

Telematikinfrastruktur 2.0

Feature: PoPP Stufe 2 - Online Check-in

Version:	1.0.0 CCCC 4
Revision:	14957881713069
Stand:	26.01 03.09.2026
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
1.0.0 CC2	11.05.2026			gematik
1.0.0 CC3	05.08.2026		zur Abstimmung	gematik
1.0.0 CC4	03.09.2026		zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments	8
1.1 Zielsetzung	8
1.2 Zielgruppe	8
1.3 Abgrenzungen	9
1.4 Methodik	9
1.4.1 Epic und User Story	9
1.4.2 Anforderungen	9
2 Konzept	11
2.1 Komponenten und Rollen	12
2.1.1 Apps/Anwendungen	12
2.1.2 Authentifizierung	14
2.1.3 Auswahl der LEI	15
2.1.4 PoPP-Modul	15
2.1.5 Informationen zur LEI: QR-Code / WorkplaceID	16
2.1.6 PoPP-Client	16
2.1.7 PoPP-Service	17
2.2 Abläufe (Workflows)	17
2.2.1 Vor-Ort in Versorgungseinrichtung	19
2.2.2 Mobile Versorgung (beispielsweise Haus-/Heimbesuch)	20
2.2.3 Fernversorgung (beispielsweise Videosprechstunde)	20
2.2.3.1 Online-Check-in über eine Drittanbieter-App (voll integriert)	20
2.2.3.2 Online-Check-in über eine Drittanbieter-App mit Nutzung der Krankenversicherungs-App (App2App)	21
2.3 Sicherheit	21
2.4 Technischer Workflow: Verarbeitung von LEI-Daten	22
2.4.1 Verarbeitung Telematik-ID	22
2.4.2 Verarbeitung WorkplaceID	23
2.5 Nicht Bestandteil des Dokuments	23
3 Einordnung in die Telematikinfrastruktur	24
4 Spezifikation	25
4.1 Änderungen in [gemSpec_PoPP_Service]	25
4.1.1 [gemSpec_PoPP_Service#2.1]: Überblick zum Ablauf eGK und GesundheitsID aus Versichertensicht	25
4.1.2 [gemSpec_PoPP_Service#2.2]: Überblick der Anwendungsfälle für die Ausstellung von PoPP-Token	25
4.1.3 [gemSpec_PoPP_Service#2.3]: Akteure und Rollen	29
4.1.3.1 [gemSpec_PoPP_Service#2.3.1.6]: Hersteller PoPP-Modul	31
4.1.3.2 [gemSpec_PoPP_Service#2.3.1.7]: Hersteller App	31
4.1.4 [gemSpec_PoPP_Service#3]: Systemkontext PoPP-Service	32
4.1.5 [gemSpec_PoPP_Service#3.1]: Produktzerlegung und Außenschnittstellen	32
4.1.6 [gemSpec_PoPP_Service#3.2]: Systemkontext	35

4.1.7 [gemSpec_PoPP_Service#3.3]: Nachbarsysteme	40
4.1.8 [gemSpec_PoPP_Service#4]: Funktionale Anwendungsfälle des PoPP Service	41
4.1.9 [gemSpec_PoPP_Service#4.1]: Übersicht der Systemanwendungsfälle für die Ausstellung des PoPP Token	42
4.1.10 Neues Kapitel 4.5: Online-Check in und Ausgabe des PoPP Token	45
4.1.11 Neues Kapitel 4.5.1: Auswahl einer LEI für den Online-Check in	49
4.1.11.1 Zugang zum FHIR VZD	50
4.1.11.2 Ermittlung von Informationen zu einer LEI	50
4.1.12 Neues Kapitel 4.5.2: Online-Check in mit GesundheitsID	50
4.1.13 Neues Kapitel 4.5.3: Online-Check in mit eGK in Fernversorgung	62
4.1.14 Neues Kapitel 4.5.4: PoPP Token bei Online-Check in	70
4.1.15 Neues Kapitel 4.5.5: Status der PoPP Token Erstellung nach Online-Check in ermitteln	77
4.1.16 Änderungen [gemSpec_PoPP_Service#5.3.4] PoPP-Service Signaturen	81
4.1.17 Änderungen [gemSpec_PoPP_Service#5.4]: ZETA Guard im PoPP-Service	82
4.1.18 Änderungen [gemSpec_PoPP_Service#5.6]: Federation Entity Statement	84
4.1.19 [gemSpec_PoPP_Service#6.1] eGK Handling	89
4.1.19.1 Ergänzung in Kap. 6.1.1 – eGK Handling, Einführung	89
4.2 Änderungen in [gemILF_PoPP_Client]	92
4.2.1 Erzeugung und Verwendung statischer QR Codes für PoPP	92
4.2.2 WorkplaceID	95
4.2.3 Verbindung zum PoPP-Service herstellen und PoPP Token abrufen	95
4.3 Änderungen in [gemSpec_PoPP_Modul]	96
4.4 Änderungen in [api-popp]	97
4.5 Änderungen in [gemSpec_ZETA]	100
4.6 Änderungen in [gemSpec_IDP_Sek]	101
4.7 Änderungen in [gemKPT_Test]	103
4.7.1 Änderungen im Kapitel 7.4 Interoperabilität	103
4.8 Änderungen in [gemSpec_Perf]	104
4.9 Änderungen in [gemKPT_Betr]	109
5 Dokumentenhaushalt	111
6 Anhang A – Verzeichnisse	112
6.1 Abkürzungen	112
6.2 Glossar	112
6.3 Abbildungsverzeichnis	116
6.4 Tabellenverzeichnis	117
6.5 Referenzierte Dokumente	118
6.5.1 Dokumente der gematik	118
6.5.2 Weitere Dokumente	120
7 Anhang B – Anforderungshaushalt	122
7.1 Umsetzungsanforderungen	122
7.2 Blattanforderungen/ spezifische Festlegungen	122

