.2 Online-Check-in über eine Drittanbieter-App mit Nutzung der Krankenversicherungs-App (App2App)

UC_PoPP_3b (GesundheitsID) und UC_PoPP_3d (eGK)

Diese Variante erfordert insgesamt weniger Implementierungsaufwand. Hier erfolgt nur die Auswahl der LEI in der App bzw. ist in der App bereits hinterlegt. Anschließend erfolgen alle weiteren Schritte in der Krankenversicherungs-App. Der Wechsel erfolgt automatische inkl. Übergabe der LEI-Auswahl (TelematikID und optional WorkplaceID)

und nach dem erfolgreichen Check-in kehrt der Nutzer wieder in die ursprüngliche Drittanbieter-App zurück. Die Drittanbieter-App ist dabei auf die Art der Umsetzung des Online-Check-ins in der Krankenversicherungs-App angewiesen.

Im Anschluss übermittelt der PoPP-Service den PoPP-Token in das PS der LEI und ermöglicht der LEI den Zugriff auf die Versichertendaten in den Fachdiensten. Sofern die optionale WorkplaceID verwendet wurde, kann diese, als SessionID genutzt, die richtige Zuordnung zwischen Aktionen der VER in der App und dem PoPP-Token im PS der LEI ermöglichen (bspw. für Online-Dienste von Apotheken)

- Der Ablauf in einer Drittanbieter-App ohne Implementierung des PoPP-Moduls am Beispiel einer Apotheken-App und Krankenversicherungs-App mit Nutzung der eGK ist visuell als Click-Dummy aufrufbar: [Link](#)
- Sowie mit einer Videosprechstunden-App und mit Nutzung der GesundheitsID: [Link](#)

Wird keine Drittanbieter-App verwendet ist ein Online-Check-in auch in der Fernversorgung ausschließlich über die Krankenversicherungs-App mit manueller Auswahl der LEI möglich.

Die VER muss entweder einen QR-Code über die Krankenversicherungs-App einscannen, der von der LEI bereitgestellt wird (zum Beispiel über eine Website eines Online-Dienstes wie eines Patientenportals oder per Messenger/E-Mail, etwa als Ankündigungsmail für eine Videosprechstunde) oder die LEI manuell in der Krankenversicherungs-App auswählen.

2.3 Sicherheit

Die Maßnahmen tragen dazu bei, dass genau die LEI den PoPP-Token erhält, welcher die VER auch den Zugriff auf ihre Versichertendaten in den Fachdiensten geben möchte.

- **Keine URL im QR-Code**
Im QR-Code ist keine URL kodiert. Bei Nutzung einer Standard-Kamera- oder QR-Code-App führt der Scan somit zu keinem Ergebnis. VER gewöhnen sich dadurch daran, die vorgesehene App mit PoPP-Modul zu verwenden, die falsche QR-Codes erkennt und den Nutzer warnt sowie an LEI-Personal verweist.
- **Bestätigung für Versicherte**
Die VER muss vor dem eigentlichen Online-Check-in zunächst die LEI bestätigen. Hierzu erfolgt ein VZD-Abruf der erfassten Telematik-ID mit anschließender Anzeige des Namens der LEI inklusive Adresse. Die VER muss den Check-in anhand dieser Daten explizit bestätigen. Nach dem Online-Check-in erhält die VER zudem eine Bestätigung in Form einer Statusmeldung zum Verlauf des Check-ins (erfolgreich, laufend, abgebrochen), jeweils inklusive des Namens der LEI.
- **Verantwortung für QR-Code-Inhalte**
Der statische QR-Code wird im PS erzeugt und in einer LEI aufgestellt bzw. positioniert. Die LEI trägt die Verantwortung für die Richtigkeit der im gezeigten QR-Code enthaltenen Inhalte sowie dafür unbekannte oder als fehlerhaft gemeldete 2D-Codes zu entfernen.
- **Minimierung der zu verarbeitenden Daten in der App**
Für den Online-Check-in benötigt das PoPP-Modul in der App selbst lediglich die Telematik-ID, weder die Krankenversicherungsnummer (KVNR) noch andere persönliche Daten der VER.
- **Unterscheidung und Sperrbarkeit von PoPP-Modulen**
Eine Unterscheidung der verschiedenen Apps die PoPP-Module beinhalten kann auf

Basis der ZETA-Guard-Client-Registry erfolgen. Apps mit PoPP-Modul können somit falls notwendig auch nachträglich vom PoPP ausgeschlossen werden.

- **Information über die Authentifizierung**

Der PoPP-Token enthält die Information, ob der Online-Check-in über ein App mit PoPP-Modul von der VER durchgeführt wurde und auf welche Weise sich die Identität der VER verifiziert wurde, also mittels GesundheitsID oder elektronischer Gesundheitskarte (eGK). Unter anderem wird diese Information von den Fachdiensten für die Zugriffsregelung genutzt, wenn für einen Use Case bspw. eine authentifizierte eGK nicht ausreicht und eine Authentifizierung der VER, also die Verwendung der GesundheitsID, erforderlich ist.

2.4 Technischer Workflow: Verarbeitung von LEI-Daten

Es gelten folgende Regelungen und Maßnahmen für die Verarbeitung der LEI-Daten Telematik-ID und WorkplaceID bei PoPP.

Die WorkplaceID ist nicht Teil des PoPP-Tokens und hat keinen Einfluss auf die Berechtigung der LEI auf die Versichertendaten in den Fachdiensten zuzugreifen. Folglich unterscheidet sich auch die technische Verarbeitung.

2.4.1 Verarbeitung Telematik-ID

- Die Telematik-ID wird vom PoPP-Modul für die VZD-Suche benutzt (Consent-Dialog).
- Die Telematik-ID wird an den PoPP-Service übergeben, um einen PoPP-Token für die zugehörige LEI zu erstellen.
- Der PoPP-Service prüft anhand der Telematik-ID, ob die zugehörige LEI authentisiert ist, und verwendet die Informationen zur Erstellung eines PoPP-Tokens.
- Der erstellte PoPP-Token wird an das Primärsystem der zur Telematik-ID zugehörigen LEI übermittelt.

2.4.2 Verarbeitung WorkplaceID

- Die WorkplaceID wird lediglich im Primärsystem einer LEI verwendet. Daher wird die WorkplaceID als (transparenter) Parameter durch den PoPP-Service geschleust.
- Die Übergabe der WorkplaceID erfolgt gemeinsam mit der Telematik-ID als Parameter des HTTP-Requests an den PoPP-Service.
- Der PoPP-Service bewahrt die Information WorkplaceID gemeinsam mit der Telematik-ID auf.
- Bei der Übermittlung des PoPP-Tokens an eine LEI übergibt der PoPP-Service die Information zur WorkplaceID innerhalb der HTTP-Nachricht, mit der der PoPP-Token übermittelt wird. Die WorkplaceID ist nicht Teil des PoPP-Tokens.
- Der PoPP-Service muss die WorkplaceID übermitteln, wenn er sie zuvor vom PoPP-Modul erhalten hat.
- Das Primärsystem prüft, ob eine WorkplaceID in der Übermittlungsnachricht eines PoPP-Tokens enthalten ist, und benutzt die Information, um das PoPP-Token an den richtigen Arbeitsplatz zu übermitteln oder eine Zuordnung zwischen Aktionen in einer App der VER und dem PoPP-Token herzustellen

518 **2.5 Nicht Bestandteil des Dokuments**

519 Nicht Teil des Dokuments ist die weitere Verwendung des PoPP-Tokens, nachdem dieser
520 ins PS übermittelt und verarbeitet wird. Die Regelungen zum Zugriff mittels PoPP-Token
521 auf die Versichertendaten erfolgen durch den jeweiligen Fachdienst. Der PoPP-Token
522 enthält neben der Rolle der LEI (professionOID) dazu Informationen, ob der Online-Check-
523 in am Gerät der VER verwendet wurde und wie sich die VER ausgewiesen hat, also mit
524 GesundheitsID oder eGK, anhand derer der Fachdienst über den Zugriff entscheiden
525 kann.

3 Einordnung in die Telematikinfrastruktur

Das Feature "Online Check-in" bildet die Stufe 2 des PoPP-Services.

Im Primärsystem der LEI wird ein statischer QR-Code erzeugt und vom Versicherten über die Versicherten-App (PoPP-Modul) gescannt. Der QR-Code stellt hierbei u.a. die Information bereit, um welche LEI (Telematik-ID) es sich handelt, bei der sich die VER einchecken möchte. Die Kommunikation mit dem PoPP-Service erfolgt über gesicherte Schnittstellen.

Die Anforderungen zu Inhalt und Format sowie zum Prüfen und Verarbeiten des statischen QR-Codes richten sich an das PoPP-Modul und sind in [gemSpec_PoPP_Modul] enthalten.

Die Anforderungen an die Erzeugung des QR-Codes richten sich an die Primärsysteme und sind in [gemILF_PoPP_Client] enthalten.

4 Spezifikation

In diesem Kapitel werden alle Änderungen an bestehenden Spezifikationen, die das Feature PoPP Online-Check-in abbilden, beschrieben. Für jede Spezifikation ist jeweils ein Unterkapitel vorgesehen.

4.1 Änderungen in [gemSpec_Popp_Service]

Es werden die Änderungen am PoPP Service für die Stufe 2 (Online-Check-in) an [gemSpec_PoPP_Service] dargestellt.
Es wird immer ein Bezug zum Zielkapitel in [gemSpec_PoPP_Service] hergestellt.

4.1.1 [gemSpec_PoPP_Service#2.1]: Überblick zum Ablauf eGK und GesundheitsID aus Versichertensicht

Kapitel 2.1 wird durch folgenden Text ersetzt:

Der Nachweis des Versorgungskontexts (PoPP-Token) erfordert eine Authentifizierung auf Seiten der LEI und des Versicherten.

Die LEI authentifiziert sich mit ihrer SMC-B. Für den Versicherten wird seine eGK authentifiziert. Dieser Authentifizierungsprozess wird als Check-in bezeichnet. Der Versicherte präsentiert seine eGK an einem geeigneten Lesegerät der LEI oder übergibt die eGK an LEI-Personal. Alles Weitere führt der PoPP-Client durch.

Für den Online-Check-in am Gerät der VER hat die VER die Wahl und authentifiziert sich entweder mittels GesundheitsID oder die eGK wird authentifiziert. Beim Online-Check-in kommt auf dem Gerät des Versicherten das PoPP-Modul zum Einsatz. Der Online-Check-in ist für alle Versorgungskontexte verfügbar. Beispielsweise für Videosprechstunden-Anwendungen ist der Online-Check-in die einzige Möglichkeit, die den Versicherten für einen Check-in zur Verfügung steht.

4.1.2 [gemSpec_PoPP_Service#2.2]: Überblick der Anwendungsfälle für die Ausstellung von PoPP-Token

Kapitel 2.2 wird durch folgenden Text ersetzt:

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

Bei der Beschreibung der Anwendungsfälle wird zwischen der Nutzung der eGK und der GesundheitsID durch den Versicherten unterschieden. Auf Seiten der Leistungserbringer (LEI) wird zudem unterschieden, ob der Versorgungskontext während der physischen Anwesenheit von Versicherten und LEI entsteht (vor Ort in einer Versorgungseinrichtung oder bei mobiler Versorgung wie Praxisbesuchen oder Haus-/Heimbesuchen) oder ob die LEI virtuell anwesend ist (bei Fernversorgung wie Videosprechstunden).

Zusätzlich wird unterschieden, ob bei der Nutzung einer App ein PoPP-Modul integriert ist oder nicht und stattdessen eine Krankenversicherungs-App nachgenutzt wird (App2App).

Tabelle 1: PoPP-Use Cases (Business Sicht)

ID	Anwendungsfälle
UC_PoPP_1a	<p>Vor-Ort in Versorgungseinrichtung mit <u>eGK</u>: bspw. Praxisbesuch</p> <p>Ein Versicherter möchte eine Versorgung in einer LEI in Anspruch nehmen. Die LEI benötigt für den Zugriff auf die Daten des physisch anwesenden Versicherten einen Nachweis des Versorgungskontexts. Dazu wird die eGK des Versicherten an einem geeigneten Lesegerät der LEI präsentiert. Nachdem der Versicherte den Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontexts.</p>
UC_PoPP_1b	<p>Vor-Ort in Versorgungseinrichtung mit <u>GesundheitsID</u>: bspw. Praxisbesuch</p> <p>Ein Versicherter möchte eine Versorgung in einer LEI in Anspruch nehmen. Die LEI benötigt für den Zugriff auf die Daten des physisch anwesenden Versicherten einen Nachweis des Versorgungskontexts. Dazu startet der Versicherte den Online-Check-in-Prozess in einer App mit integriertem PoPP-Modul, scannt den von der LEI für den Check-in bereitgestellten QR-Code, bestätigt die LEI und authentifiziert sich anschließend mittels GesundheitsID. Nachdem der Versicherte den Online-Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontexts.</p>
UC_PoPP_2a	<p>In mobiler Versorgung mit <u>eGK</u>: bspw. Haus-/Heimbesuch</p> <p>Ein Versicherter möchte eine Versorgung außerhalb einer LEI in Anspruch nehmen. Dazu kommt das Personal der LEI zum Versicherten. Die LEI benötigt für den Zugriff auf die Daten des physisch anwesenden Versicherten einen Nachweis des Versorgungskontexts. Dazu wird die eGK des Versicherten an einem geeigneten mobilen Lesegerät der LEI präsentiert. Nachdem das LEI-Personal die eGK eingelesen hat, ist der Check-in-Vorgang abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontexts.</p>
UC_PoPP_2b	<p>In mobiler Versorgung mit <u>GesundheitsID</u>: bspw. Haus-/Heimbesuch</p> <p>Ein Versicherter möchte eine Versorgung außerhalb einer LEI in Anspruch nehmen. Dazu kommt das Personal der LEI zum Versicherten. Die LEI benötigt für den Zugriff auf die Daten des physisch anwesenden Versicherten einen Nachweis des Versorgungskontexts. Dazu startet der Versicherte den Online-Check-in-Prozess in einer App mit integriertem PoPP-Modul, scannt den von der LEI für den Check-in bereitgestellten QR-Code, bestätigt die LEI und authentifiziert sich anschließend mittels GesundheitsID. Nachdem der Versicherte den Online-Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontexts.</p>
UC_PoPP_3a	<p>In Fernversorgung mit <u>GesundheitsID</u>: bspw. Videosprechstunde</p>

	<p><i>Online-Check-in über Krankenversicherungs-App oder Drittanbieter-App mit PoPP-Modul</i></p> <p>Ein Versicherter möchte virtuell eine Versorgung einer LEI in Anspruch nehmen. Die LEI benötigt für den Zugriff auf die Daten des Versicherten den Nachweis des Versorgungskontexts. Dazu startet der Versicherte zuvor den Online-Check-in-Vorgang in einer App mit integriertem PoPP-Modul, bestätigt die LEI und authentifiziert sich anschließend mittels GesundheitsID. Nachdem der Versicherte den Online-Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontexts.</p>
UC_PoPP_3b	<p>In Fernversorgung mit <u>GesundheitsID</u>: bspw. Videosprechstunde <i>Online-Check-in über Drittanbieter-App, die PoPP-Modul einer Krankenversicherungs-App nachnutzt (App2App)</i></p> <p>Ein Versicherter möchte virtuell eine Versorgung einer LEI in Anspruch nehmen. Die LEI benötigt für den Zugriff auf die Daten des Versicherten den Nachweis des Versorgungskontexts. Dazu startet der Versicherte zuvor den Online-Check-in-Vorgang in einer App ohne integriertes PoPP-Modul. Anschließend öffnet sich die App der Krankenversicherung mit PoPP-Modul, der Versicherte bestätigt die LEI und authentifiziert sich mittels GesundheitsID. Nachdem der Versicherte den Online-Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontexts.</p>
UC_PoPP_3c	<p>In Fernversorgung mit <u>eGK</u>: bspw. Videosprechstunde <i>Online-Check-in über Krankenversicherungs-App oder Drittanbieter-App mit PoPP-Modul</i></p> <p>Ein Versicherter möchte virtuell eine Versorgung einer LEI in Anspruch nehmen. Die LEI benötigt für den Zugriff auf die Daten des Versicherten den Nachweis des Versorgungskontexts. Dazu startet der Versicherte zuvor den Online-Check-in-Vorgang in einer App mit integriertem PoPP-Modul, bestätigt die LEI und authentifiziert die eGK durch Präsentation der eGK an der NFC-Schnittstelle seines Smartphones. Nachdem der Versicherte den Online-Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontexts.</p>
UC_PoPP_3d	<p>In Fernversorgung mit <u>eGK</u>: bspw. Videosprechstunde <i>Online-Check-in über Drittanbieter-App, die PoPP-Modul einer Krankenversicherungs-App nachnutzt (App2App)</i></p> <p>Ein Versicherter möchte virtuell eine Versorgung einer LEI in Anspruch nehmen. Die LEI benötigt für den Zugriff auf die Daten des Versicherten den Nachweis des Versorgungskontexts. Dazu startet der Versicherte zuvor den Online-Check-in-Vorgang in einer App ohne integriertes PoPP-Modul. Anschließend öffnet sich die App der Krankenversicherung mit PoPP-Modul, der Versicherte bestätigt die LEI und authentifiziert die eGK durch Präsentation der eGK an der NFC-Schnittstelle seines Smartphones. Nachdem der Versicherte den Online-Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und die LEI erhält im PS den notwendigen Nachweis des Versorgungskontexts.</p>

Hinweis: Das vom PoPP-Service erstellte PoPP-Token enthält die Information, mit welcher Methode (siehe proofMethod im Kapitel "PoPP-Token-Erstellung") der Versorgungskontext nachgewiesen wurde. Somit ist es den PoPP-Token nutzenden Anwendungen und Diensten möglich, in ihrem Anwendungs- oder Dienstkontext Autorisierungsentscheidungen auch aufgrund der Prüfmethode zu treffen.