8 Anhang C – Offene Punkte, Fragen	123
8.1 Offene Punkte.....	123
1 Einordnung des Dokuments	8
1.1 Einordnung Konzeptdokumente.....	8
1.2 Zielsetzung	8
1.3 Zielgruppe	8
1.4 Abgrenzungen	9
1.5 Methodik	9
1.5.1 Epic und User Story.....	9
1.5.2 Anforderungen.....	9
2 Konzept	11
2.1 Komponenten und Rollen.....	12
2.1.1 Anwendungen und Zusammenspiel der Komponenten.....	12
2.1.2 Authentifizierung.....	14
2.1.3 Ermittlung der Telematik-ID	14
2.1.4 PoPP-Modul	15
2.1.5 Informationen zum Inhaber der Telematik-ID: QR-Code / WorkplaceID	16
2.1.6 PoPP-Client	16
2.1.7 PoPP-Service	17
2.2 Abläufe (Workflows)	17
2.2.1 Vor-Ort in Versorgungseinrichtung	19
2.2.2 Mobile Versorgung (beispielsweise Haus-/Heimbesuch).....	20
2.2.3 Fernversorgung (beispielsweise Videosprechstunde)	20
2.2.3.1 <i>Online Check-in über eine Anbieter-App mit Nutzung einer Kassen-App (App2App).....</i>	<i>20</i>
2.3 Sicherheit	21
2.4 Technischer Workflow: Verarbeitung von Daten des Inhabers der Telematik-ID	22
2.4.1 Verarbeitung Telematik-ID	22
2.4.2 Verarbeitung WorkplaceID	23
2.5 Nicht Bestandteil des Dokuments	23
3 Einordnung in die Telematikinfrastruktur	24
4 Spezifikation	25
4.1 Änderungen in [gemSpec_Popp_Service].....	25
4.1.1 [gemSpec_PoPP_Service#2.1]: Überblick zum Ablauf eGK und GesundheitsID aus Versichertensicht	25
4.1.2 [gemSpec_PoPP_Service#2.2]: Überblick der Anwendungsfälle für die Ausstellung von PoPP-Token	25
4.1.3 [gemSpec_PoPP_Service#2.3]: Akteure und Rollen.....	29
4.1.3.1 [gemSpec_PoPP_Service#2.3.1.6]: Hersteller PoPP-Modul	31
4.1.3.2 [gemSpec_PoPP_Service#2.3.1.7]: Hersteller App	31
4.1.4 [gemSpec_PoPP_Service#3]: Systemkontext PoPP-Service	32
4.1.5 [gemSpec_PoPP_Service#3.1]: Produktzerlegung und Außenschnittstellen....	32