4.1.3 [gemSpec_PoPP_Service#2.3]: Akteure und Rollen

In Kapitel 2.3.1 Herstellung und Betrieb wird die Abbildung 2 "Rollen und Akteure bei Herstellung und Betrieb des PoPP-Service" um die Akteure Hersteller PoPP-Modul und Hersteller App erweitert:

neu

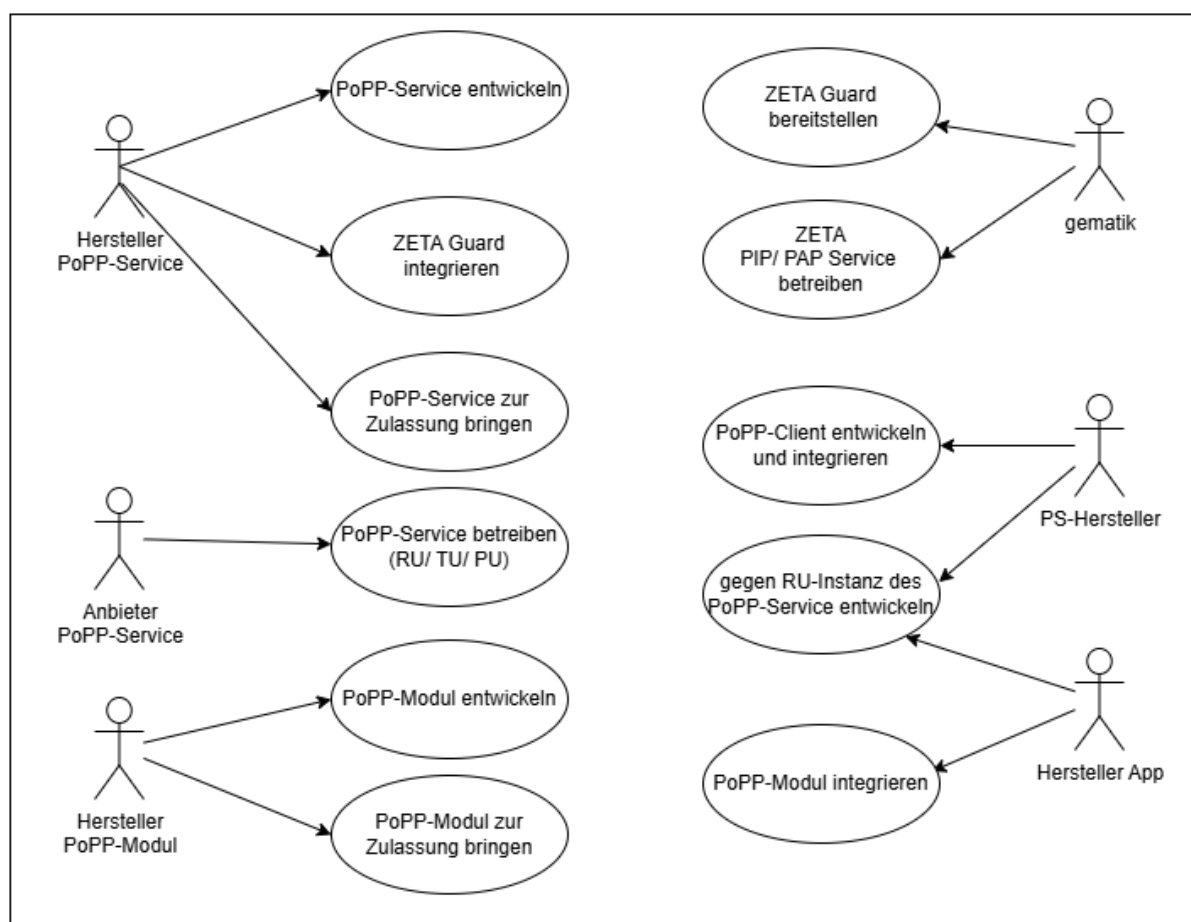


Abbildung 1: Rollen und Akteure bei Herstellung und Betrieb des PoPP-Service

Es werden in der Folge zwei Unterkapitel für Hersteller PoPP-Modul und Hersteller App ergänzt

4.1.3.1 [gemSpec_PoPP_Service#2.3.1.6]: Hersteller PoPP-Modul

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

599 [gemSpec_PoPP_Modul].
600 Der Hersteller PoPP-Modul erwirkt eine Produktzulassung für sein PoPP-Modul.

601 **4.1.3.2 [gemSpec_PoPP_Service#2.3.1.7]: Hersteller App**

602 App-Hersteller integrieren das PoPP-Modul eines PoPP-Modul-Herstellers für einen Online-
603 Check-in-Prozess. Sie entwickeln Funktionalität für die Unterstützung des Online-Check-
604 ins. Sie nutzen den PoPP-Service in der RU, um die Funktionalität zu testen. Sie
605 registrieren jede App-Version bei der gematik, damit die entsprechenden
606 Attestierungsdaten im ZETA hinterlegt werden können.

607 **4.1.4 [gemSpec_PoPP_Service#3]: Systemkontext PoPP-Service**

608 **Das alte Kapitel 3 inklusive der Unterkapitel wird durch Folgendes ersetzt**
609 **(enthält Stufe 1 und Stufe 2):**

610 In diesem Kapitel findet sich die logische Zerlegung des Produkttyps PoPP-Service anhand
611 eines Komponentendiagramms, die Beschreibung des Systemkontexts mit allen
612 bereitstellenden Außenschnittstellen des PoPP-Service sowie die Auflistung und kurze
613 Beschreibung der Nachbarsysteme.

614 **4.1.5 [gemSpec_PoPP_Service#3.1]: Produktzerlegung und** 615 **Außenschnittstellen**

616 Das Produkt PoPP-Service besteht aus mehreren Komponenten. Die Komponenten für die
617 Erstellung des PoPP-Token sind im Produkttyp PoPP-Service zusammengefasst. Die
618 Kommunikation zwischen LEI und PoPP-Service wird durch einen ZETA Guard
619 abgesichert. Die Kommunikation für den Online-Check-in zwischen einem Versicherten
620 und dem PoPP-Service erfolgt über ein PoPP-Modul und ZETA Client welche in einer App
621 auf dem Gerät des Versicherten integriert sein müssen.

622 Der Produkttyp PoPP-Service besteht aus mehreren Komponenten, die unterschiedliche
623 Aufgaben erfüllen. Für die Bearbeitung von Token Requests, bei denen die elektronische
624 Gesundheitskarte (eGK) verwendet wird, gehören dazu die eGK-Kommunikation, die eGK-
625 Hash-Datenbank sowie Funktionen zur Unterstützung kontaktlos angebundener eGK. Für
626 Fälle, in denen Versicherte die GesundheitsID nutzen, wird die Komponente "Online-
627 Check-in - glID & eGK-in-Frrnversorgung" genutzt.

628 Zum Produkttyp gehören auch die Komponenten für die abschließende Token-Erstellung
629 und der sichere Schlüsselspeicher. Zudem bietet der PoPP-Service eine VZD-Suche mit
630 einer Telematik-ID zur Ermittlung von Daten zu einer LEI an. Ferner gehören betriebliche
631 Komponenten für die Erfassung und Aufbereitung von Monitoring-Daten für die gematik-
632 Betriebsdatenerfassung (BDE) und ein Security Monitoring dazu.

633

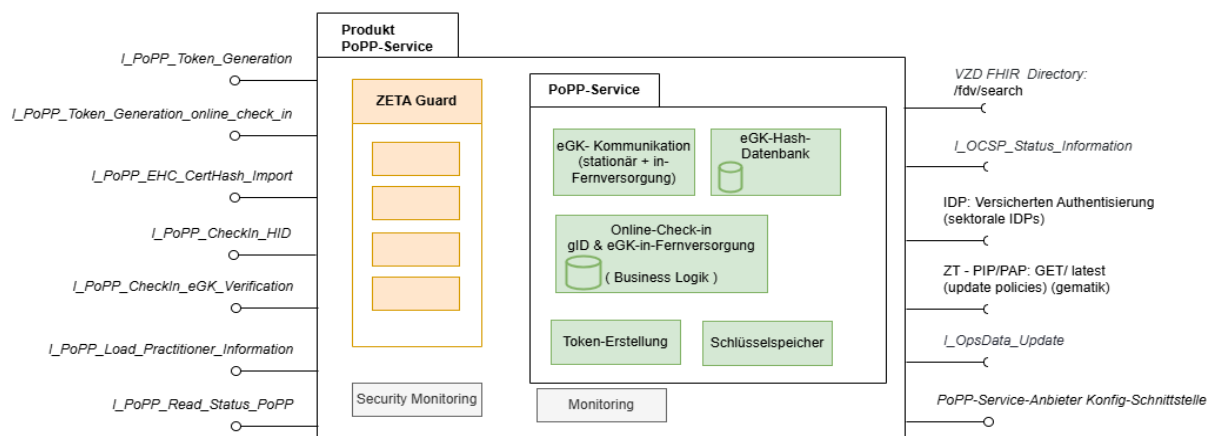


Abbildung 2: Produkttypzerlegung PoPP-Service

Der PoPP-Service stellt folgende Außenschnittstellen bereit:

- **I_PoPP_Token_Generation** wird vom Primärsystem einer LEI verwendet, um vom PoPP-Service einen PoPP-Token zu erlangen.
- **I_PoPP_CheckIn_HID** wird vom PoPP-Modul in der APP auf dem Gerät des Versicherten verwendet. Der PoPP-Service erstellt nach einer Authentifizierung des Versicherten mit seiner GesundheitsID einen PoPP-Token.
- **I_PoPP_CheckIn_eGK_Verification** wird vom PoPP-Modul in der APP auf dem Gerät des Versicherten verwendet. Der PoPP-Service erzeugt APDU-Kommandos an die eGK. Nach Prüfung der eGK erstellt der PoPP-Service einen PoPP-Token.
- **I_PoPP_Load_Practitioner_Information** wird vom PoPP-Modul in der APP auf dem Gerät des Versicherten verwendet. Der PoPP-Service führt mit einem übergebenen FHIR-VZD Search Request eine Anfrage am FHIR-VZD durch. Das Ergebnis der Suche wird vom PoPP-Service an das PoPP-Modul gesendet.
- **I_PoPP_Read_Status_PoPP** wird vom PoPP-Modul in der APP auf dem Gerät des Versicherten verwendet. Der PoPP-Service prüft, ob ein PoPP-Token der LEI erfolgreich zugestellt werden konnte und liefert den Status zur Zustellung an das PoPP-Modul.
- **I_PoPP_EHC_CertHash_Import** wird von den TSPs der Kassen aufgerufen und dient der Befüllung der CertHash-Datenbank, mittels derer das Mapping von CV-Zertifikaten zu X.509-Zertifikaten von eGKs erreicht wird. Dies dient der Unterstützung von Anwendungsfällen, bei denen der Versicherte die eGK mit einem kontaktlosen Kartenlesegerät der LEI verwendet.
- **I_PoPP_Token_Generation_online_check_in** wird vom Primärsystem einer LEI verwendet, um vom PoPP-Service einen PoPP-Token zu erlangen nachdem ein Online-Check-in durch einen Nutzer stattgefunden hat.

Der PoPP-Service benutzt die folgenden Schnittstellen:

- **ZETA PIP/PAP: GET/latest (update policies) (gematik)**
Wird vom ZETA Guard für die Versorgung mit den stets aktuellen Zugriffs-Policies und weiteren Konfigurationsdaten genutzt. Details siehe [gemSpec_ZETA].
- **I_OCSP_Status_Information:**
Wird vom PoPP-Service für die Statusabfragen für eGK, für SM(C)-B (ZETA Guard), für die eigene TI 1.0 PoPP APDU-Paket-Signatur-Identität und das eigene Internet-TLS-Server-Zertifikat verwendet.

- **I_OpsData_Update:**

Wird vom PoPP-Service für die Lieferung von Betriebsdaten verwendet.

- **VZD FHIR Directory: /fdv/search**

Wird vom PoPP-Service für die Ermittlung der Informationen zu einer LEI für eine bestimmte Telematik-ID oder bestimmte Suchkriterien zu einer LEI genutzt. Die Informationen werden zur Darstellung im PoPP-Modul für den Online-Check-in benötigt.

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

- **PoPP-Service-Anbieter Konfig-Schnittstelle**

Interne Schnittstellen, die vom PoPP-Service-Anbieter genutzt werden um den PoPP-Service zu konfigurieren.

4.1.6 [gemSpec_PoPP_Service#3.2]: Systemkontext

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

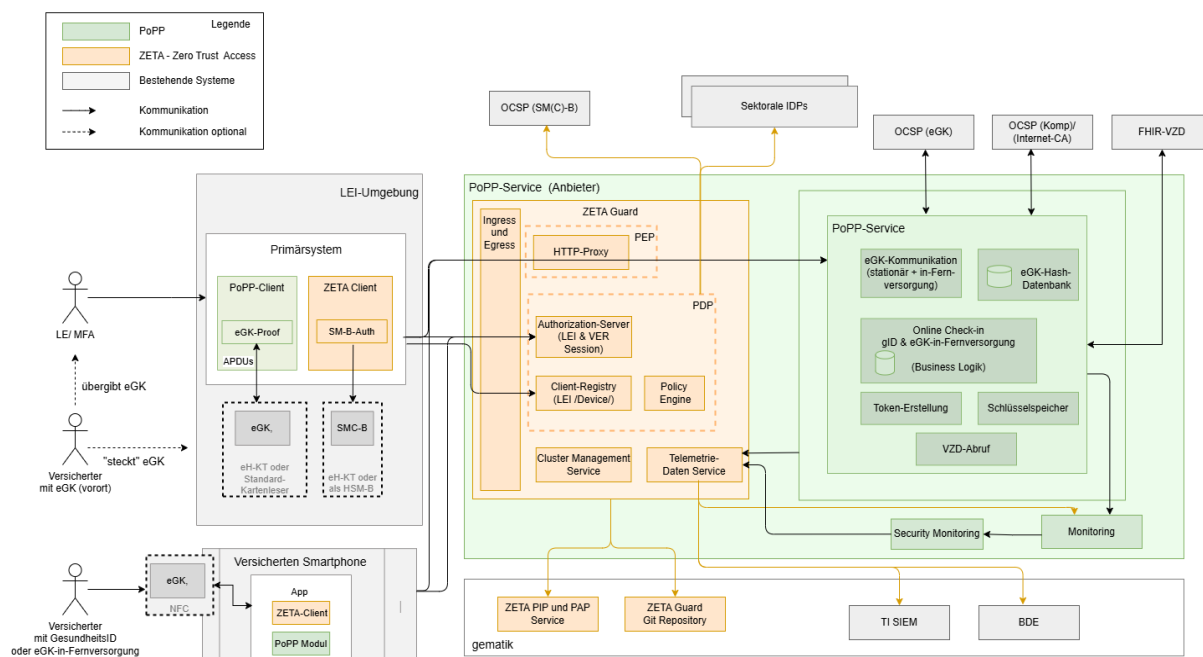


Abbildung 3: Systemkontext PoPP-Service

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

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

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

Tabelle 2: Kurzbeschreibung der Komponenten in der PoPP-Lösung

Komponente	Kurzbeschreibung	Anforderungen
PoPP-Service	Der PoPP-Service umfasst folgende Komponenten der PoPP-Lösung: <ul style="list-style-type: none"> • ZETA Guard • PoPP-Service. 	
ZETA Guard	Der Zero Trust Cluster ZETA Guard schützt die Kommunikation zwischen dem PoPP-Service und den PoPP-Clients der LEI sowie die Kommunikation der Versicherten zwischen PoPP-Modul und PoPP-Service. Die Authentifizierung der LEI erfolgt mittels SM(C)-B. Für die Kommunikation des PoPP-Modul mit dem PoPP-Service stellt ZETA Guard ein Client Access Token auf Basis der Geräte- und App-Attestation aus der ZETA Client Registrierung aus.	[gemSpec_ZETA]
<i>PoPP-Service</i>	Der PoPP-Service enthält die eigentliche Businesslogik des PoPP-Service für das Ausstellen von PoPP-Token an LEI-Systeme.	
eGK-Kartenkommunikation	In der Komponente eGK-Kartenkommunikation sind die Funktionalitäten für die Token-Erstellung in den Fällen enthalten, wenn ein Versicherter mittels seiner eGK beteiligt ist.	
eGK-Hash-DB	Die Komponente eGK-Hash-DB enthält die Datenbank und die steuernde Funktionalität für den Abgleich von anonymisierten eGK-Metadaten zur Unterstützung der kontaktlosen und der kontaktbehafteten Nutzung der	

	eGK.	
Online-Check-in (gID & eGK-in-Fernversorgung)	Die Komponente Online-Check-in enthält die steuernde Funktionalität, wenn ein Versicherter einen Online-Check-in durchführt.	
Token-Erstellung	Die Komponente Token-Erstellung enthält die Funktionalität zum Erstellen des PoPP-Token; hier werden die Daten von der LEI und dem Versicherten im PoPP-Token zusammengefügt.	
Schlüsselspeicher	Die Komponente Schlüsselspeicher enthält die Funktionalität zur sicheren Ablage der verwendeten Schlüssel und zur Speicherung von Daten.	
VZD-Abruf	Die Komponente VZD-Abruf enthält die Funktion zum Aufruf der FHIR-VZD-Schnittstelle zur Ermittlung von Informationen zu einer LEI. Das Suchergebnis wird vom PoPP-Service dem PoPP-Modul zugestellt.	
Monitoring	Die Komponente Monitoring sammelt Funktionalitäten für das Eigenmonitoring der verwendeten Systeme zur Überwachung und Analyse des Betriebszustands.	(bis zur Veröffentlichung in C_11939)
BDE-Lieferung	Die Komponente BDE-Lieferung fasst die Daten des PoPP-Service für die Betriebsdatenerfassung (BDE) der gematik zusammen und versendet sie.	(bis zur Veröffentlichung in C_11939)
Security Monitoring	Die Komponente Security Monitoring enthält Funktionen für das Sicherheits- und Event-Monitoring im PoPP-Service.	(bis zur Veröffentlichung in C_11939)
Primärsystem (PS)	Bestehende Primärsysteme werden für PoPP erweitert.	
ZETA Client	Der Trust Client (ZETA Client) im PS einer LEI ist der direkte Kommunikationspartner der ZETA Guard Komponente des PoPP-	[gemSpec_ZETA]

	Service.	
PoPP-Client	Der PoPP-Client ist der direkte Kommunikationspartner des PoPP-Service im PS einer LEI.	[gemILF_PoPP_Client]
App	App ist eine Krankenversicherungs-App oder Drittanbieter-App (Smartphone-App, Desktop-Anwendung, Browser-Anwendung), die von einem Versicherten mit GesundheitsID oder von einem Versicherten mit eGK online genutzt wird.	
ZETA Client	Der Trust Client (ZETA Client) in der App eines Versicherten ist der direkte Kommunikationspartner der ZETA Guard Komponente des PoPP-Service.	
PoPP-Modul	Das PoPP-Modul übernimmt beim Online-Check-in die Kommunikation (über die ZETA-Komponenten) mit dem PoPP-Service .	[gemSpec_PoPP_Modul]

4.1.7 [gemSpec_PoPP_Service#3.3]: Nachbarsysteme

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

- Sektoraler IDP:
verantwortlich für die Authentisierung eines Versicherten mit GesundheitsID,
- FHIR-VZD:
im Internet verfügbar zum Abruf von Informationen einer LEI,
- OCSP-Responder des TSP für SM(C)-B:
im Internet verfügbar für die OCSP-Prüfung von SM(C)-B durch den ZETA Guard,
- OCSP-Responder des TSP für eGK:
im Internet verfügbar für die OCSP-Prüfung von eGK durch den PoPP-Service,
- OCSP-Responder des TSP für Komponenten PKI:
im Internet verfügbar für die OCSP-Prüfung des TI 1.0 Komponenten-Zertifikats der PoPP-Service-Identität, verwendet bei der Signatur der Application Protocol Data Units (APDU) im eGK-Ablauf,
- OCSP-Responder Internet-CA:
im Internet verfügbar für die OCSP-Prüfung des TLS-Internet-Zertifikats des PoPP-Service (für die Client-Schnittstelle),
- Die gematik stellt folgende Dienste bereit:
PIP- und PAP-Service für Zero Trust, Git-Repository für die ZETA Guard Images,

Überwachung und Betriebsdatenerfassung: BDE und Telematikinfrasturktur Security Information and Event Management (TI-SIEM).

Die für PoPP erforderlichen OCSP-Responder (eGK, SM(C)-B, Komponenten-PKI, Internet-CA) sind jeweils kritisch für die erfolgreiche Prüfung von Zertifikaten. Sie müssen für die Token-Erstellung verfügbar sein.

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

- Fachanwendungen und FD im Internet, sowie Dienste und Komponenten, die noch in der TI 1.0 verortet sind, wie E-Rezept-FD, ePA < 3.x:
 - VSDM 2.0,
 - ePA für alle,
 - E-Rezept.
- TSP für eGK, die über I_PoPP_EHC_CertHash_Import zur Befüllung der eGK-Hash-Datenbank beitragen

Außerdem sind die App-Backend-Systeme nicht abgebildet.

4.1.8 [gemSpec_PoPP_Service#4]: Funktionale Anwendungsfälle des PoPP-Service

In Kapitel 4 wird der Einleitungstext aktualisiert: Neuer Text:

In diesem Kapitel werden die Anwendungsfälle beschrieben, die von der Proof of Patient Presence (PoPP)-Lösung abgedeckt werden. Die Anwendungsfälle zum Online-Check-in mit elektronischer Gesundheitskarte (eGK) oder GesundheitsID resultieren wie der Anwendungsfall eines Check-in mit eGK vorort in der LEI in der Ausstellung eines PoPP-Token für die LEI.

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

Darüber hinaus wird ein Use Case zur Befüllung der eGK-Hash-Datenbank durch Lieferanten definiert.

4.1.9 [gemSpec_PoPP_Service#4.1]: Übersicht der Systemanwendungsfälle für die Ausstellung des PoPP-Token

Der Inhalt von Kapitel 4.1 wird aktualisiert: Neuer Text:

Die Anwendungsfälle für die Ausstellung eines PoPP-Token lassen sich in drei Gruppen einteilen, die sich teils überlappen.

- Anwendungsfall AF_10402* zur Authentisierung einer LEI:
 - AF_10402* ist immer Voraussetzung für die Ausgabe eines PoPP-Token
- Anwendungsfälle, wie sich ein Versicherter für die Ausstellung des PoPP-Token authentisiert:
 - AF_10393* - PoPP-Token mittels eGK im eH-KT
 - AF_10387* - PoPP-Token mittels eGK im Standard-Kartenterminal
 - AF_10386* - Online-Check-in mit GesundheitsID

- AF_10389* - Online-Check-in mit eGK
- Anwendungsfälle, die beschreiben, wie die Ausgabe des PoPP-Token an das PS einer LEI erfolgt:
- AF_10393* - PoPP-Token mittels eGK im eH-KT
- AF_10387* - PoPP-Token mittels eGK im Standard-Kartenterminal
- AF_10390* - PoPP-Token Erstellung bei Online-Check-in

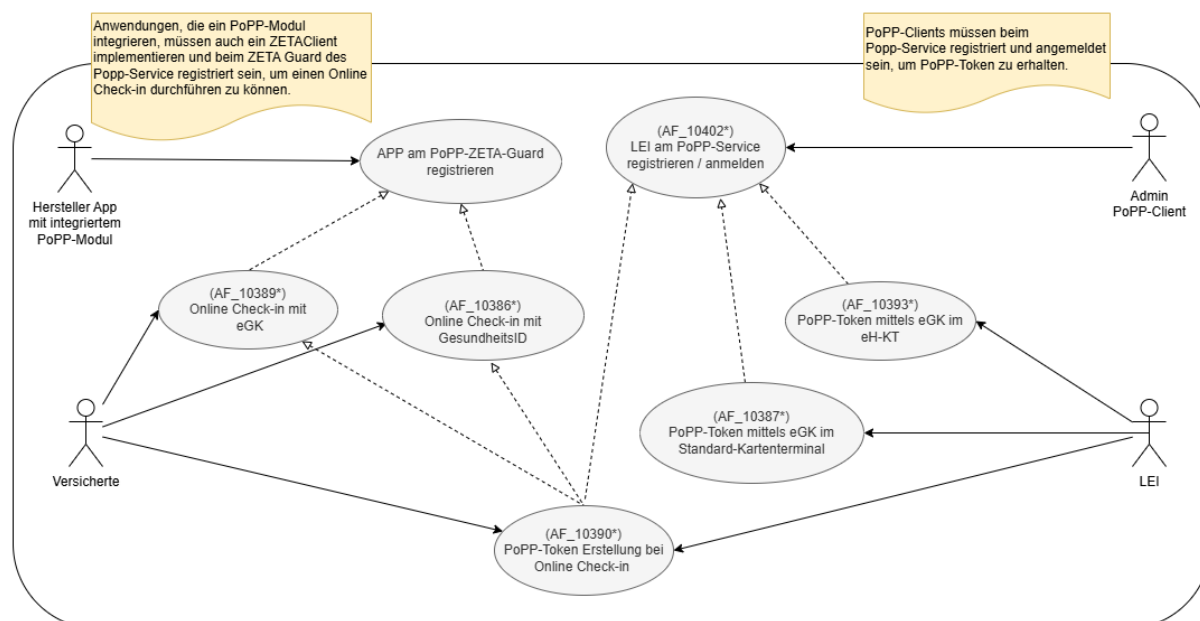


Abbildung 4: Anwendungsfälle zur Attestierung des Versorgungskontexts

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

Tabelle 3: Zuordnung der Anwendungsfälle zu den Use Cases

Anwendungsfall	Kurzbeschreibung	technische Anwendungsfälle
UC_PoPP_1a	PoPP-Token bei physischer Anwesenheit in der LEI / vor Ort-eGK	<ol style="list-style-type: none"> zunächst AF_10402*- LEI am PoPP-Service registrieren/ anmelden und dann entweder AF_10393* - PoPP-Token mittels eGK im eH-KT oder AF_10387* - PoPP-Token mittels eGK im Standard-Kartenleser
UC_PoPP_1b	PoPP-Token bei physischer Anwesenheit in der LEI/ vor Ort - GesundheitsID	<ol style="list-style-type: none"> zunächst AF_10402*- LEI am PoPP-Service registrieren/ anmelden und dann AF_10386* - Online-Check-in mit GesundheitsID, dann AF_10390* - PoPP-Token-Erstellung bei

		Online-Check-in
UC_PoPP_2a	PoPP-Token bei physischer Anwesenheit außerhalb der LEI/ Hausbesuch - eGK	<p>Identisch zu UC_PoPP_1a</p> <ol style="list-style-type: none"> 1. zunächst AF_10402*- LEI am PoPP-Service registrieren/ anmelden und dann 2. entweder AF_10393* - PoPP-Token mittels eGK im eH-KT 3. oder AF_10387* - PoPP-Token mittels eGK im Standard-Kartenleser
UC_PoPP_2b	PoPP-Token bei physischer Anwesenheit außerhalb der LEI/ Hausbesuch - GesundheitsID	<p>Identisch zu UC_PoPP_1b</p> <ol style="list-style-type: none"> 1. zunächst AF_10402*- LEI am PoPP-Service registrieren/ anmelden und dann 2. AF_10386* - Online-Check-in mit GesundheitsID, dann 3. AF_10390* - PoPP-Token-Erstellung bei Online-Check-in
UC_PoPP_3a	PoPP-Token ohne physische Anwesenheit in der LEI / in Fernversorgung- GesundheitsID - Check-in mit Drittanbieter-App oder Browser-Anwendung	<ol style="list-style-type: none"> 1. zunächst AF_10402*- LEI am PoPP-Service registrieren/ anmelden und dann 2. AF_10386* - Online-Check-in mit GesundheitsID, dann 3. AF_10390* - PoPP-Token-Erstellung bei Online-Check-in
UC_PoPP_3b	PoPP-Token ohne physische Anwesenheit in der LEI/ in Fernversorgung - GesundheitsID - Check-in mit Krankenversicherungs-App	<p>Identisch zu UC_PoPP_3a,</p> <ol style="list-style-type: none"> 1. zunächst AF_10402*- LEI am PoPP-Service registrieren/ anmelden und dann 2. AF_10386* - Online-Check-in mit GesundheitsID, dann 3. AF_10390* - PoPP-Token-Erstellung bei Online-Check-in
UC_PoPP_3c	PoPP-Token ohne physische Anwesenheit in der LEI/ in Fernversorgung - eGK-in-Fernversorgung - Check-in mit Drittanbieter-App oder Browser-Anwendung	<ol style="list-style-type: none"> 1. zunächst AF_10402*- LEI am PoPP-Service registrieren/ anmelden und dann 2. AF_10389* - Online-Check-in mit eGK-in-Fernversorgung, dann 3. AF_10390* - PoPP-Token-Erstellung bei Online-Check-in
UC_PoPP_3d	PoPP-Token ohne physische Anwesenheit in der LEI/ in	Identisch zu UC_PoPP_3c

	Fernversorgung - eGK-in-Fernversorgung - Check-in mit Krankenversicherungs-App	<ol style="list-style-type: none"> 1. zunächst AF_10402*- LEI am PoPP-Service registrieren/ anmelden und dann 2. AF_10389* - Online-Check-in mit eGK-in-Fernversorgung, dann 3. AF_10390* - PoPP-Token-Erstellung bei Online-Check-in
--	--------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

4.1.10 Neues Kapitel 4.5: Online-Check-in und Ausgabe des PoPP-Token

Versicherte Personen (VER) haben die Möglichkeit, sich unabhängig vom Ort für eine Leistungserbringung anzumelden (Online-Check-in). Der Online-Check-in erfolgt dabei unter Verwendung einer Anwendung, die ein PoPP-Modul und ein ZETA Client integriert (siehe [gemSpec_PoPP_Modul]). Als Ergebnis einer Anfrage des PoPP-Moduls über den ZETA Client an den ZETA Guard des PoPP-Service wird die Ausstellung eines PoPP-Token für eine LEI im PoPP-Service initiiert.

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

Über das in eine App integrierte PoPP-Modul ist eine Auswahl der Telematik-ID einer LEI für den Online-Check-in möglich. Die Auswahl der LEI kann über das Auswerten des von der LEI präsentierten statischen QR-Codes, oder über alternative Wege erfolgen. Über den PoPP-Service erfolgt ein VZD-Abruf, um die Gültigkeit einer Telematik-ID zu prüfen und Information zur LEI zu ermitteln.

Nach erfolgreicher Authentisierung der VER mit GesundheitsID oder Authentifizierung der eGK-in-Fernversorgung wird vom PoPP-Service ein Datensatz zur Erstellung eines PoPP-Token erzeugt. Ist die betroffene LEI online (d.h. sie ist zu dem Zeitpunkt authentifiziert), so wird das PoPP-Token erstellt und der LEI zugestellt. Ist die LEI nicht online, so wird das PoPP-Token erstellt und zugestellt, sobald diese online ist. Spätestens nach einem festgelegten Zeitraum (72h) wird der aus dem Online-Check-in erstellte Datensatz vom PoPP-Service gelöscht.

Das PoPP-Modul kann den Status der PoPP-Token-Zustellung am PoPP-Service abfragen und im PoPP-Modul auf dem Gerät des Versicherten darstellen. Sollte der Check-in nicht erfolgreich gewesen sein, wird der Versicherte auch darüber informiert.