4.1.6 [gemSpec_PoPP_Service#3.2]: Systemkontext	35
4.1.7 [gemSpec_PoPP_Service#3.3]: Nachbarsysteme	40
4.1.8 [gemSpec_PoPP_Service#4]: Funktionale Anwendungsfälle des PoPP-Service	41
4.1.9 [gemSpec_PoPP_Service#4.1]: Übersicht der Systemanwendungsfälle für die Ausstellung des PoPP-Token	42
4.1.10 Neues Kapitel [gemSpec_PoPP_Service#4.5]: Online Check-in und Ausgabe des PoPP-Token	45
4.1.11 Neues Kapitel 4.5.1: Auswahl des Inhabers der Telematik-ID für den Online Check-in	49
4.1.11.1 Neues Kapitel 4.5.1.1: Zugang zum FHIR-VZD	50
4.1.11.2 Neues Kapitel 4.5.1.2: Ermittlung von Informationen zum Inhaber der Telematik-ID	50
4.1.12 Neues Kapitel 4.5.2: Online Check-in mit GesundheitsID	50
4.1.13 Neues Kapitel 4.5.3: PoPP-Token bei Online Check-in	62
4.1.14 Neues Kapitel 4.5.5: Status der PoPP-Token-Erstellung nach Online Check-in ermitteln	77
4.1.15 Änderungen [gemSpec_PoPP_Service#5.2]: 5.2 Datenschutz und Sicherheit	81
4.1.16 Änderungen [gemSpec_PoPP_Service#5.4]: ZETA Guard im PoPP-Service ..	82
4.1.17 Änderungen [gemSpec_PoPP_Service#5.4.1]: Bereitstellung, Konfiguration und Verwendung vom ZETA Guard	83
4.1.18 Neues Kapitel [gemSpec_PoPP_Service#5.4.2]: Versand von Push- Notification über ZETA Guard an das Smartphone des Versicherten	83
4.1.19 Änderungen [gemSpec_PoPP_Service#5.6]: Federation Entity Statement ...	84
4.1.20 Änderungen in [gemSpec_PoPP_Service#6.1.2]: Schnittstelle für Token- Abrufe	88
4.1.20.1 PoPP-Token Abruf nach eGK-Anbindung durch LEI	90
4.1.20.2 PoPP-Token Abruf nach Online-Check-in	91
4.1.20.2.1 REST-Betrieb	91
4.1.20.2.2 WebSocket-Betrieb	91
4.2 Änderungen in [gemILF_PoPP_Client]	92
4.2.1 Erzeugung und Verwendung statischer QR-Codes für PoPP	92
4.2.2 WorkplaceID.....	95
4.2.3 Verbindung zum PoPP-Service herstellen und PoPP-Token abrufen	95
4.3 Änderungen in [api-popp]	97
4.4 Änderungen in [gemSpec_ZETA]	100
4.5 Änderungen in [gemKPT_Test].....	101
4.5.1 Änderungen im Kapitel 7.4 Interoperabilität	101
4.6 Änderungen in [gemSpec_IDP_Sek]	101
4.7 Änderungen in [gemSpec_Perf]	104
4.8 Änderungen in [gemKPT_Betr].....	109
5 Dokumentenhaushalt.....	111
6 Anhang A – Verzeichnisse	112
6.1 Abkürzungen	112
6.2 Glossar	112
6.3 Abbildungsverzeichnis.....	116

6.4 Tabellenverzeichnis	117
6.5 Referenzierte Dokumente	118
6.5.1 Dokumente der gematik.....	118
6.5.2 Weitere Dokumente.....	120
7 Anhang B - Anforderungshaushalt	122
7.1 Umsetzungsanforderungen	122
7.2 Blattanforderungen/ spezifische Festlegungen	122
8 Anhang C – Offene Punkte, Fragen	123
8.1 Offene Punkte.....	123

1 Einordnung des Dokuments

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

1.1 Einordnung Konzeptdokumente

Die grundlegenden fachlichen Konzepte zu PoPP wurden in [gemKPT_PoPP] beschrieben. Das Dokument enthält bereits ein Konzept für den mobilen Check-in mit GesundheitsID (Kapitel 4.3 „PoPP mit GesundheitsID“) und bildet den fachlichen Stand von 2024 ab. Es wird nicht weiter fortgeschrieben.

Kapitel 2 dieses Dokuments [gemF_PoPP_Online_Check-in] führt das bisherige Konzept fort und beschreibt das aktuelle Fachkonzept für den Online Check-in (PoPP Stufe 2). Es berücksichtigt insbesondere das PoPP-Modul, die Verwendung von ZETA (für die Versicherten-Authentisierung), das Zusammenspiel von Anbieter-Apps und Kassen-Apps sowie die Authentifizierung mittels GesundheitsID und Verifikation einer eGK-in-Fernversorgung.

Für die fachliche Beschreibung des Online Check-ins in PoPP Stufe 2 ist daher Kapitel 2 dieses Dokuments maßgeblich. Die Inhalte aus [gemKPT_PoPP] dienen ergänzend der fachlichen Einordnung und Herleitung.

~~1.1~~ 1.2 Zielsetzung

~~Diese~~~~Dieses~~ Feature-Dokument dient Herstellern, Anbietern und ~~Umsetzenden~~Herstellern des PoPP-Services als Orientierung und bietet eine konsolidierte Übersicht über ~~die~~ ~~neuen~~~~neue~~ Anforderungen für den Online –Check-in ~~beim~~ PoPP-Service. Dies betrifft alle Szenarien, in denen ~~der Versicherte~~~~ein Versicherte~~ sein ~~mobiles Endgerät~~ Smartphone 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~~ 1.3 Zielgruppe

Dieses Dokument richtet sich an:

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

~~1.3~~1.4 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~~nach [gemSpec_PoPP_Service], bzw. die anderen betroffenen Dokumente überführt. ~~Die~~Die überarbeitete Version von [gemSpec_PoPP_Service] wird dann für Stufe 1 und Stufe 2 gelten.