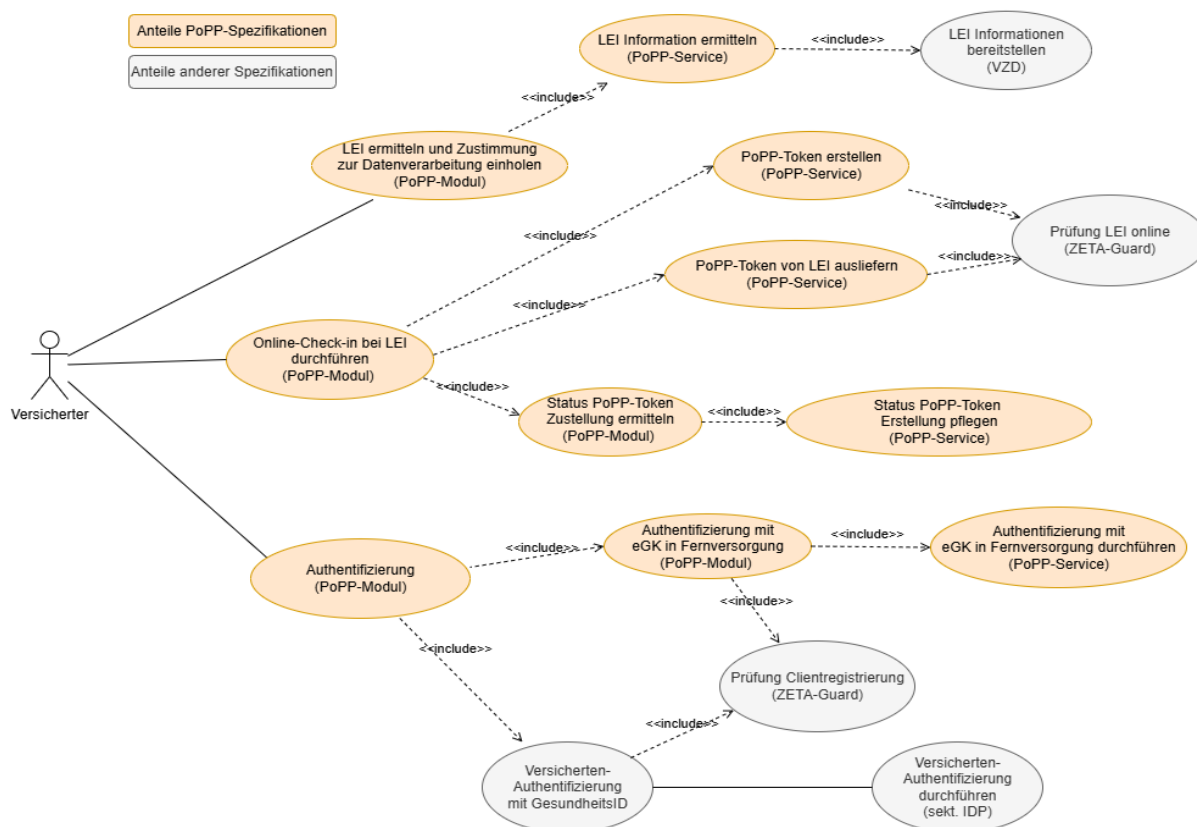


Abbildung 5: Use-Case-Übersicht Online-Check-in aus einer App mit integriertem PoPP-Modul

Tabelle 4: Kurzbeschreibung technische Use Cases Online-Check-in aus einer App mit integriertem PoPP-Modul

Anwendungsfall Online-Check-in App mit PoPP-Modul	Kurzbeschreibung
	Der Versicherte startet in der App mit PoPP-Modul (Krankenversicherungs-App, Drittanbieter-App) über einen Eintrag in der UX den "Online-Check-in" Prozess
"LEI ermitteln und Zustimmung zur Datenverarbeitung"	Der Online-Check-in startet mit der Auswahl einer LEI. Die Auswahl der LEI kann z.B. erfolgen durch: <ul style="list-style-type: none"> • Scannen eines QR-Code durch den Versicherten über eine Funktion in der App • Darstellen einer Auswahlliste in der App und Auswahl einer LEI durch den Versicherten • Visualisierung einer fest zugeordneten LEI durch die APP Der Versicherte muss zustimmen, dass seine KVNR an die LEI übermittelt werden darf.
"LEI Information"	Die Prüfung einer Telematik-ID und die Ermittlung der

ermitteln"	Informationen zu einer LEI (Name, Adresse, ..) wird durch den PoPP-Service über eine Abfrage am VZD durchgeführt.
"Check-in bei LEI durchführen"	<p>Der Check-in umfasst</p> <ul style="list-style-type: none"> • die Erstellung eines PoPP-Datensatzes im PoPP-Service mit allen Informationen zur PoPP-Token Erstellung • die Erstellung eines PoPP-Token im PoPP-Service, wenn die LEI online ist • die Übertragung des PoPP-Token an die LEI, wenn diese online ist • Die Auskunft zum Status der PoPP-Token Erstellung
"Authentifizierung"	<p>Die Authentifizierung kann erfolgen über:</p> <ul style="list-style-type: none"> • die Authentifizierung des Versicherten über seine GesundheitsID • die Authentifizierung einer eGK (eGK-in-Fernversorgung) <p>Die Authentifizierung mit GesundheitsID wird durch den GesundheitsID-Flow über die sektoralen IDPs abgebildet. Die Authentifizierung mit eGK-in-Fernversorgung wird durch Auslesen der eGK über PoPP-Modul und PoPP-Service abgebildet.</p> <p>Wobei "eGK-in-Fernversorgung" keine Authentifizierung der Person beinhaltet, welche die eGK benutzt. Ein auf dieser Basis ausgestelltes PoPP-Token wird nicht von allen Fachdiensten akzeptiert.</p>

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

4.1.11 Neues Kapitel 4.5.1: Auswahl einer LEI für den Online-Check-in

Die Abläufe zur Auswahl der Telematik-ID einer LEI, einer Suche im FHIR-VZD, der Aufbereitung der LEI-Informationen und die Erteilung der Einwilligung zur Datennutzung der Versicherten sind im Diagramm "Laufzeitsicht - Ermittlung Telematik-ID, VZD-Datenabruf mit Telematik-ID und Einwilligung in die Datenweitergabe" im Anhang von [gemSpec_PoPP_Modul] dargestellt.

Die Anmeldung am FHIR-VZD und die Suche erfolgt dann gemäß [gemSpec_VZD_FHIR] (AF_10403, Abbildung "Sequence diagram - Fachdienst Authentisierung und Suche").

Aus diesen Abläufen ergeben sich für den PoPP-Service folgende Anforderungen.

4.1.11.1 Zugang zum FHIR-VZD

A_28664 -PoPP-Service - Registrierung am FHIR-VZD

Der PoPP-Service MUSS sich als Client beim FHIR-VZD registrieren um Client-Credentials vom FHIR-VZD zu erhalten. Der PoPP-Service kann unter Angabe der Client-Credentials

Zugangstoken für den Zugang zum FHIR-VZD abrufen.
[<=]

A_28665 -PoPP-Service - Aktualisierung des FHIR-VZD Zugang

Der PoPP-Service MUSS mindestens alle 24h das Zugangstoken für den Zugang zum FHIR-VZD erneuern.[<=]

4.1.11.2 Ermittlung von Informationen zu einer LEI

A_28659 -PoPP-Service - Entgegennahme des HTTP-Request zur Ermittlung von Informationen zu einer LEI

Der PoPP-Service MUSS eine Schnittstelle gemäß [I_PoPP_Load_Practitioner_Information.yaml] zur Ermittlung von Informationen zu einer LEI implementieren. Der PoPP-Service MUSS den an der Schnittstelle übergebenen FHIR-VZD Search Request am FHIR-VZD ausführen und das Ergebnis als Antwort auf den Schnittstellenaufwurf zurückzugeben.[<=]

Hinweis: Wenn VZD-Daten im PoPP-Service gecached vorliegen, ist kein VZD-Abruf notwendig.

4.1.12 Neues Kapitel 4.5.2: Online-Check-in mit GesundheitsID

Ist die Telematik-ID der LEI ermittelt, bei welcher der Versicherte einen Check-in durchführen möchte und hat der Versicherte der Datennutzung durch die LEI zugestimmt, so kann er sich mit seiner GesundheitsID authentifizieren, um sich innerhalb oder außerhalb einer LEI (bspw. für eine Videosprechstunde) anzumelden. Als Ergebnis einer erfolgreichen Authentifizierung wird im PoPP-Service ein Datensatz zur Ausstellung eines PoPP-Token angelegt. Das PoPP-Token selbst wird erstellt, wenn die LEI sich beim PoPP-Service authentifiziert hat und das PoPP-Token abrufen.





Der Ablauf zum Online-Check-in mit GesundheitsID ist im Anhang Kapitel "[Detaillierter Ablauf der PoPP-Token Generierung durch Authentifizierung Versicherter über ihre GesundheitsID](#)" der [gemSpec_PoPP_Modul] dargestellt und beschrieben.

AF_10386-01 -Online-Check-in mit GesundheitsID

Attribute	Bemerkung
Beschreibung	<p>Ist die Telematik-ID der LEI, bei welcher der Online-Check-in erfolgen soll, ermittelt und hat der Versicherte der Datennutzung durch die LEI zugestimmt, bietet das PoPP-Modul dem Versicherten Möglichkeiten an, über welche die Versichertenidentität verifiziert werden kann. Eine Möglichkeit ist die Authentifizierung mit GesundheitsID. Bei diesem Verfahren wird der Versicherte durch den sektoralen IDP seiner Krankenversicherung authentifiziert. Dem Versicherten stehen dafür unterschiedliche Authentisierungsmittel zur Verfügung [gemSpec_IDP_Sek].</p> <p>Nach erfolgreicher Authentifizierung durch den sektoralen IDP stellt dieser ein ID-Token aus, welches u.a. die KVNR des authentifizierten Versicherten und die IK-Nummer seiner Krankenkasse enthält. Außerdem liefert das ID-Token Informationen über die Vertrauenswürdigkeit der Authentifizierung (Vertrauensniveau) und über das eingesetzte Authentisierungsmittel.</p>

	<p>Der für den PoPP-Service bereitgestellte ZETA Guard Authorization-Server erstellt daraufhin ein Access-Token und speichert die Informationen zur späteren Verwendung:</p> <ul style="list-style-type: none"> • KVNR des Versicherten • IK-Nummer der Krankenversicherung • Vertrauensniveau der durchgeführten Authentifizierung • Durchgeführte Authentisierungsmethode <p>ZETA Guard übermittelt das Access-Token an den ZETA Client worauf der eigentliche Request für den Check-in über den ZETA Guard HTTP-Proxy am PoPP-Service erfolgt. Der PoPP-Service erstellt in diesem Aufruf einen Datensatz mit</p> <ul style="list-style-type: none"> • KVNR des Versicherten - diese wurde im Request durch den ZETA Guard HTTP-Proxy als Headerattribut ergänzt • IK-Nummer der Krankenversicherung - diese wurde im Request durch den ZETA Guard HTTP-Proxy als Headerattribut ergänzt • Durchgeführte Authentisierungsmethode (amr) - diese wurde im Request durch den ZETA Guard HTTP-Proxy als Headerattribut ergänzt • Telematik-ID - Query-Parameter des HTTP-Request • WorkplaceID - Query-Parameter des HTTP-Request <p>und speichert diesen zusammen mit einem Zeitstempel einem eindeutigen Identifier und einer Statusinformation zur PoPP-Token-Erstellung.</p>
Vorbedingungen	<ol style="list-style-type: none"> 1. Der Versicherte hat einer Datennutzung (KVNR) durch die LEI zugestimmt. 2. Im PoPP-Modul wurde ein HTTP-Request an den PoPP-Service mit folgenden Query-Parametern formuliert: <ul style="list-style-type: none"> • Telematik-ID der LEI (mandatory) • WorkplaceID (optional) 3. Die Authentifizierung des Versicherten mit GesundheitsID wurde von den ZETA-Komponenten und den Komponenten des sektoralen IDP seiner Krankenversicherung erfolgreich durchgeführt. <ol style="list-style-type: none"> a. Zum Zeitpunkt der Authentisierung des Versicherten muss dieser einen Internetzugang haben. b. Der Versicherte verwendet eine App mit integrierten PoPP-Modul und ZETA Client. c. Gerät und App sind in der ZETA Guard Client-Registry registriert. d. Die GesundheitsID ist für den Versicherten im sektoralen IDP seiner Krankenversicherung eingerichtet und der Versicherte kann sich über sein Smartphone gegenüber dem sektoralen IDP seiner Krankenversicherung

	<p>authentifizieren.</p> <ol style="list-style-type: none"> 4. Der ZETA Guard HTTP-Proxy hat den PoPP-Service aufgerufen mit <ol style="list-style-type: none"> a. dem vom PoPP-Modul erstellten HTTP-Request b. dem vom ZETA-Guard ausgestellten Access-Token c. den zum Access-Token gespeicherten Informationen d. den Informationen zum aufrufenden Client
Ablauf	<ol style="list-style-type: none"> 1. Der PoPP-Service nimmt den HTTP-Request vom ZETA Guard HTTP-Proxy entgegen. 2. Der PoPP-Service extrahiert <ol style="list-style-type: none"> a. KVNR des Versicherten (mandatory) - aus dem Header des HTTP-Request b. IK-Nummer der Krankenversicherung (mandatory) - aus dem Header des HTTP-Request c. Authentisierungsmethode (mandatory) - aus dem Header des HTTP-Request d. Telematik-ID der LEI (mandatory) - aus dem HTTP-Request e. WorkplaceID der LEI (optional) - aus dem HTTP-Request 3. Der PoPP-Service erzeugt und speichert einen PoPP-Datensatz mit extrahierten Daten (KVNR, IK-Nummer, Telematik-ID, WorkplaceID), der erzeugten proofMethod=" und einem aktuellen Zeitstempel. 4. Der PoPP-Service erstellt und speichert einen Nachrichten-Datensatz zum Status der PoPP-Token-Erstellung mit <ol style="list-style-type: none"> a. <i>id</i>- eindeutiger Identifier zur Identifikation der Nachricht bei asynchronem Abruf b. <i>status</i> - repräsentiert den Status der PoPP-Token-Erstellung (<i>success</i>, <i>pending</i>, <i>cancelled</i>) c. <i>message</i>- enthält Detailinformationen zu Status 5. Der PoPP-Service speichert den Identifier (<i>id</i>) der Nachricht zum Status der PoPP-Token-Erstellung zusätzlich im PoPP-Datensatz. 6. Der PoPP-Service hat den eingegangenen Request mit der Statusnachricht zur PoPP-Token-Erstellung beantwortet
Nachbedingung	<ul style="list-style-type: none"> • Erfolgsfall <ul style="list-style-type: none"> • Der PoPP-Service hat einen PoPP-Datensatz mit allen Daten angelegt, die zur Erstellung eines PoPP-Token notwendig sind. • Der PoPP-Service hat dem ZETA Guard HTTP-Proxy mit HTTP-200 und der Statusnachricht zur PoPP-Token-Erstellung geantwortet.

	<ul style="list-style-type: none"> Es ist ein Fehler aufgetreten <ul style="list-style-type: none"> Der PoPP-Service hat dem ZETA Guard HTTP-Proxy mit einem Fehler Code und der Statusnachricht zur PoPP-Token-Erstellung geantwortet
Akzeptanzkriterien	<ul style="list-style-type: none">  ML-184424 - AF_10386 - Bereitsstellung einer Schnittstelle für die Erzeugung eines PoPP-Token nach Authentifizierung mit GesundheitsID <ul style="list-style-type: none"> Der PoPP-Service hat den HTTP-Request vom ZETA Guard HTTP-Proxy entgegengenommen, die Daten zum Anlegen des PoPP-Datensatzes extrahiert und die Vollständigkeit der übergebenen Daten geprüft. Der PoPP-Service hat geantwortet mit einem <ul style="list-style-type: none"> HTTP-200 (OK), wenn die Bearbeitung des Requests fehlerfrei abgearbeitet werden konnte HTTP-400 (Bad Request) , wenn nicht alle mandatory Attribute extrahiert werden konnten HTTP-500 in allen anderen Fehlerfall  ML-184338 - AF_10386 - Erstellung und Speicherung PoPP-Datensatz GesundheitsID <ul style="list-style-type: none"> Der PoPP-Service hat einen PoPP-Datensatz angelegt bestehend aus <ul style="list-style-type: none"> KVNR des Versicherten IK-Nummer der Krankenversicherung Telematik-ID der LEI WorkplaceID der LEI proofMethod="" Zeitstempel Identifizier der Nachricht zur PoPP-Token-Generierung  ML-184339 - AF_10386_10389 - Erstellung und Speicherung eines Nachrichten-Datensatz <ul style="list-style-type: none"> Der PoPP-Service hat einen Nachrichten-Datensatz mit der Nachricht zum Status der PoPP-Token-Generierung angelegt, bestehend aus <ul style="list-style-type: none"> Identifizier der Nachricht Status der PoPP-Token-Generierung Message zum PoPP-Token Status  ML-185491 - AF_10386 - Response an ZETA Guard HTTP-Proxy zum eingegangenen Request <ul style="list-style-type: none"> Der PoPP-Service hat den eingegangenen Request mit der Statusnachricht zur PoPP-Token-Erstellung beantwortet <ul style="list-style-type: none"> "success", wenn der PoPP-Datensatz angelegt werden

	<p>konnte und das PoPP-Token erstellt und der LEI zugestellt wurde</p> <ul style="list-style-type: none"> • "pending", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token noch nicht erstellt und der LEI zugestellt wurde • "cancelled", wenn ein Fehler aufgetreten ist. • message mit Informationen im Fehlerfall
Fehlerfälle	<ul style="list-style-type: none"> • Die Prüfung Gerät und/oder App durch ZETA ist fehlgeschlagen • Die Prüfung der übergeben Parameter zum Anlegen des PoPP-Datensatzes ist fehlgeschlagen • Die Authentifizierung des Nutzers über ZETA und sektoralen IDP ist fehlgeschlagen • Das Anlegen des Datensatzes im PoPP-Service ist fehlgeschlagen
Alternativen	Alternativ zur GesundheitsID kann der Versicherte den Versorgungskontext mit seiner eGK (eGK-in-Fernversorgung) attestieren.

857
858 **[<=]**

859
860 **ML-184424 -AF_10386 - Bereitsstellung einer Schnittstelle für die Erzeugung**
861 **eines PoPP-Token nach Authentifizierung mit GesundheitsID**

862 Der PoPP-Service implementiert eine Schnittstelle gemäß [I_PoPP_CheckIn_HID.yaml] für
863 die Entgegennahme eines HTTP-Requests zur Erzeugung eines PoPP-Token, nachdem der
864 Versicherte über seine GesundheitsID authentifiziert wurde.

865 **[<=]**

866
867 **ML-184338 -AF_10386 - Erstellung und Speicherung PoPP-Datensatz**
868 **GesundheitsID**

869 Der PoPP-Service hat einen PoPP-Datensatz angelegt bestehend aus

Datensatz Element	Kurzbeschreibung	Wert / Format
	KVNR des Versicherten, ermittelt aus dem HTTP-Header des HTTP-Request	string Wertebereich:
	IK-Nummer der Krankenversicherung, ermittelt aus dem HTTP-Header des HTTP-	string Wertebereich:

	Request	
	Telematik-ID der LEI, ermittelt aus dem Query-Parameter aus dem HTTP-Request	Gültige Telematik-ID
workplaceId	WorkplaceID der LEI, ermittelt aus dem Query-Parameter aus dem HTTP-Request	string Wertebereich: <code>^[^\\:.*? "<>]{64}\$</code>
proofMethod	Fester Wert "" repräsentiert die Authentifizierung des Versicherten mit GesundheitsID	string zulässiger Werte: "
timestamp	Zeitstempel, Zeitpunkt Anlage des Datensatzes	number, Alle time Werte in Sekunden seit 1970, [RFC7519#section-2] https://tools.ietf.org/html/rfc7519#section-2
messageId	Identifiziert des Nachrichten Datensatz zur PoPP-Token Generierung	UUID

871 [`<=`]

872 ML-184339 -AF_10386_10389 - Erstellung und Speicherung eines Nachrichten-Datensatz

873 Der PoPP-Service hat einen Nachrichten-Datensatz angelegt bestehend aus

Datensatz Element	Kurzbeschreibung	Wert / Format
id	Eindeutiger Identifier der Nachricht für die Zuordnung zu einem PoPP-Datensatz	UUID
status	Repräsentiert den Status der PoPP-token Erstellung <ul style="list-style-type: none"> "success" - PoPP-Token wurde erstellt und erfolgreich zugestellt "pending" - PoPP-Datensatz ist angelegt, PoPP-Token wurde noch nicht erstellt "cancelled" - Erstellung des 	string Wertebereich: ["success", "pending", "cancelled"]

	PoPP-Token wurde abgebrochen	
message	Detailinformationen zum Status	String (max. 128 Zeichen) Wertebereich: ^[ÄÖÜäöüßw\ \-\.&\+*V] {1,128}\$

[<=]

ML-185491 -AF_10386 - Response an ZETA Guard HTTP-Proxy zum eingegangenen Request

Der PoPP-Service hat auf den eingegangenen Request gemäß [I_PoPP_CheckIn_HID.yaml] eine Response an den ZETA Guard HTTP-Proxy zurück gesendet.

Dabei MUSS die Response im Responsebody die Statusnachricht zur PoPP-Token Erzeugung enthalten:

- "success", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token erstellt und der LEI zugestellt wurde
- "pending", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token noch nicht erstellt und der LEI zugestellt wurde
- "cancelled", wenn ein Fehler aufgetreten ist.

Im Fehlerfall muss die "message" der Statusnachricht Informationen zum aufgetretenen Fehler enthalten.**[<=]**

4.1.13 Neues Kapitel 4.5.3: Online-Check-in mit eGK-in- Fernversorgung

Ein Versicherter mit eGK befindet sich außerhalb einer LEI (bspw. für eine Videosprechstunde) und nutzt die eGK mit seinem Smartphone, um sich anzumelden.

Als Ergebnis einer erfolgreichen Authentifizierung der eGK wird im PoPP-Service ein Datensatz zur Ausstellung eines PoPP-Token angelegt. Das PoPP-Token selbst wird erstellt, wenn die LEI sich beim PoPP-Service authentifiziert hat und das PoPP-Token abrufen.






Der Ablauf zum Online-Check-in mit eGK ist im Gang Kapitel "[Detaillierter Ablauf der PoPP-Token Generierung durch Authentifizierung der eGK über den PoPP-Service](#)" der [gemSpec_PoPP_Modul] dargestellt und beschrieben.

AF_10389-01 -Online-Check-in mit eGK

Attribute	Bemerkung
Beschreibung	Ist die Telematik-ID der LEI, bei welcher der Online-Check-in erfolgen soll, ermittelt und hat der Versicherte der Datennutzung durch die LEI zugestimmt, bietet das PoPP-Modul dem Versicherten Möglichkeiten an, über welche die Versichertenidentität verifiziert werden kann. Eine Möglichkeit ist die Authentifizierung der eGK ohne Eingabe der PIN (eGK-in-Fernversorgung). Bei diesem Verfahren wird eine eGK direkt über

	<p>eine Kartenschnittstelle über PoPP-Modul und ZETA-Komponenten durch den PoPP-Service ausgelesen. Der PoPP-Service prüft die eGK auf Echtheit und Gültigkeit. Ist die Prüfung erfolgreich erstellt der PoPP-Service einen Datensatz mit</p> <ul style="list-style-type: none"> • KVNR des Versicherten - aus dem X.509-Zertifikat der eGK • IK-Nummer der Krankenversicherung - aus dem X.509-Zertifikat der eGK • Telematik-ID - Query-Parameter des HTTP-Request • WorkplaceID - Query-Parameter des HTTP-Request <p>und speichert diesen zusammen mit einem Zeitstempel einem eindeutigen Identifier und einer Statusinformation zur PoPP-Token Erstellung.</p>
Vorbedingung	<ol style="list-style-type: none"> 1. Der Versicherte hat einer Datennutzung (KVNR) durch die LEI zugestimmt. 2. Im PoPP-Modul wurde ein HTTP-Request zum Auslesen der eGK an den PoPP-Service mit folgenden Query-Parametern formuliert: <ul style="list-style-type: none"> • Telematik-ID der LEI (mandatory) • WorkplaceID (optional) 3. Zum Zeitpunkt der Authentisierung des Versicherten muss dieser einen Internetzugang haben. 4. Der Versicherte verwendet eine App mit integrierten PoPP-Modul und ZETA Client. 5. Gerät und App sind in der ZETA Guard Client-Registry registriert. Zeta Guard hat ein Client Access-Token erstellt. 6. Das Endgerät des Versicherten verfügt über ein Lesegerät für kontaktlose oder kontaktbehaftete Kartenkommunikation. 7. Der ZETA Guard HTTP-Proxy hat den PoPP-Service aufgerufen mit <ol style="list-style-type: none"> a. dem vom PoPP-Modul erstellten HTTP-Request b. dem vom ZETA-Guard ausgestellten Client Access-Token
Ablauf	<ol style="list-style-type: none"> 1. Der PoPP-Service nimmt den HTTP-Request vom ZETA Guard HTTP-Proxy entgegen. 2. Der PoPP-Service liest die Daten der eGK in einem rekursiven Ablauf <ol style="list-style-type: none"> a. Der PoPP-Service erstellt APDU-Commands b. Der PoPP-Service überträgt die APDU-Commands (via ZETA-Komponenten) an das PoPP-Modul c. Das PoPP-Modul ruft die eGK mit den APDU-Commands auf d. Das PoPP-Modul nimmt die Antworten der eGK auf die

	<p>APDU-Commands entgegen</p> <ul style="list-style-type: none"> e. Das PoPP-Modul sendet die Antworten über die ZETA-Komponenten an den PoPP-Service f. Der PoPP-Service wertet die Antworten der eGK aus und erstellt ein weiteres APDU-Command oder verlässt die Rekursion, wenn die eGK Informationen vollständig vorliegen. <ol style="list-style-type: none"> 3. Der PoPP-Service prüft CV-Zertifikat und X.509-Zertifikat der eGK. 4. Der PoPP-Service erzeugt Hashwerte der Zertifikate und ruft die Hash-DB auf. 5. Der PoPP-Service extrahiert <ul style="list-style-type: none"> a. KVN-Nummer des Versicherten - aus dem X.509-Zertifikat der eGK b. IK-Nummer der Krankenversicherung - aus dem X.509-Zertifikat der eGK c. Telematik-ID der LEI - aus dem HTTP-Request d. WorkplaceID der LEI (optional) - aus dem HTTP-Request 6. Der PoPP-Service erzeugt und speichert einen PoPP-Datensatz mit extrahierten Daten (KVN-Nummer, IK-Nummer, Telematik-ID, WorkplaceID), der erzeugten proofMethod=" und dem einem aktuellen Zeitstempel. 7. Der PoPP-Service erstellt und speichert einen Nachrichten-Datensatz zum Status der PoPP-Token Erstellung mit <ul style="list-style-type: none"> a. <i>id</i>- eindeutiger Identifier zur Identifikation der Nachricht bei asynchronem Abruf b. <i>status</i> - repräsentiert den Status der PoPP-Token Erstellung (<i>success</i>, <i>pending</i>, <i>cancelled</i>) c. <i>message</i>- enthält Detailinformationen zu Status 8. Der PoPP-Service speichert den Identifier (<i>id</i>) der Nachricht zum Status der PoPP-Token Erstellung im PoPP-Datensatz 9. Der PoPP-Service hat den eingegangenen Request mit der Statusnachricht zur PoPP-Token Erstellung beantwortet
Nachbedingung	<ul style="list-style-type: none"> • Erfolgsfall <ul style="list-style-type: none"> • Der PoPP-Service hat einen PoPP-Datensatz mit allen Daten angelegt, die zur Erstellung eines PoPP-Token notwendig sind. • Der PoPP-Service hat dem ZETA Guard HTTP-Proxy mit HTTP-200 und der Statusnachricht zur PoPP-Token Erstellung geantwortet. • Es ist ein Fehler aufgetreten <ul style="list-style-type: none"> • Der PoPP-Service hat dem ZETA Guard HTTP-Proxy mit einem Fehler Code und der Statusnachricht zur PoPP-Token Erstellung geantwortet

Akzeptanzkriterien	<ul style="list-style-type: none">•  ML-184423 - AF_10389 - Bereitstellung einer Schnittstelle für das Auslesen und Prüfen der eGK und die Erzeugung eines PoPP-Token nach eGK-Prüfung<ul style="list-style-type: none">• Der PoPP-Service hat den HTTP-Request vom ZETA Guard HTTP-Proxy entgegengenommen und die Zugriffsberechtigung geprüft.• Der PoPP-Service hat geantwortet mit einem<ul style="list-style-type: none">• HTTP-200 (OK), wenn die Bearbeitung des Requests fehlerfrei abgearbeitet werden konnte• HTTP-403 (Forbidden), wenn die Prüfung der eGK fehlgeschlagen und demnach der Zugriff nicht berechtigt ist• HTTP-400 (Bad Request) , wenn nicht alle mandatory Attribute extrahiert werden konnten• HTTP-500 in allen anderen Fehlerfällen• •  ML-184342 - AF_10389 - Der PoPP-Service hat die Daten der eGK ausgelesen und geprüft<ul style="list-style-type: none">• Der PoPP-Service hat die Daten der eGK ausgelesen und geprüft•  ML-184341 - AF_10389 - Erstellung und Speicherung PoPP-Datensatz eGK-in-Fernversorgung<ul style="list-style-type: none">• Der PoPP-Service hat einen PoPP-Datensatz angelegt bestehend aus<ul style="list-style-type: none">• KVNR des Versicherten• IK-Nummer der Krankenversicherung• Telematik-ID der LEI• WorkplacelD der LEI• proofMethod=• Zeitstempel• Identifier des Nachrichten-Datensatz zur PoPP-Token Generierung•  ML-184339 - AF_10386_10389 - Erstellung und Speicherung eines Nachrichten-Datensatz<ul style="list-style-type: none">• Der PoPP-Service hat einen Nachrichten-Datensatz mit der Nachricht zum Status der PoPP-Token Generierung angelegt bestehend aus<ul style="list-style-type: none">• Identifier der Nachricht• Status der PoPP-Token Generierung• Message zum PoPP-Token Status•  ML-185492 - AF_10389 - Response an ZETA Guard HTTP-
--------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>Proxy zum eingegangenen Request</p> <ul style="list-style-type: none"> • Der PoPP-Service hat den eingegangenen Request mit einem APDU-Kommande beantwortet oder • Der PoPP-Service hat den eingegangenen Request mit der Statusnachricht zur PoPP-Token Erstellung beantwortet <ul style="list-style-type: none"> • "success", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token erstellt und der LEI zugestellt wurde • "pending", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token noch nicht erstellt und der LEI zugestellt wurde • "cancelled", wenn ein Fehler aufgetreten ist. • message mit Informationen im Fehlerfall
Fehlerfälle	<ul style="list-style-type: none"> • Die Prüfung Gerät und/oder App durch ZETA ist fehlgeschlagen • Die Prüfung der übergeben Parameter zum Anlegen des PoPP-Datensatzes ist fehlgeschlagen • Die Authentifizierung der eGK führt zu einem Fehler (Response der eGK auf APDU-Commands, Zertifikatsprüfung, Abgleich mit Hash-DB) • Das Anlegen des Datensatzes im PoPP-Service ist fehlgeschlagen
Alternativen	Alternativ zur eGK kann der Versicherte den Versorgungskontext mit seiner GesundheitsID attestieren.

[<=]

ML-184423 -AF_10389 - Bereitstellung einer Schnittstelle für das Auslesen und Prüfen der eGK und die Erzeugung eines PoPP-Token nach eGK-Prüfung

Der PoPP-Service implementiert eine Schnittstelle gemäß [I_PoPP_CheckIn_eGK_Verification.yaml] für das Auslesen und Prüfen der eGK und die Erzeugung eines PoPP-Token nach eGK-Prüfung.[<=]

ML-184342 -AF_10389 - Der PoPP-Service hat die Daten der eGK ausgelesen und geprüft

Der PoPP-Service hat die Daten der eGK gemäß Schnittstellenbeschreibung [I_PoPP_CheckIn_eGK_Verification.yaml] ausgelesen und

- die Gültigkeit des CV-Zertifikats geprüft,
- die Gültigkeit des X.509-Zertifikats geprüft,
- eine Überprüfung der Zusammengehörigkeit der Zertifikate gegen die Hash-DB durchgeführt.

[<=]

ML-184341 -AF_10389 - Erstellung und Speicherung PoPP-Datensatz eGK-in-Fernversorgung

Der PoPP-Service hat einen PoPP-Datensatz angelegt bestehend aus

Datensatz Element	Kurzbeschreibung	Wert / Format
	KVNR des Versicherten, ermittelt aus dem HTTP-Header des HTTP-Request	string Wertebereich:
	IK-Nummer der Krankenversicherung, ermittelt aus dem HTTP-Header des HTTP-Request	string Wertebereich:
	Telematik-ID der LEI, ermittelt aus dem Query-Parameter aus dem HTTP-Request	Gültige Telematik-ID
workplaceId	WorkplaceID der LEI, ermittelt aus dem Query-Parameter aus dem HTTP-Request	string Wertebereich: <code>^[^\\:.*? "<>]{64}\$</code>
proofMethod	Fester Wert "" repräsentiert die Authentifizierung der eGK des Versicherten in Fernversorgung	string zulässiger Werte: "
timestamp	Zeitstempel, Zeitpunkt Anlage des Datensatzes	number, Alle time Werte in Sekunden seit 1970, [RFC7519#section-2] https://tools.ietf.org/html/rfc7519#section-2
messageId	Identifiziert des Nachrichten-Datensatz zum Status der PoPP-Token Erzeugung	UUID

[<=]

ML-185492 -AF_10389 - Response an ZETA Guard HTTP-Proxy zum eingegangenen Request

Der PoPP-Service hat auf den eingegangenen Request gemäß [I_PoPP_CheckIn_eGK_Verification.yaml] eine Response an den ZETA Guard HTTP-Proxy zurück gesendet.

Dabei MUSS die Response folgende Informationen im Responsebody enthalten:

- solange das Auslesen der eGK nicht abgeschlossen ist

- das nächste APDU-Kommando an die eGK
- nach Abschluss des Auslesens der eGK
- die Statusnachricht zur PoPP-Token Erzeugung. Dabei MUSS die Statusnachricht wie folgt gefüllt sein:
 - "success", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token erstellt und der LEI zugestellt wurde
 - "pending", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token noch nicht erstellt und der LEI zugestellt wurde
 - "cancelled", wenn ein Fehler aufgetreten ist
- Im Fehlerfall muss die "message" der Statusnachricht Informationen zum aufgetretenen Fehler enthalten.

[<=]

A_28676 -PoPP-Service - eGK-in-Fernversorgung - PoPP-Token nur nach erfolgreicher eGK-Prüfung

Der PoPP-Service MUSS durchsetzen, dass im Falle eGK-in-Fernversorgung das Anlegen eines PoPP-Datensatzes ausschließlich nach erfolgreichem Durchlaufen der eGK-Prüfung entsprechend gemSpec_PoPP_Service#6.1.1 stattfindet. [<=]

4.1.14 Neues Kapitel 4.5.4: PoPP-Token bei Online-Check-in

Offener Punkt: OP-PoPP-1




Der konkrete Ablauf zur Benachrichtigung der LEI über ZETA Guard - ZETA Client, dass PoPP-Token abgerufen werden können, ist noch offen. Die Spezifikation von ZETA Guard hierzu ist noch nicht abgeschlossen.

Der Anwendungsfall beschreibt den Ablauf und die Aktivitäten des PoPP-Service bei Erstellen eines PoPP-Token für einen Online-Check-in.