Die konzeptionellen Anteile dieses Feature-Dokuments (~~Fachliches2-Konzept und Technisches Konzept~~) verbleiben in [gemF_PoPP_Online_Check-in]. ~~Diese~~Dieses wird ~~dann~~nach Freigabe ebenfalls veröffentlicht.

Im Kapitel 2-Konzept werden zur Veranschaulichung Click-Dummies referenziert. Die darin dargestellten Umsetzungen, Abläufe und Benutzeroberflächen dienen ausschließlich der Illustration des beschriebenen Konzepts. Aus den Click-Dummies lassen sich keine normativen oder verbindlichen Anforderungen ableiten. Maßgeblich und verbindlich sind ausschließlich die Festlegungen in den Spezifikationen.

~~1.4~~1.5 Methodik

~~1.4.1~~1.5.1 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~~1.5.2 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 dem Inhaber einer Telematik-ID (Leistungserbringerinstitution (LEI, DiGA, Kostenträger) und Versicherten (VER). Neu eingeführt wird mit Stufe 2 der Online -Check-in für PoPP, der direkt am Smartphone des VERVersicherten 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 allen Versorgungsszenarien für ~~die LEI~~Inhaber einer Telematik-ID zu ermöglichen und zusätzlich den VER Versicherten 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~~Inhabern einer Telematik-ID den Zugriff auf die Versichertendaten in ~~den~~ Fachdiensten ermöglicht.

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

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

Der Prozess startet mit der Auswahl des Inhabers der ~~LEI~~Telematik-ID, bei der ~~der~~sich die VER einchecken möchte.

1. Dies ~~erfolgt in der Regel~~kann erfolgen durch
 - a. das Scannen eines statischen QR-Codes (beinhaltet die Telematik-ID ~~der LEI~~) aus einer App für den Online -Check-in heraus,
 - b. eine Suche im Verzeichnisdienst (VZD) über die Erfassung von Suchkriterien,
 - c. Übernahme der Telematik-ID aus anderen Quellen.
2. Danach weist sich ~~der~~die VER mithilfe seiner GesundheitsID ~~oder eGK an seinem Smartphone aus.~~
3. Abschließend wird der PoPP-Token im PoPP-Service Resource Server erstellt und ~~über diesen der LEI~~der PoPP-Service stellt dem Inhaber der Telematik-ID den PoPP-Token für den Zugriff auf die Versichertendaten in den Fachdiensten zur Verfügung ~~gestellt.~~

~~Die App erhält durch den~~Der Online -Check-in vermittelt der verwendeten App keinen Zugriff auf ~~die~~Versichertendaten ~~im Fachdienst. Dieser. Der Zugriff ist weiterhin auf die~~

Versichertendaten bleibt, wie ~~auch~~ bereits in Stufe 1, ausschließlich ~~derdem~~ berechtigten LEI-Inhaber der vom Versicherten ausgewählten Telematik-ID vorbehalten, ~~die zuvor durch~~ PoPP-Token gelangen zu keinem Zeitpunkt in den ~~VER~~ ~~ausgewählt wurde~~ Verfügungsbereich der Versicherten (inklusive App), sondern werden vom PoPP-Service ausschließlich direkt an den im Primärsystem des Inhabers der ausgewählten Telematik-ID integrierten PoPP-Client übermittelt.

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 die Aufgaben, bzw. Rollen der 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. des Inhabers einer Telematik-ID 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~~ ~~werden~~ 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~~ ~~Workflows~~ dargestellt ~~wird~~ ~~werden~~.

2.1 Apps/Komponenten und Rollen

2.1.1 Anwendungen und Zusammenspiel der Komponenten

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

~~Es können sowohl~~ Der Online Check-in wird stets durch ein PoPP-Modul durchgeführt. Das PoPP-Modul muss bei Verwendung der GesundheitsID in einer Kassen-App auf dem Smartphone des Versicherten integriert sein und wird durch die gematik zugelassen. Das PoPP-Modul ist Bestandteil der Anwendung, die das Authenticator-Modul des sektoralen Identity Providers (IDP) der Krankenversicherung des Versicherten implementiert. Das PoPP-Modul und das Authenticator-Modul werden daher immer gemeinsam innerhalb derselben Anwendung bereitgestellt. Die Umsetzung erfolgt in unterschiedlichen Ausprägungen:

1. Das Authenticator-Modul und das PoPP-Modul sind in eine Kassen-App integriert, die zusätzlich weitere Funktionen der Krankenversicherung bereitstellt.
2. Das Authenticator-Modul und das PoPP-Modul werden als eigenständige Anwendung der Krankenversicherung bereitgestellt.

Im Folgenden bezeichnet der Begriff **Kassen-App** stets die Anwendung, welche sowohl das Authenticator-Modul als auch das PoPP-Modul implementiert.

Der Online Check-in lässt sich aus unterschiedlichen Anwendungen heraus initiieren. Solche Anwendungen werden in dieser Spezifikation als **Anbieter-Apps** bezeichnet. Anbieter-Apps führen den Online Check-in bei Verwendung der GesundheitsID nicht selbst durch. Stattdessen übergeben sie die notwendigen Informationen an eine Kassen-App und nutzen das dort implementierte PoPP-Modul. Anbieter-Apps werden nicht durch die gematik zugelassen. Beispiele für Anbieter-Apps:

1. Apps ohne eigenes PoPP-Modul, bereitgestellt von Krankenkassenversicherungen ~~als auch Drittanbieter den Online Check-in in Apps oder in (Web-)Anwendungen implementieren,~~
- ~~iOS-/Android-Apps der Krankenkassenversicherungen:~~ 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 Krankenkassenversicherungs-App handeln.
2. ~~iOS-/Android-Apps von Drittanbietern:~~ Beispielsweise Leistungserbringern, etwa Apotheken ~~App oder,~~
3. Videosprechstunden-App zur Nutzung des Online-Apps,
4. DiGA-Apps,
5. Patientenportale,
6. browserbasierte Webanwendungen.

Anbieter-Apps können auf mobilen Endgeräten, Desktop-Systemen oder als Webanwendungen betrieben werden.

Es werden folgende Nutzungsszenarien der verschiedenen App-Typen unterstützt:

Online Check-in am Smartphone für eine (in einer Kassen-App

Die VER startet den Online Check-in unmittelbar in der Kassen-App. Es ist kein Wechsel in eine andere Anwendung erforderlich. Die Auswahl des Inhabers einer Telematik-ID erfolgt durch die VER beispielsweise mittels:

1. VZD-Suche,
2. Scannen eines QR-Codes,
3. Auswahl aus einer Favoritenliste,
4. Auswahl aus einer Historie.

Online ~~Apotheke oder Praxis~~ Check-in aus einer Anbieter-App (App2App)

Die VER startet den Online Check-in in einer Anbieter-App. Die Anbieter-App übergibt die notwendigen Informationen an eine Kassen-App. Die Durchführung des Online Check-ins erfolgt anschließend im PoPP-Modul der Kassen-App. Hierfür ist ein Wechsel von der Anbieter-App in die Kassen-App erforderlich. Die Auswahl des Inhabers einer Telematik-ID in der Krankenkassen-App kann entfallen, sofern die hierfür notwendigen Informationen (z. B. die Telematik-ID) bereits durch die Anbieter-App bereitgestellt wurden.

- ~~Webanwendungen von Drittanbietern:~~ Beispielsweise

Online Check-in aus einer Webanwendung

Die VER startet den Online Check-in in einer Webanwendung, beispielsweise einem Patientenportal oder einer Videosprechstunden-Lösung ~~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.App. Die Webanwendung übergibt die notwendigen Informationen an die Kassen-App. Der Vorteil bei Nutzung der eGK besteht darin, dass der kompletteeigentliche 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**~~ wird anschließend durch das PoPP-Modul der Kassen-App durchgeführt. Sofern die Telematik-ID bereits durch die Webanwendung festgelegt wurde, kann 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 erneute Auswahl des Inhabers einer Telematik-ID 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~~; erfolgt mit der GesundheitsID auf dem Smartphone.

- **GesundheitsID auf dem Smartphone:** Die GesundheitsID auf dem Smartphone der VER Versicherten wird verwendet. Technisch erfolgt die Authentifizierung ~~der VER bei der~~ des Versicherten mittels GesundheitsID stets über das Authenticator-Modul, das in derselben ~~Krankenversicherungs~~ Kassen-App integriert sein muss, in der auch das PoPP-Modul vorhanden ist.

2.1.3 ~~eGK über NFC-Schnittstelle:~~ Die Ermittlung der Telematik-ID

- ~~VER wählen den Inhaber einer Telematik-ID aus~~ 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 lässt sich auf verschiedene Weise durch die VER erfasst werden einen Versicherten erfassen:~~

1. **Scannen eines QR-Codes:** Ein statischer QR-Code, der die Telematik-ID beinhaltet ~~und von~~, wird vom Inhaber der ~~LEI~~ Telematik-ID etwa als Aufsteller am Empfang bereitgestellt ~~wird~~.
2. **Hinterlegung in Apps:** Die Telematik-ID wird ~~von vom~~ Inhaber der ~~LEI~~ Telematik-ID direkt in der ~~Drittanbieter~~ Anbieter-App hinterlegt, beispielsweise in einem Patientenportal oder einer Apotheken-App.
3. **Manuelle Ermittlung über VZD-Suche in der App:** ~~Die LEI mit~~ Der Inhaber der ~~notwendigen~~ Telematik-ID wird durch eine manuelle Suche im Verzeichnisdienst (VZD) ermittelt.
4. **Historie oder Favoriten in der App:** Die Telematik-ID wird durch Auswahl ~~des Inhaber~~ der ~~LEI~~ Telematik-ID über einen Eintrag aus der Historie der letzten Online -Check-ins oder aus angelegten Favoriten ermittelt.
5. **Übergabe aus einer aufrufenden Anwendung:** Die Telematik-ID wird von der aufrufenden Anwendung an das PoPP-Modul in der Kassen-App übergeben.