AF_10390-01 -PoPP-Token Erstellung bei Online-Check-in

Attribute	Bemerkung
Beschreibung	<p>Nach einem durch den Versicherten initiierten Online-Check-in ist ein Datensatz für die Erstellung eines PoPP-Token angelegt. Wenn sich die LEI gegenüber dem ZETA-Guard (mit SMC-B) authentifiziert hat, wird aus diesem Datensatz ein PoPP-Token erzeugt.</p> <p>Über ZETA-Guard erhält das Primärsystem eine Nachricht, dass PoPP-Token abrufbar im PoPP-Service liegen. Dieses PoPP-Token kann vom Primärsystem der LEI abgerufen werden. Der Abruf von PoPP-Token kann auch ohne vorherige Benachrichtigung manuell oder automatisiert durch das Primärsystem der LEI erfolgen.</p> <p>Der PoPP-Service generiert eine Nachricht, welche den Status der PoPP-Token Erstellung an das PoPP-Modul mit folgendem Inhalt enthält.</p>

	<ul style="list-style-type: none"> • <i>id</i> = eindeutiger Identifier der Nachricht • <i>status</i> <ul style="list-style-type: none"> • <i>success</i> - PoPP-Token wurde erzeugt und der LEI zugestellt • <i>pending</i> - PoPP-Token wurde erzeugt und noch nicht zugestellt, da die LEI nicht online ist. Die Zustellung wird weiter versucht. • <i>cancelled</i> - Prozess wurde aufgrund eines Fehlers oder wegen Überschreitung der maximalen Wartezeit (z.B. 72h) abgebrochen • <i>message</i> = Detailinformationen zum jeweiligen Status <p>Der PoPP-Service übermittelt die Nachricht im synchronen Ablauf als Ergebnis des jeweiligen HTTP-Request (AF_10386*, AF_10389*) oder asynchron auf Anfrage des PoPP-Modul (AF_10425).</p>
Vorbedingung	<ol style="list-style-type: none"> 1. Der Datensatz für die PoPP-Token Generierung ist im PoPP-Service erstellt und gespeichert. 2. Die LEI ist als PoPP-Client am ZETA-Guard registriert 3. Die LEI hat sich gegenüber dem ZETA-Guard (mit SMC-B) authentifiziert
Ablauf	<p>Information an LEI</p> <ol style="list-style-type: none"> 1. Der PoPP-Service erstellt eine Nachricht für die LEI zum Abholen des PoPP-Token 2. Der PoPP-Service sendet die Nachricht an ZETA-Guard <p><i>Hinweis: Wie die Nachricht erstellt (1) und über ZETA-Guard versendet wird (2) ist im Moment noch ein offener Punkt (OP-PoPP-1)</i></p> <p>Abholen des PoPP-Token durch Primärsystem der LE</p> <ol style="list-style-type: none"> 1. Das Primärsystem sendet einen HTTP-Request (über die ZETA-Komponenten) an den PoPP-Service. ZETA prüft in diesem Ablauf die Vertrauenswürdigkeit des anfragenden Primärsystems und validiert dessen Identität (SMC-B). 2. Der PoPP-Service sucht alle Datensätze zur Telematik-ID der LEI, <ol style="list-style-type: none"> a. zu denen noch kein PoPP-Token erstellt und ausgegeben wurde. b. die innerhalb der letzten 72 Stunden erstellt wurden. 3. Der PoPP-Service signiert das PoPP-Token. 4. Der PoPP-Service antwortet auf den HTTP-Request mit dem PoPP-Token. 5. Der PoPP-Service ändert den Status der Nachricht zum PoPP-Datensatz auf <i>status = success</i>

	<ol style="list-style-type: none"> 6. Der PoPP-Service stellt dem PoPP-Modul über die ZETA-Komponenten die Nachricht zu <ol style="list-style-type: none"> a. im synchronen Fall als Antwort auf den jeweiligen HTTP-Request (AF_10386*, AF_10389*) b. asynchron auf Anfrage des PoPP-Modul an den PoPP-Service.
Nachbedingung	<ol style="list-style-type: none"> 1. Der PoPP-Service löscht alle Datensätze <ol style="list-style-type: none"> a. zu denen ein PoPP-Token erstellt und ausgeliefert und zu denen eine Nachricht an das PoPP-Modul erfolgreich zugestellt wurde. b. die älter als 72h sind. Der Status der Nachricht zu diesem Datensatz wird auf <i>status = cancelled</i> und <i>message</i> auf <i>message = "Der Check-in wurde nach 72h erfolglos abgebrochen"</i> 2. Der PoPP-Service löscht alle Nachrichten-Datensätze mit <i>status = cancelled</i> oder <i>status = success</i> sobald sie zugestellt wurden, spätestens jedoch nach 5 Tagen.
Akzeptanzkriterien	<ul style="list-style-type: none"> •  ML-184426 - AF_10390 - PoPP-Token erstellt und übermittelt oder Abbruch des Check-in <ul style="list-style-type: none"> • Der PoPP-Service hat PoPP-Token erstellt und an das Primärsystem übermittelt oder den Zustellungsversuch nach 72h abgebrochen •  ML-184425 - AF_10390 - Aktualisierung der Nachricht für den Versicherten <ul style="list-style-type: none"> • Der PoPP-Service hat eine Nachricht zum Status der PoPP-Token Erstellung aktualisiert. •  ML-184427 - AF_10390 - Löschung zugestellter oder abgelaufener Nachrichten <ul style="list-style-type: none"> • Der PoPP-Service hat zugestellte Nachrichten-Datensätze gelöscht. • Der PoPP-Service hat abgelaufene Nachrichten-Datensätze gelöscht.
Fehlerfälle	<ul style="list-style-type: none"> • Die Zustellung der Benachrichtigung ist fehlgeschlagen • Das PoPP-Token wurde nicht innerhalb von 72h abgeholt
Alternativen	keine

959 [\leq]

960
961 **ML-184426 -AF_10390 - PoPP-Token erstellt und übermittelt oder Abbruch des**
962 **Check-in**

963 Der PoPP-Service hat gemäß [I_PoPP-Token_Generation.yaml] ein PoPP-Token erstellt.
964 Das PoPP-Token wurde dem Primärsystem zugestellt. Konnte innerhalb von 72h nach

Erstellung des PoPP-Datensatz kein PoPP-Token dem Primärsystem zugestellt werden, hat der PoPP-Service den Check-in Prozess abgebrochen.

【<=】

ML-184425 -AF_10390 - Aktualisierung der Nachricht für den Versicherten

Der PoPP-Service hat den Nachrichtendatensatz aktualisiert

- status = success, wenn dem Primärsystem ein PoPP-Token zugestellt werden konnte.
- status = cancelled, wenn der Check-in Prozess nach 72h abgebrochen wurde.

【<=】

ML-184427 -AF_10390 - Löschung zugestellter oder abgelaufener Nachrichten

Der PoPP-Service hat alle Nachrichtendatensätze gelöscht, die

- den status "success" oder "canceld" haben und erfolgreich dem PoPP-Modul zugestellt werden konnten.
- die älter als 5 Tage sind.


【<=】


4.1.15 Neues Kapitel 4.5.5: Status der PoPP-Token-Erstellung nach Online-Check-in ermitteln

Der Anwendungsfall beschreibt den Ablauf, wenn ein PoPP-Modul nach dem Prozess des Online-Check-in den Status zur PoPP-Token-Erstellung beim PoPP-Service abfragen möchte. Dieser Anwendungsfall wird durchlaufen, wenn im Prozess des Online-Check-in zwar der PoPP-Datensatz angelegt werden konnte, der PoPP-Token jedoch noch nicht erstellt und an die LEI ausgeliefert wurde ("LEI offline").

AF_10425 -Status der PoPP-Token-Erstellung nach Online-Check-in ermitteln

Attribute	Bemerkung
Beschreibung	<p>Im Prozess des Online-Check-in wurde zwar der PoPP-Datensatz mit allen für die Erstellung des PoPP-Token relevanten Informationen erstellt, das PoPP-Token selbst konnte jedoch noch nicht ausgestellt werden. Dies ist der Fall, wenn die LEI, für die das PoPP-Token erstellt werden soll, zum Zeitpunkt des Online-Check-in nicht am ZETA Guard authentifiziert ist (z.B. weil die LEI nicht online ist).</p> <p>In diesem Fall erhält das PoPP-Modul Ergebnis des Online-Check-in eine Statusnachricht mit dem Status "pending".</p> <p>Kann zu einem späteren Zeitpunkt die LEI authentifiziert werden und ruft die PoPP-Token am PoPP-Service ab, so wird beim Abruf des PoPP-Token der Status der Nachricht auf "success" gesetzt.</p> <p>Kann die LEI auch zu einem späteren Zeitpunkt nicht authentifiziert werden (z.B. innerhalb von 72h), so wird der PoPP-Datensatz gelöscht und der Status der Nachricht auf "cancelled" geändert.</p> <p>Das PoPP-Modul kann nun zu späteren Zeitpunkten nach dem Online-Check-in beim PoPP-Service den aktuellen Status der PoPP-Token Generierung anfragen und den Versicherten</p>

	informieren, ob sein Online-Check-in bei der LEI erfolgreich war oder abgebrochen wurde.
Vorbedingung	<ol style="list-style-type: none"> 1. Der Online-Check-in wurde erfolgreich durchlaufen, ein PoPP-Datensatz wurde angelegt 2. Zum PoPP-Datensatz wurde ein Nachrichten-Datensatz angelegt, der Status im Nachrichten-Datensatz ist "pending" 3. Im PoPP-Modul wurde ein HTTP-Request zur Abfrage des Status zur PoPP-Token Erstellung an den PoPP-Service mit dem Identifier (id) des Nachrichten-Datensatzes Query-Parametern formuliert. 4. Zum Zeitpunkt der Authentisierung des Versicherten muss dieser einen Internetzugang haben. 5. Der Versicherte verwendet eine App mit integrierten PoPP-Modul und ZETA Client. 6. Gerät und App sind in der ZETA Guard Client-Registry registriert. Zeta Guard hat ein Client Access-Token erstellt. 7. Der ZETA Guard HTTP-Proxy hat den PoPP-Service aufgerufen mit <ol style="list-style-type: none"> a. dem vom PoPP-Modul erstellten HTTP-Request b. dem vom ZETA-Guard ausgestellten Client Access-Token
Ablauf	<ol style="list-style-type: none"> 1. Der PoPP-Service nimmt den HTTP-Request vom ZETA Guard HTTP-Proxy entgegen. 2. Der PoPP-Service prüft die Berechtigung der Anfrage (Client Access-Token) 3. Der PoPP-Service extrahiert den Identifier (id) des Nachrichten-Datensatzes aus dem HTTP-Request 4. Der PoPP-Service ermittelt die aktuellen Informationen zur PoPP-Token Erzeugung aus dem Nachrichten-Datensatz 5. Der PoPP-Service hat den eingegangenen Request mit der Statusnachricht zur PoPP-Token Erstellung beantwortet
Nachbedingung	<ul style="list-style-type: none"> • Erfolgsfall <ul style="list-style-type: none"> • Der PoPP-Service hat dem ZETA Guard HTTP-Proxy mit HTTP-200 und der Statusnachricht zur PoPP-Token Erstellung geantwortet • Es ist ein Fehler aufgetreten <ul style="list-style-type: none"> • Der PoPP-Service hat dem ZETA Guard HTTP-Proxy mit einem Fehler Code und der Statusnachricht zur PoPP-Token Erstellung geantwortet
Akzeptanzkriterien	 ML-185508 - AF_10425 - Bereitsstellung einer Schnittstelle zur Abfrage des aktuellen Status der PoPP-Token-Erstellung nach

	<p>einem Online-Check-in</p> <ul style="list-style-type: none"> • Der PoPP-Service hat den HTTP-Request vom ZETA Guard HTTP-Proxy entgegengenommen und die Zugriffsberechtigung geprüft • Der PoPP-Service hat geantwortet mit einem <ul style="list-style-type: none"> • HTTP-200 (OK), wenn die Bearbeitung des Requests fehlerfrei abgearbeitet werden konnte • HTTP-403 (Forbidden), wenn der Zugriff nicht berechtigt ist • HTTP-400 (Bad Request) , wenn nicht alle mandatory Attribute extrahiert werden konnten • HTTP-500 in allen anderen Fehlerfall <p> ML-185507 - AF_10425 - Response an ZETA Guard HTTP-Proxy zum eingegangenen Request</p> <p>Der PoPP-Service hat den eingegangenen Request mit der Statusnachricht zur PoPP-Token Erstellung beantwortet</p> <ul style="list-style-type: none"> • "success", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token erstellt und der LEI zugestellt wurde • "pending", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token noch nicht erstellt und der LEI zugestellt wurde • "cancelled", wenn ein Fehler aufgetreten ist. • message mit Informationen im Fehlerfall
Alternativen	Keine

[<=]

ML-185508 -AF_10425 - Bereitsstellung einer Schnittstelle zur Abfrage des aktuellen Status der PoPP-Token-Erstellung nach einem Online-Check-in

Der PoPP-Service implementiert eine Schnittstelle gemäß [I_PoPP_Read_Status_PoPP.yaml] für die Entgegennahme eines HTTP-Requests zur Abfrage des aktuellen Status der PoPP-Token-Erstellung nach einem Online-Check-in.

[<=]

ML-185507 -AF_10425 - Response an ZETA Guard HTTP-Proxy zum eingegangenen Request

Der PoPP-Service hat auf den eingegangenen Request gemäß [I_PoPP_Read_Status_PoPP.yaml] eine Response an den ZETA Guard HTTP-Proxy zurück gesendet. Dabei MUSS die Response im Responsebody die Statusnachricht zur PoPP-Token-Erzeugung enthalten:

- "success", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token erstellt und der LEI zugestellt wurde
- "pending", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token noch nicht erstellt und der LEI zugestellt wurde

- "cancelled", wenn ein Fehler aufgetreten ist. Im Fehlerfall muss die "message" der Statusnachricht Informationen zum aufgetretenen Fehler enthalten

[<=]

4.1.16 Änderungen [gemSpec_PoPP_Service#5.3.4] PoPP-Service Signaturen

Der Hinweis unter [A_26495 - PoPP-Service - PoPP-Token-Signatur-Identität](#) entfällt.

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

4.1.17 Änderungen [gemSpec_PoPP_Service#5.4]: ZETA Guard im PoPP-Service

Folgender Text wird dem Kapitel 5.4 am Ende zugefügt:

Für die Umsetzung des Online-Check-in für Versicherte kommen weitere Komponenten der Zero-Trust-Architektur (ZETA) zum Einsatz.

ZETA Client

Beim Online-Check-in ist der ZETA Client ist die Zero Trust-Komponente für ein FdV, das zusammen mit dem PoPP-Modul in einer App integriert sein muss. Der ZETA Client überträgt bei der Initialisierung der Anwendung die Geräte- und App-Informationen an das ZETA Guard backend.

Im laufenden Prozess kapselt den ZETA Client die gesamte Kommunikation zwischen der Anwendung auf dem Gerät des Versicherten und den Komponenten im Backend, u.a. auch zwischen PoPP-Modul und PoPP-Service.

Der ZETA Client steuert die Client-Authentisierung am ZETA Guard Authorization-Server und unterstützt die Nutzerauthentifizierung mit GesundheitID und eGK-in-Fernversorgung.

ZETA Guard Authorization-Server

Bevor eine Anwendung über ein registrierten ZETA Client auf einen Fachdienst zugreifen kann, führt ZETA Guard Authorization-Server die Client-Authentifizierung durch und stellt dem ZETA Client der Anwendung bei erfolgreicher Authentifizierung ein Access-Token aus.

Wird von der Anwendung darüber hinaus die Authentifizierung des Nutzers über die GesundheitsID angefragt, so stößt der ZETA Guard Authorization-Server den Authentifizierungsprozess beim jeweiligen Sektoren IDP an. Der ZETA Guard Authorization-Server nimmt bei erfolgreicher Authentifizierung das ID-Token entgegen und verarbeitet dessen Inhalt.

ZETA Guard HTTP-Proxy

Fachliche Requests aus den Anwendungen werden vom ZETA Client der Anwendung an den ZETA Guard HTTP-Proxy geschickt. Nach Prüfung des Clients gegen die ZETA Guard Client-Registry und ggf. Durchführung von Prüfregeln durch die ZETA Guard Policy-

Engine reichert der ZETA Guard HTTP-Proxy den Request mit Header-Informationen an und sendet den Request dann an den eigentlichen Empfänger. Das Ergebnis des Requests wird dem ZETA Client der aufrufenden Anwendung zugestellt.

Die detaillierten Abläufe für Online-Check-in sind in [gemSpec_PoPP_Modul] Kapitel "Anhang B - Ablaufbeschreibungen" dargestellt.