2.1.4 PoPP-Modul ~~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.~~

2.1.4 Technisch

Das PoPP-Modul ist eine Softwarekomponente zur Durchführung des Online-Check-ins auf Seiten der Versicherten. Es führt die Kommunikation zwischen dem Smartphone der Versicherten und dem PoPP-Service durch.

PoPP-Module werden von der gematik zugelassen.

Das PoPP-Modul ist in einer Kassen-App integriert, welche zusätzlich das Authenticator-Modul des sektoralen Identity Providers (IDP) der jeweiligen Krankenversicherung implementiert. Ein Versicherter kann bei Verwendung der GesundheitsID das PoPP-Modul entweder direkt über eine Kassen-App nutzen oder indirekt aus einer Anbieter-App heraus aufrufen.

Anbieter-Apps, wie beispielsweise Apps von Leistungserbringern, Apotheken oder Videosprechstunden-Anbietern, implementieren für die Verwendung der GesundheitsID kein eigenes PoPP-Modul. Stattdessen können sie über geeignete

Betriebssystemmechanismen das PoPP-Modul einer Kassen-App aufrufen und für den Online Check-in nachnutzen (App2App-Kommunikation).

Das PoPP-Modul ist von dem **PoPP-Client** abzugrenzen. Der PoPP-Client wird vom Personal des Telematik-ID-Inhabers im Primärsystem genutzt. Das PoPP-Modul wird von Versicherten auf ihren Smartphones genutzt.

Die technische Absicherung der Kommunikation erfolgt ~~die sichere Kommunikation für den Online-Check-in immer über die Komponentengemäß~~ der Zero-Trust-Architektur, ~~das heißt, der TI. Hierzu nutzt die Kassen-App mit integriertem PoPP-Modul benötigt zusätzlich einen ZETA -Client, der die gesicherte Kommunikation mit dem ZETA Guard imdes PoPP-Service kommuniziertermöglicht. Sämtliche Kommunikation zwischen PoPP-Modul und PoPP-Service Resource Server erfolgt über diese Sicherheitsarchitektur.~~

2.1.5 Informationen ~~zur LEI~~ zum Inhaber der Telematik-ID: QR-Code / WorkplaceID

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~~ ein QR-Code aus der App, in der der Online ~~-~~Check-in integriert ist, von ~~der VER~~ den Versicherten abgescannt wird.

Zusätzlich kann der QR-Code weitere Informationen enthalten, ~~nämlich etwa~~ eine optionale WorkplaceID, die ~~verschieden~~ verschiedene Aufgaben übernehmen kann.

1. **Arbeitsplatzzuordnung:** Die WorkplaceID kann ~~bspw.~~ 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~~ eines Versicherten direkt dem richtigen Arbeitsplatz zugeordnet werden kann.
2. **SessionID:** Die WorkplaceID kann zusammen mit der Telematik-ID auch in ~~Drittanbieter~~ Anbieter-Apps hinterlegt werden, um als SessionID eine richtige Zuordnung zwischen Aktionen in einer App ~~der VER~~ des Versicherten und dem PoPP-Token nach dem erfolgreichen Online ~~-~~Check-in im PS ~~des Inhabers~~ der ~~LEI~~ Telematik-ID zu gewährleisten.

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

Erfolgt die Auswahl ~~des Inhabers einer Telematik-ID~~ in der ~~LEI in der~~ ~~Krankenversicherungs~~ Kassen-App ~~jedoch~~ aus dem Verzeichnisdienst (VZD), den Favoriten oder der Historie, ~~ohne eine dort hinterlegte WorkplaceID, so~~ wird ~~auch~~ keine WorkplaceID 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~~ des Inhaber der Telematik-ID 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 ~~zur~~ Stufe ~~2~~ ¹ unverändert. Im PoPP-Service werden PoPP-Token erzeugt und nach erfolgreicher Authentifizierung ~~desInhabers~~ der ~~LEITelematik-ID~~ sowie nach dem Ausweisen ~~des Versicherten an das Primärsystem desInhabers~~ der ~~VER an die LEITelematik-ID~~ übermittelt.

Neu ist, dass der PoPP-Service auch mit dem PoPP-Modul kommuniziert. Dadurch kann sich ~~eine VER ein Versicherter~~ direkt über ihr Smartphone für den Online -Check-in ausweisen, eine ~~LEITelematik-ID~~ 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 Krankenversicherungsmit Kassen-App mit~~, PoPP-Modul und GesundheitsID ~~vor Ort~~ in einer Versorgungseinrichtung tabellarisch ~~beschrieben, dargestellt~~. Ergänzend werden exemplarisch einzelne Alternativen mit aufgeführt. Anschließend folgt die Beschreibung der einzelnen Workflows in folgenden Versorgungsszenarien:

1. vor Ort in einer Versorgungseinrichtung,
2. mobiles Versorgungsszenario (zum Beispiel Haus- oder Heimbefuch),
3. 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 ~~möglicherweise~~ variieren ~~können~~.

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

Der Ablauf des Referenzpfad ist visuell als Click-Dummy aufrufbar:
[Linkhttps://www.figma.com/proto/z8DtEV6loj6d00GD24V3dk/PoPP?page-id=2117%3A20775&node-id=2535-5273&viewport=231%2C4358%2C0.18&t=mZ0JER1Gw40VpZoG-9&scaling=scale-down&content-scaling=fixed&starting-point-node-id=2535%3A5273](https://www.figma.com/proto/z8DtEV6loj6d00GD24V3dk/PoPP?page-id=2117%3A20775&node-id=2535-5273&viewport=231%2C4358%2C0.18&t=mZ0JER1Gw40VpZoG-9&scaling=scale-down&content-scaling=fixed&starting-point-node-id=2535%3A5273)

Tabelle 1: Ablauf Online Check-in

ID	Beschreibung
Einstieg	VER öffnet seine KrankenversicherungsKassen-App auf seinem seinem Smartphone beim Betreten der Versorgungseinrichtung. Alternativ VER checkt über eine DrittanbieterAnbieter-App ein, zum Beispiel zuhause mit einer Videosprechstunden-App.
Check-in	VER wählt die Funktion "Online -Check-in" in der Kassen-App mit PoPP-Modul aus.
Auswahl desInhabers der LEI Telematik-ID	LEIDerInhaber der Telematik-ID stellt einen statischen QR-Code (etwa Zettel, Bildschirm) am Empfang sichtbar bereit. DieserDer QR-Code enthält die Telematik-ID. VER scannt am Empfang den QR-Code. Alternativ, wenn beispielsweise in der Fernversorgung kein QR-Code gescannt werden kann: VER wählt manuell die LEIdenInhaber der Telematik-ID 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 DrittanbieterAnbieter-App hinterlegt ist, beispielsweise bei einer Apotheken-App.
Einwilligungen	VER wird in der App der Name desInhabers der LEI inkl. Telematik-ID inklusive Adresse angezeigt, welche zur ausgewählten Telematik-ID gehört; via VZD-Abruf VER bestätigt nach der Kontrolle den Online -Check-in.
Authentifizierung	VERFalls noch keine Authentifizierung erfolgt ist, weist sich mit seinerVER am Smartphone über die GesundheitsID auf seinem Smartphone aus; via in der Kassen-App (Authenticator -Modul in der Krankenversicherungs-App Alternativ VER weist sich mittels eGK ohne PIN (mit CAN) über die NFC-Schnittstelle am Smartphone aus. Dies erfolgt via Card-to-Card-Authentisierung mit PoPP-Service) aus.
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 AuthentifizierungsnachweisInformationen zur Art der durchgeführtenAuthentifizierung, an den PoPP-Service.

ID	Beschreibung
PoPP-Token-Erstellung und Abholung	PoPP-Service prüft die Daten, und speichert diese in einem temporären Datensatz. Das Primärsystem des Inhabers der Telematik-ID fragt bei PoPP-Service an, anschließend generiert dieser ein PoPP-Token und übermittelt dieses an das Primärsystem der LEI des Telematik-ID Inhabers holt den PoPP-Token ab.
Statusinformation	VER wird nach erfolgreicher Authentifizierung in der App eine Statusmeldung vom PoPP-Service angezeigt, die den erfolgreichen Online -Check-in bei der beim ausgewählten LEI Inhaber der Telematik-ID bestätigt. Alternativ VER Versicherten kann auch angezeigt werden, dass der Online -Check-in noch ausstehend ist, beispielsweise wenn die LEI der Inhaber der Telematik-ID bei einer Fernversorgung noch nicht online ist. In diesem Fall kann eine Statusänderung auch nachträglich übermittelt und der VER dem Versicherten angezeigt werden.
Abschluss	LEI erhält Der Inhaber der Telematik-ID erhält das PoPP-Token und kann damit, sofern diese berechtigt ist, um auf die Versichertendaten in den Fachdiensten zugreifen zuzugreifen.

2.2.1 Vor-Ort in Versorgungseinrichtung

VER Inhaber der Telematik-ID nutzt eGK (UC_PoPP_1a)

Bereits mit der ersten Stufe 1 umgesetzt, diesbezüglich keine Änderung. Beschreibung siehe [gemSpec_PoPP_Service].