4.1.18 Änderungen [gemSpec_PoPP_Service#5.6]: Federation Entity Statement

Text in Kapitel 5.6 wird aktualisiert:

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

Das Entity Statement beaufkundet allgemeine Informationen wie:

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

und Metadaten Informationen zur Konfiguration als:

1. OAuth Protected Resource (oauth_resource),
2. Teilnehmer der TI-Föderation (federation_entity).

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

Die folgenden Anforderungen werden an die Inhalte des Entity Statement gestellt:

Anforderungen aus dem Kapitel 5.6 werden aktualisiert:

Alt:

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

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

Tabelle 5: Attribute im well-known document des PoPP-Service

Name	Werte	Beispiel / Beschreibung
iss	URL	URL des PoPP-Service, Identifizier in der TI- Föderation
sub	URL	URL des PoPP-Service, (=iss)
jwks	JWKS Objekt	Federation Entity Key für die Signatur des Entity Statement [OpenID

		Federation 1.0]
iat	Alle time Werte in Sekunden seit 1970, [RFC7519#section-2]	1645484401 für 2022-02-22 00:00:01
exp	Alle time Werte in Sekunden seit 1970, [RFC7519#section-2]	1645570800 für Ablauf 24h nach iat
authority_hints	[string]	iss Bezeichnung des Federation Master (PU: "https://app.federationmaster.de")

1085 **[<=]**

1086 **Neu:**

1087 **A_27294-01 -PoPP-Service - Bereitstellung .well-known für PoPP-Service**

1088 Der Anbieter eines PoPP-Service MUSS sicherstellen, dass unter <Identifizier-URL>/ .well-
1089 known/openid-federation ein Entity Statement gemäß [\[OpenID Federation 1.0\]](#)
1090 veröffentlicht ist. Das Entity Statement MUSS über das Internet erreichbar sein. Das
1091 Metadaten-Statement MUSS mindestens die folgenden Werte enthalten:

1092 **Tabelle 6: Attribute im well-known document des PoPP-Service**

Name	Werte / Wertebereich
iss	string, URL nach [RFC1738]
sub	string, URL nach [RFC1738]
iat	number, Alle time-Werte in Sekunden seit 1970, [RFC7519#section-2]
exp	number, Alle time-Werte in Sekunden seit 1970, [RFC7519#section-2]
jwtks	Set von JWK [RFC7517] zulässige Werte sind, gemäß [OpenID Federation "Claims that MUST or MAY Appear in both Entity Configurations and Subordinate Statements"] - jwtks, nur die öffentlichen Schlüssel zu Schlüsseln, mit den das Entity Statement signiert ist.
authority_hints*	[string] zulässige Werte gemäß [OpenID Federation "Claims that MUST or MAY Appear in Entity Configurations but Not in Subordinate Statements"] - authority_hints

metadata	string, zulässiger Wert: "oauth_resource"
----------	----------------------------------------------

* Der claimauthority_hints wird nur benötigt, wenn des Entity Statement des PoPP-Service in der TI-Föderation registriert wird.
[<=]

Alt:

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

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

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

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

[<=]

Neu:

A_27295-01 -PoPP-Service - Bereitstellung oauth_resource im .well-known für den PoPP-Service

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

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

Name	Werte
organization_name	string (gemäß [OpenID-Federation "Informational Metadata Extensions"] - organization_name) Wertebereich: ^[ÄÖÜäöüß\w\ \-\.\&\+*V]{1,128}\$
display_name	string (gemäß [OpenID-Federation "Informational Metadata Extensions"] - display_name) Wertebereich: ^[ÄÖÜäöüß\w\ \-\.\&\+*V]{1,128}\$
keywords	[JSON] (gemäß [OpenID-Federation "Informational Metadata Extensions"] - keywords)

	erforderlicher Wert: "product_type_version" : "<von der gematik zugelassene Produkttyp-Version>"
contacts	[JSON] (gemäß [OpenID-Federation "Informational Metadata Extensions"] - contacts) erforderlicher Wert: "support" : "<e-mail Adresse für Supportanfragen>"
signed_jwks_uri	string, URL nach [RFC1738]

[<=]

Folgende Afo entfällt gemäß aktueller [OpenID Federation 1.0]:

**A 27296 - PoPP-Service - Bereitstellung .well-known als Teilnehmer der TI-
Föderation**

4.1.19 [gemSpec_PoPP_Service#6.1]- eGK-Handling

4.1.19.1 Ergänzung in Kap. 6.1.1 - eGK-Handling, Einführung

**Im einleitenden Text zur Use Case Übersicht wird der Punkt 2 für die Stufe 2
ergänzt:**

.....

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

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

4.2 Änderungen in [gemILF_PoPP_Client]

Dieses Kapitel ist nicht normativ für den Hersteller und Anbieter PoPP-Service. Es dient zur Information und Orientierung über die gesamte Lösung. Folgende Themen werden in [gemILF_PoPP_Client] ergänzt:

1. Festlegungen zum Generieren von QR Codes.
2. Festlegungen für den "Asynchronen Empfang" von PoPP-Token
3. Festlegungen für die Verarbeitung von WorkplaceID und SessionID

Im [gemILF_PoPP_Client] auf gitHub werden die Use-Cases für den Online Check-in erweitert. Zusätzlich zu den Anforderungen, die in Form von Festlegungen definiert sind, werden detaillierte Erläuterungen und Hinweise zur technischen und organisatorischen Umsetzung ergänzt. Diese Inhalte werden außerhalb dieser Feature-Spezifikation erstellt und unterliegen nicht dem Freigabeprozess für gematik-Dokumente.

4.2.1 Erzeugung und Verwendung statischer QR-Codes für PoPP

A_28532 -PS - PoPP - Inhalt QR-Code

Das PS MUSS einen QR-Code für eine LEI erzeugen, in dem die Telematik-ID der LEI enthalten ist. Der QR-Code enthält optional die WorkplaceID des Arbeitsplatzes, für den der QR-Code verwendet wird.【<=】

A_28533 -PS - PoPP - Format QR-Code

Das PS MUSS diesen QR-Code gemäß ISO/IEC 18004:2024 kodieren.【<=】

A_28534 -PS - PoPP - QR-Code Inhalt Payload

Das PS MUSS den Payload des QR-Codes als JSON Struktur gemäß [RFC8259] im UTF-8 Format nach [RFC3629] ausstellen. Der Inhalt des Payload MUSS gemäß Tabelle [Tab_PoPP_Modul_Payload_stat_QRCode] in [gemSpec_PoPP_Modul] erzeugt werden.【<=】

A_28535 -PS - PoPP - QR-Code Scan-Hinweis

Das PS MUSS neben dem QR-Code einen Hinweis in Klartext aufdrucken, der den Nutzer auffordert, den QR-Code nicht direkt mit der Kamera-App seines Endgerätes, sondern mittels der App, die für den Check-in-Vorgang verwendet wird, zu scannen.
Beispiel: "Wir bitten Sie diesen QR-Code immer mit Ihrer Check-in-App zu scannen."【<=】

Um eine sichere Verwendung der QR-Codes im Versorgungsalltag zu gewährleisten, gelten die folgenden Empfehlungen der gematik für die Gestaltung der präsentierten QR-Codes:

- Neben dem QR-Code den Namen der LEI-Name, die (verkürzte) Telematik-ID und (optional) die Arbeitsplatzbezeichnung im Klartext aufdrucken.
- Es ist ratsam, regelmäßige Überprüfungen des ausgestellten QR-Codes auf Unversehrtheit vorzunehmen.

A_28732 -PS - PoPP - Hinweis zu QR-Codes an Nutzer

Das PS MUSS dem Nutzer beim Erzeugen eines QR-Codes den Hinweis anzeigen, dass QR-Codes innerhalb der LEI in einem gut durch LEI-Personal frequentiert Bereich - idealerweise am Tresen - aufgestellt bzw. angebracht werden soll sowie regelmäßig auf Korrektheit geprüft werden soll.【<=】

4.2.2 WorkplacelD

**Für den ILF wird einleitend noch weiterer erklärendes Text zur WorkplacelD
zugefügt, bzw. Hinweis auf den Konzept Teil dieser Feature-Spezifikation.**

Die optional vom PoPP-Service übertragene WorkplacelD dient beispielweise der Zuordnung eines PoPP-Token zu einem Arbeitsplatz in der LEI, an dem ein Online Check-in von einem Versicherten durchgeführt wurde.

Die WorkplacelD kann durch die LEI auch wie eine SessionID verwendet werden, um das letztendlich erzeugte PoPP-Token dann dem richtigen Versicherten zuordnen zu können. Dies kann bspw. im Online-Apotheken-Anwendungsfall notwendig werden. Die LEI muss dabei beachten, dass die in A_28629* beschriebenen Einschränkungen für die WorkplacelD entsprechend genauso gelten.

A_28537 -PS - PoPP - WorkplacelD entnehmen

Das PS MUSS die optionale WorkplacelD aus der HTTP-Nachricht, mit der der PoPP-Token vom PoPP-Service zum PoPP-Client übertragen wird, entnehmen, wenn sie vom PoPP-Service gesetzt wurde und in der HTTP-Nachricht enthalten ist. [≤]

4.2.3 Verbindung zum PoPP-Service herstellen und PoPP-Token abrufen

Ein Primärsystem einer LEI kann PoPP-Token am PoPP-Service abfragen, indem die Schnittstelle `I_PoPP_Token_Generation_online_check_in` [`I_PoPP_Token_Generation_online_check_in.yaml`] aufgerufen wird. Im Zuge des Online-Check-in eines Nutzers wird ein PoPP-Datensatz im PoPP-Service angelegt und maximal 72h vorgehalten. Fragt ein Primärsystem einer LEI während dieser Zeit die Schnittstelle nach PoPP-Token an, wird aus dem hinterlegten PoPP-Datensatz ein PoPP-Token erstellt und der LEI an der Schnittstelle zurück geliefert.

Das Primärsystem einer LEI kann den Abruf z.B. manuell über Interaktion mit Nutzern des Primärsystems oder automatisiert durch regelmäßiges Abfragen bzw. nach Benachrichtigung durch den PoPP-Service durchführen.

Offener Punkt: OP-PoPP-1

Der konkrete Ablauf zur Benachrichtigung der LEI über ZETA Guard - ZETA Client, dass Popp-Token abgerufen werden können, ist noch offen. Die Spezifikation von ZETA Guard hierzu ist noch nicht abgeschlossen.

4.3 Änderungen in [gemSpec_PoPP_Modul]

Die Anforderung an ein PoPP-Modul sind in [gemSpec_PoPP_Modul] spezifiziert.

4.4 Änderungen in [api-popp]

Die Änderungen für die Stufe 2 von PoPP wirken sich auch auf die externen Schnittstellen des PoPP Service [api-popp] aus. Dort werden Änderungen vorgenommen:

Schnittstelle	Status	Änderungsbeschreibung
[I_PoPP_Token_Generation.yaml]	unverändert	ohne Änderung
[I_PoPP_Token_Generation_online_check_in.yaml]	neu	Neues Interface zur Übertragung von PoPP-Token an den PoPP-Client, wenn die Übertragung durch den PoPP-Service nach einem Online Check-in initiiert wird. (SessionID, WorkplacelD, ...)
[I_PoPP_CheckIn_HID.yaml]	neu	Schnittstelle für Authentifizierung mit GesundheitsID und Anlegen eines PoPP-Datensatzes
[I_PoPP_CheckIn_eGK_Verification.yaml]	neu	Schnittstelle für Authentifizierung einer eGK und Anlegen eines PoPP-Datensatzes
[I_PoPP_load_Practitioner_Information.yaml]	neu	Schnittstelle für das Laden der Informationen zu einer LEI vom FHIR-VZD
[I_PoPP_Read_Status_PoPP.yaml]	neu	Schnittstelle für das Lesen des aktuellen Status zur PoPP-Token Erstellung und Auslieferung
[I_PoPP_CheckIn_AuthorizationServer.yaml]	entfällt	Die Aufgabe wird nun von ZETA Guard übernommen
[I_PoPP_CheckIn_ResourceServer.yaml]	entfällt	Die Aufgabe wird nun von ZETA Guard übernommen

1223

1224 4.5 Änderungen in [gemSpec_ZETA]

1225 Für die Authentisierung von Versicherten wird in PoPP Stufe 2 der ZETA Guard verwendet.
 1226 Die Festlegungen dazu stehen in [gemSpec_ZETA] Stufe 2.

4.6 Änderungen in [gemSpec_IDP_Sek]

Bedingt durch die Rahmenbedingung für Apps der Krankenversicherungen, dass PoPP-Modul, ZETA Client und Authenticator-Modul der sektoralen IDPs in einer APP integriert sein müssen, ergeben sich Anforderungen an den sektoralen IDP und an dessen Authenticator-Modul.

Zum einen werden für die technische Abbildung eines PoPP-Modul Aufrufs aus einer Drittanbieter-App die Plattformmechanismen von Android und iOS (deeplink / universal link) verwendet. Hier kann allerdings bereits nachgenutzt werden, dass für eine Authentifizierung des Versicherten mit GesundheitsID die entsprechende Konfiguration schon eingerichtet ist. Allerdings ist es notwendig, die Mechanismen der eigentlichen Authentifizierung vom Mechanismus des Aufrufs des PoPP-Moduls zu trennen. Zu diesem Zweck soll eine weiterer Endpunkt im Entity Statement der sektoralen IDPs aufgenommen werden.

Zum anderen muss auch berücksichtigt werden, dass die App mit dem Authenticator-Modul auch ohne vollständige Einrichtung der GesundheitsID (d.h. ohne Durchlauf des Identifikationsprozesses) auf dem Gerät des Versicherten installierbar ist, da das Ausstellen eines PoPP-Token für einige Anwendungsfälle ausschließlich auf das Auslesen der Zertifikate der eGK erfolgen kann. Eine GesundheitsID ist hier nicht erforderlich und ggf. für den Versicherten auch nicht eingerichtet.

Änderungen in Kapitel "4.1 Entity Statement des sektoralen IDP"

Änderungen in

A_22643* - Entity Statement des sektoralen IDP

Tabelle "Attribute des Metadatenblocks openid_provider im well-known-Dokument des sektoralen IDP"

neu:

Name	Werte
ti_feature_popp_endpoint	string, URL nach [RFC1738]

Änderungen in Kapitel "5.1 Funktionsmerkmale Authenticator-Modul"

A_28689 -Authenticator-Modul: Installation mit Gerätebindung ohne Ident-Prozess

Die Installation der App mit integriertem Authenticator-Modul des sektoralen IDP MUSS auf dem Gerät des Versicherten auch ohne Durchlaufen des Identifikationsprozess möglich sein. Es muss auch für diesen Fall eine Gerätebindung eingerichtet werden.【<=】

Hinweis: Für diesen Fall ist die GesundheitsID nicht für ein Vertrauensniveau "gematik-ehealth-loa-high" eingerichtet. Die Anhebung des Vertrauensniveaus kann durch nachfolgende Identifikation ("step-up-authentication") durchgeführt werden.

Das Authenticator-Modul des sektoralen IDP MUSS eine Schnittstelle anbieten, über die ermittelt werden kann, ob die GesundheitsID vollständig (d.h. inklusive Durchlauf des Identifikations-Prozesses) oder unvollständig (ohne Identifikation des Nutzers) erfolgt ist.

Offener Punkt: OP-PoPP-2
Es soll eine Testtreiberschnittstelle analog zum Vorgehen beim ePA-FdV für PoPP-Modul/ App-mit-Popp-Modul entwickelt werden. Die entsprechenden Festlegungen werden in [gemKPT Test] an geeigneter Stelle aufgenommen werden..

Die Tabelle Tab_Test_033 Mindestumfang der Interoperabilitätsprüfung wird durch die Folgende ersetzt:

[illegible]

4.8 Änderungen in [gemSpec_Perf]

Änderungen am PoPP Service spezifischen Kapitel 3.X.

Umbenennung der UseCases in PoPP.UC_<01-...07>

Die folgenden neuen Anwendungsfälle werden ebenfalls in gemSpec_Perf hinzugefügt:

Table 1 Tab_gemSpec_Perf_PoPP_Service: Performancerelevante UseCases

UseCase	Fachdienstoperation	Beschreibung
<...>		
PoPP.UC_03	I_PoPP_CheckIn_HID	<p>In diesem Aufruf erstellt und speichert der PoPP-Service einen PoPP-Datensatz und einen Nachrichten-Datensatz. Der Nachrichten-Datensatz wird vom PoPP-Service in der Response an das PoPP-Modul gesendet.</p> <p>Der UC Beginnt mit dem Aufruf CheckInGIDRequest im PoPP RessourceServer und endet mit dem Absenden der Response StatusPoppTokenGeneration.</p>
PoPP.UC_04	I_PoPP_CheckIn_eGK_Verification	<p>In diesem Aufruf erzeugt der PoPP-Service APDU-Kommandos für die eGK und liefert diese in der Response an das PoPP-Modul und führt folgende Schritte aus</p> <ul style="list-style-type: none"> • Prüfung CV-Zertifikat und X.509 Zertifikat • Erzeugung von Hashwerten zu den Zertifikaten • Aufruf Hash-DB zur Prüfung des Hashwert-Paares • Auslesen des X.509 Zertifikats • Erstellen und Speichern eines PoPP-Datensatzes und Nachrichten-Datensatzes <p>Der Nachrichten-Datensatz wird vom PoPP-Service in der Response an das PoPP-Modul gesendet.</p> <p>Der UC Beginnt mit dem Erhalt des Aufrufs ReadEgkRequest im PoPP-Dienst und endet mit dem</p>

		Absenden der Response zum PoPP-Modul. Die Kommunikation über das PoPP-Modul zur eGK ist darin mit enthalten.
PoPP.UC_05	I_PoPP_Load_Practitioner_Information	In diesem Aufruf führt der PoPP-Service mit einem übergebenen FHIR-VZD Search Request eine Anfrage am FHIR-VZD durch. Der UC Beginnt mit dem Erhalt der Anfrage LoadPractitionerInformationRequest im PoPP-Dienst und endet mit dem Absenden der Response an das PoPP-Modul.
PoPP.UC_06	I_PoPP_Read_Status_PoPP	In diesem Aufruf liest der PoPP-Service den aktuellen Nachrichten-Datensatz. Der aktuelle Nachrichten-Datensatz wird vom PoPP-Service in der Response an das PoPP-Modul gesendet.
PoPP.UC_07	I_PoPP_Token_Generation_online_check_in	In diesem Aufruf ruft das Primärsystem einer LEI PoPP-Token zu Online-Check-in ab. Der PoPP-Service <ul style="list-style-type: none"> ermittelt PoPP-Datensätze zur LEI Erstellt PoPP-Token Aktualisiert den Nachrichten-Datensatz zum PoPP-Datensatz Die erstellten PoPP-Token werden vom PoPP-Service in der Response an das Primärsystem der LEI gesendet.

1285
1286 Aktualisierung der Anforderung zu den Performance-Kenngrößen:

1287 **A_27030-01 -Performance - PoPP-Service - Bearbeitungszeit unter Last**
1288 Der PoPP-Service MUSS die Bearbeitungszeitvorgaben unter Last aus Tabelle
1289 "Tab_gemSpec_Perf_PoPP_Service: Last- und Bearbeitungszeitvorgaben" erfüllen.

1291 **Tabelle 9 Tab_gemSpec_Perf_PoPP_Service: Last- und Bearbeitungszeitvorgaben**

Operation	Spitzenlast [1/sec]	Mittlere Bearbeitungszeit [msec]	Maximale Bearbeitungszeit [msec]	Erfüllungsquote [%]
-----------	------------------------	----------------------------------------	----------------------------------------	------------------------

PoPP.UC_01	1400	600	1500	99,99
PoPP.UC_02	-	-	-	-
PoPP.UC_03	1400	1800 (600+1200 PoPP.UC_05)	3500	99,99
PoPP.UC_04	350	1700 (500+1200 PoPP.UC_05)	3250	99,99
PoPP.UC_05	350	1200	2000	99,99
PoPP.UC_06	1400	600	1500	99,99
PoPP.UC_07	1400	600	1500	99,99

[<=]

4.9 Änderungen in [gemKPT_Betr]

Anpassung Tabelle

Tabelle 10: Tab_gemKPT_Betr_Produkttypen

ID	Produkttyp / Anwendungstyp	Produkttyp-Name / Anwendungsname
PDT69	gemProdT_NCPeH_FD	National Contact Point for eHealth Fachdienst
PDT70	gemProdT_IDP_FedMaster	Federation Master
PDT71	gemProdT_PoPP_Service_PTV	Proof of Patient Presence-Service
...		

**Tabelle der PerformanceKenngrößen ist nicht mehr im Betriebskonzept
enthalten. Daher keine Anpassung dort.**

5 Dokumentenhaushalt

Im Rahmen dieser Feature-Spezifikation werden die folgenden Dokumente angepasst:

Dokument	Normativ für	Anpassungen
[gemSpec_Popp_Service]	Hersteller Anbieter	
[gemILF_PoPP_Client]	Hersteller (PS)	
[gemSpec_PoPP_Modul]	Hersteller	
[api.popp]	Hersteller	
[gemSpec_ZETA]	Hersteller Anbieter	
[gemSpec_IDP_Sek]		
[gemKPT_Test]	Hersteller	
[gemSpec_Perf]	Hersteller Anbieter	
[gemKPT_Btr]	Hersteller Anbieter	
[gemSpec_VZD_FHIR]	Hersteller	

Es wird ein Dokument neu erstellt: [gemSpec_PoPP_Modul]

6 Anhang A - Verzeichnisse

6.1 Abkürzungen

Kürzel	Erläuterung
LEI	Leistungserbringerinstitution
LE	Leistungserbringer
VER	versicherte Person

6.2 Glossar

Tabelle 11: Glossar der explizit im Dokument verwendeten Begriffe

Begriff	Erläuterung
Authenticator-Modul	Die Komponente, durch die der Nutzer die Authentifizierung gegenüber dem Identity Provider (IDP) durchführt, ist ein wesentlicher Bestandteil des Sicherheitssystems.
Authenticator-App	Authenticator-App der Krankenkassen oder Krankenversicherungen, über die die Authentifizierung des Versicherten mit der GesundheitsID erfolgt. Diese Apps enthalten immer das von der gematik spezifizierte Authenticator-Modul. Einige Kassen integrieren das Authenticator-Modul direkt in ihre Krankenversicherungs-Apps (1-App-Strategie), andere halten Krankenversicherungs-App und Authenticator-App getrennt (2-App-Strategie).
Card Access Number (CAN)	Wird verwendet um eine vertrauenswürdige, kontaktlose Kommunikation zu einer Smartcard aufzubauen
CVC-Root	Die CVC-Root ist die zentrale Root-CA der PKI für CV-Zertifikate in der TI. Die CVC-Root ist ein Produkttyp.
Distinguished Encoding Rules (DER)	Eine Variante zur Codierung von ASN.1 Objekten als Bytestring.
Drittanbieter-App	Drittanbieter-App bieten den Versicherten digitale Service

	zur Unterstützung medizinischer Anwendungsfälle an. Beispiele für Drittanbieter-Apps sind Apotheken-Apps, Videosprechstunden-Apps oder DiGA-Apps. Die Apps von Krankenkassen aka Krankenversicherungs-Apps sind von Drittanbieter-Apps verschieden. Drittanbieter-App können für beliebige Smartphone-Betriebssysteme wie Android oder iOS sowie für unterschiedliche Desktop Betriebssysteme wie Windows oder Linux verfügbar sein. Zudem ist es möglich, dass Drittanbieter-Apps innerhalb beliebiger Internetbrowser laufen.
GesundheitsID	Die GesundheitsID ist die digitale Identität im Gesundheitswesen für Versicherte, welche durch die eigene Krankenversicherung bereitgestellt wird. Sie dient zur Anmeldung an TI-Anwendungen und weiteren versorgungsrelevanten Fachanwendungen und kann perspektivisch auch als Versicherungsnachweis - analog zur elektronischen Gesundheitskarte - verwendet werden.
Krankenversicherungs-App	Mit einer Krankenversicherungs-App bieten Krankenversicherungen ihren Versicherten digitale Service zur Unterstützung medizinischer Anwendungsfälle an.
Leistungserbringer (LE)	Ein Leistungserbringer gehört zu einem zugriffsberechtigten Personenkreis nach § 352 SGB V und erbringt Leistungen des Gesundheitswesens für Versicherte. Nach § 339 SGB V darf er auf Versichertendaten in Anwendungen der TI zugreifen.
Leistungserbringerinstitution (LEI)	Die in organisatorischen Einheiten oder juristischen Personen zusammengefassten Leistungserbringer (bspw. Arztpraxen, Krankenhäuser).
Mobiles PS	Mobiles Endgerät, auf dem ein PS-Client einer LEI installiert ist. Ein LE nutzt den mobilen PS-Client bei Anwendungsfällen außerhalb der LEI.
PoPP-Client	Eine Komponente im Primärsystem, die für die sichere Kommunikation zum PoPP-Service verantwortlich ist.
PoPP-Modul	Eine Komponente von Krankenversicherung-App oder Drittanbieter-App, welche beim Online Check-in die Kommunikation mit dem PoPP-Service übernimmt. Das PoPP-Modul verwaltet TAN, die es vom PoPP-Service im Rahmen eines Online Check-ins erhält und hilft bei der Übertragung einer TAN an das Primärsystem.
PoPP-Service	Zentraler Dienst in der Telematikinfrastruktur 2.0 (TI 2.0), der PoPP-Token generiert und an LEIs ausliefert..
PoPP-Token	Der PoPP-Token dient als Nachweis für einen

	Versorgungskontext im Gesundheitswesen. Er ist ein kryptografisch gesicherter Beleg, der die Verbindung zwischen zwei Identitäten im Gesundheitswesen darstellt: dem Versicherten, bzw. dessen eGK, und einer LEI.
Proof of Patient Presence (PoPP)	PoPP ist ein Nachweis, der belegt, dass ein Versicherter sich zu einem bestimmten Zeitpunkt in einem Versorgungskontext mit einer bestimmten LEI befindet.
Versorgungskontext (VK)	Der Versorgungskontext beschreibt die sichere und kryptografisch belegte Verbindung zwischen einem berechtigten Versicherten und einer authentifizierten LEI. Diese Verbindung autorisiert den Zugriff auf anwendungsbezogene Versicherungsdaten über die Telematikinfrastruktur (TI) Anwendungen. Ein Versorgungskontext besteht, wenn ein Leistungserbringer und ein Versicherter zum Zweck einer Versorgung zusammenkommen. Dabei kann die Versorgung eine medizinische Behandlung, eine pflegerische Leistung oder eine andere Versorgungsleistung sein, beispielsweise in einer Apotheke. Das Zusammentreffen kann lokal in einer Leistungserbringerumgebung, mobil, beispielsweise bei einem Hausbesuch oder virtuell, beispielsweise bei einer Telefon- oder Videosprechstunde sein. Ein Versorgungskontext entsteht durch die erfolgreiche Authentifizierung des Versicherten mittels digitaler Identität oder durch die erfolgreiche Authentifizierung seiner eGK, und ist auch bei telemedizinischen Anwendungen relevant.
VZD	FHIR VZD (siehe Glossar der gematik)
ZETA Client	Zero Trust Client Komponente im Primärsystem; Client Komponente gegenüber der Zero Trust Server Komponente ZETA Guard.
ZETA Guard	Der beim Fachdienst einzubindende Zero Trust Cluster.

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

6.3 Abbildungsverzeichnis

Abbildung 1: Rollen und Akteure bei Herstellung und Betrieb des PoPP-Service.....	23
Abbildung 2: Produkttypzerlegung PoPP-Service.....	24
Abbildung 3: Systemkontext PoPP-Service.....	26
Abbildung 4: Anwendungsfälle zur Attestierung des Versorgungskontexts.....	31

Abbildung 5: Use-Case-Übersicht Online-Check-in aus einer App mit integriertem PoPP-Modul..... 34

6.4 Tabellenverzeichnis

Tabelle 1: PoPP-Use Cases (Business Sicht).....20

Tabelle 2: Kurzbeschreibung der Komponenten in der PoPP-Lösung.....26

Tabelle 3: Zuordnung der Anwendungsfälle zu den Use Cases.....31

Tabelle 4: Kurzbeschreibung technische Use Cases Online-Check-in aus einer App mit integriertem PoPP-Modul..... 34

Tabelle 5: Attribute im well-known document des PoPP-Service.....57

Tabelle 6: Attribute im well-known document des PoPP-Service.....57

Tabelle 7: Attribute des Metadatenblock oauth_resource im well-known document des PoPP-Service..... 58

Tabelle 8: Attribute des Metadatenblock oauth_resource im well-known document des PoPP-Service..... 59

Tabelle 9 Tab_gemSpec_Perf_PoPP_Service: Last- und Bearbeitungszeitvorgaben.....67

Anpassung Tabelle Tabelle 10: Tab_gemKPT_Betr_Produkttypen.....68

Tabelle 11: Glossar der explizit im Dokument verwendeten Begriffe.....70

6.5 Referenzierte Dokumente

6.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[PoPP-Service-RC2]	gematik Spezifikation "Proof of Patient Presence (PoPP)-Service" , Releasekandidat 2 vom 17.06.2025 https://gemspec.gematik.de/prereleases/Draft_PoPP_25_1/gemSpec_PoPP_Service_V1.0.0_CC2/
[gemSpec_Popp_Service]	gematik Spezifikation "Proof of Patient Presence (PoPP)-Service" , Releasekandidat 2 vom 17.06.2025 https://gemspec.gematik.de/prereleases/Draft_PoPP_25_1/gemSpec_PoPP_Service_V1.0.0_CC2/

	1/gemSpec_PoPP_Service_V1.0.0_CC2/
[gemSpec_PoPP_Service_US1]	Angepasste (reduzierte) Version von [gemSpec_PoPP_Service] für die Ausschreibungsunterlagen, in der nur die Inhalte von Umsetzungsstufe 1 adressiert sind. (nicht über gemSpec_Pages verfügbar) Polarion: <i>Mainline_OPB1/PoPP_Ausschreibung/gemSpec_PoPP_Service_US1_V1_0_x</i>
[gemILF_PoPP_Client]	Implementierungsleitfaden Primärsystemfunktionalität PoPP-Client https://github.com/gematik/spec-ilf-popp-client/tree/main (Version 1.0.0 vom 04.07.2025)
[gemSpec_PoPP_Modul]	
[gemSpec_ZETA]	gematik Spezifikation Zero Trust Access (ZETA) https://gemspec.gematik.de/docs/gemSpec/gemSpec_ZETA/
[api-popp]	OpenAPI Schnittstellenspezifikation des PoPP-Service für Clients https://github.com/gematik/api-popp insbesondere: https://github.com/gematik/api-popp/tree/US-2_CC1 (vom 22.01.2026)
[I_PoPP_CheckIn_HID.yaml]	OpenAPI Schnittstellenspezifikation für Authentifizierung mit GesundheitsID und Anlegen eines PoPP-Datensatzes https://github.com/gematik/api-popp/blob/US-2_CC1/src/openapi/I_PoPP_CheckIn_HID.yaml
[I_PoPP_CheckIn_eGK_Verification.yaml]	OpenAPI Schnittstellenspezifikation für Authentifizierung einer eGK und Anlegen eines PoPP-Datensatzes https://github.com/gematik/api-popp/blob/US-2_CC1/src/openapi/I_PoPP_CheckIn_eGK_Verification.yaml
[I_PoPP_Load_Practitioner_Information.yaml]	OpenAPI Schnittstellenspezifikation für das Laden der Informationen zu einer LEI vom FHIR-VZD https://github.com/gematik/api-popp/blob/US-2_CC1/src/openapi/I_PoPP_Load_Practitioner_Information.yaml
[I_PoPP_Read_Status_PoPP.yaml]	OpenAPI Schnittstellenspezifikation für das Lesen des aktuellen Status zur PoPP-Token Erstellung und Auslieferung https://github.com/gematik/api-popp/blob/US-2_CC1/src/openapi/I_PoPP_Read_Status_PoPP.yaml

[I_PoPP_Token_Generation_online_check_in.yaml]	OpenAPI Schnittstellenspezifikation zur Übertragung von PoPP-Token an den PoPP-Client, wenn die Übertragung durch den PoPP-Service nach einem Online Check-in initiiert wird https://github.com/gematik/api-popp/blob/US-2_CC1/src/openapi/I_PoPP_Token_Generation_online_check_in.yaml
[I_PoPP_Token_Generation.yaml]	OpenAPI Schnittstellenspezifikation des PoPP-Service für PoPP-Clients: https://github.com/gematik/api-popp/blob/US-2_CC1/src/openapi/I_PoPP_Token_Generation.yaml

1346

1347

6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ISO/IEC 18004:2024]	ISO/IEC 18004:2024] "Information technology – Automatic Identification and Data Capture Techniques – QR Code 2005 Bar Code Specification," ISO/IEC 18004:2024, International Organization for Standardization, 2024. https://www.iso.org/standard/83389.html
[RFC3629]	D. B. Cohen, "UTF-8, a transformation format of ISO 10646," RFC 3629, Nov. 2003. https://datatracker.ietf.org/doc/html/rfc3629
[RFC1738]	Uniform Resource Locators (URL) https://www.rfc-editor.org/rfc/rfc1738.html
[RFC7517]	https://datatracker.ietf.org/doc/html/rfc7517 JSON Web Key (JWK)
[RFC7519]	JSON Web Token (JWT) https://datatracker.ietf.org/doc/html/rfc7519
[RFC8259]	D. B. Crockford, "The JavaScript Object Notation (JSON)," RFC 8259, Dez. 2017. https://datatracker.ietf.org/doc/html/rfc8259
[OpenID Federation 1.0]	OpenID Federation Standard https://openid.net/specs/openid-federation-1_0.html

1348

7 Anhang B - Anforderungshaushalt

7.1 Umsetzungsanforderungen

Die folgenden High-Level Anforderungen gründen sich aus dem Feature Online-Check-in:

A_28149 -PS - QR-Code erzeugen für PoPP

Das Primärsystem MUSS für jeden Arbeitsplatz einen statischen QR-Code erzeugen, der Telematik-ID und optional eine WorkplaceID enthält. [≤]

A_28150 -PoPP-Modul - QR-Code und Versicherten Authentisierung

Das PoPP-Modul MUSS den QR-Code scannen und die Authentifizierung der versicherten Person durchführen. [≤]

A_28151 -PoPP-Modul - Datenübergabe an PoPP-Service

Nach erfolgreicher Authentifizierung MUSS das PoPP-Modul die relevanten Daten an den PoPP-Service übermitteln. [≤]

A_28152 -PoPP-Service - PoPP-Token erzeugen und liefern

Der PoPP-Service MUSS ein PoPP-Token erzeugen und an die LEI zurückgeben. [≤]

A_28153 -PoPP-Lösung - unterstützte Szenarien

Das Verfahren MUSS für Vor-Ort-, mobile und Fernversorgung nutzbar sein. [≤]

A_28154 -PoPP-Lösung - Missbrauchsschutz QR-Code

Der QR-Code MUSS die Einschränkung von Missbrauchsszenarien unterstützen (z. B. darf der QR-Code keine url enthalten). [≤]

7.2 Blattanforderungen/ spezifische Festlegungen

Die konkreten Anforderungen und Festlegungen zu den Änderungen sind im Kapitel 6.2 von diesem Dokument enthalten.

8 Anhang C - Offene Punkte, Fragen

8.1 Offene Punkte

<i>OP-PoPP-1</i>	Kap 4.1.14 (PoPP-Service) Kap 4.2.3 (ILF PoPP Clint)	<i>Der konkrete Ablauf zur Benachrichtigung der LEI über ZETA Guard - ZETA Client, dass Popp-Token abgerufen werden können, ist noch offen. Die Spezifikation von ZETA Guard hierzu ist noch nicht abgeschlossen.</i>	
<i>OP-PoPP-2</i>	Kap 4.7 (Testkonzept)	<i>Es soll eine Testtreiberschnittstelle analog zum Vorgehen beim ePA-FdV für PoPP-Modul/ App-mit-Popp-Modul entwickelt werden. Die entsprechenden Festlegungen werden in [gemKPT_Test] an geeigneter Stelle aufgenommen werden..</i>	