VER nutzt GesundheitsID (UC_PoPP_1b)

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

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

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

Entspricht dem Ablauf des Happy-Path Referenzpfad. Ablauf des Happy-Path Referenzpfad ist visuell als Click-Dummy aufrufbar:

[Link](https://www.figma.com/proto/z8DtEV6loj6d00GD24V3dk/PoPP?page-) <https://www.figma.com/proto/z8DtEV6loj6d00GD24V3dk/PoPP?page->

[id=2117%3A20775&node-id=2535-5273&viewport=231%2C4358%2C0.18&t=mZ0JER1Gw4OVpZoG-9&scaling=scale-down&content-scaling=fixed&starting-point-node-id=2535%3A5273](#)

2.2.2 Mobile Versorgung (beispielsweise Haus-/Heimbesuch)

VERInhaber der Telematik-ID nutzt eGK (UC_PoPP_2a)

Bereits mit ~~der ersten~~ Stufe 1 umgesetzt, diesbezüglich keine Änderung. Beschreibung siehe [gemSpec_PoPP_Service].

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~~ der Inhaber der Telematik-ID den QR-Code mit ~~zur VER~~ zum Versicherten 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 VS DM1 dann nicht mehr zur Verfügung stehen wird.~~

~~Bei Nutzung der GesundheitsID ist für den reinen Authentifizierungsvorgang zwingend ein App Wechsel in die KrankenversicherungsAnbieter-App mit Authentifizierungsmodul erforderlich, die anderen Schritt 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](#)~~

~~2.2.3.22.2.3.1 Online-Check-in über eine Drittanbieter-App mit Nutzung der KrankenversicherungsNutzung einer Kassen-App (App2App)~~

UC_PoPP_3b (GesundheitsID)

~~und UC_PoPP_3d (eGK)~~

Diese Variante erfordert insgesamt weniger Implementierungsaufwand. Hier erfolgt nur die Auswahl ~~desInhaber~~ der ~~LEI~~Telematik-ID in der App bzw. ist in der App bereits hinterlegt. Anschließend erfolgen alle weitere Schritte in der ~~KrankenversicherungsKassen~~-App. Der Wechsel erfolgt ~~automatische~~automatisch inkl. Übergabe der ~~LEI-Auswahl~~ (TelematikIDTelematik-ID und (optional) einer WorkplaceID) ~~und~~. Nach dem erfolgreichen Check-in kehrt der Nutzer wieder in die ursprüngliche ~~DrittanbieterAnbieter~~-App zurück. Die ~~DrittanbieterAnbieter~~-App ist dabei auf die Art der Umsetzung des Online -Check-ins in der ~~KrankenversicherungsKassen~~-App angewiesen.

Im Anschluss übermittelt der PoPP-Service den PoPP-Token in das PS ~~desInhabers~~ der ~~LEI~~Telematik-ID und ermöglicht ~~demInhaber~~ der ~~LEI~~Telematik-ID 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~~dem Versicherten in der App und dem PoPP-Token im PS ~~desInhabers~~ der ~~LEI~~Telematik-ID 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~~ Der Ablauf in einer Anbieter-App am Beispiel einer Videosprechstunden-App und mit Nutzung der GesundheitsID: [Link](#)

Feldfun

Wird keine ~~DrittanbieterAnbieter~~-App verwendet ist ein Online -Check-in auch in der Fernversorgung ausschließlich über die ~~KrankenversicherungsKassen~~-App mit manueller Auswahl ~~der LEI~~desInhabers einer Telematik-ID möglich.

Die VER muss entweder einen QR-Code über die ~~KrankenversicherungsKassen~~-App einscannen, der ~~vomInhaber~~ der ~~LEI~~Telematik-ID 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~~denInhaber der Telematik-ID manuell in der ~~KrankenversicherungsKassen~~-App auswählen.

2.3 Sicherheit

~~Die~~Folgende Maßnahmen tragen dazu bei, dass genau ~~die LEI~~derInhaber der Telematik-ID den PoPP-Token erhält, ~~welcher die VER auch~~welche vom Versicherten für den Zugriff auf ihre Versichertendaten in ~~den Fachdiensten geben möchte~~ ausgewählt wurde:

1. 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: ~~bzgl. des Online Check-in-Vorgangs~~. VER gewöhnen sich dadurch daran, die vorgesehene ~~Kassen-App~~ mit PoPP-Modul zu verwenden, ~~die~~. Diese erkennt falsche QR-Codes ~~erkennt~~ und ~~den Nutzer~~ warnt ~~sowie~~die Versicherten und verweist an ~~LEI~~das Personal ~~verweist~~des Inhabers der Telematik-ID.

2. Bestätigung für ~~Versicherte~~VER

Die VER muss vor dem eigentlichen Online -Check-in zunächst ~~die LEI~~denInhaber

der Telematik-ID bestätigen. Hierzu erfolgt ein VZD-Abruf der erfassten Telematik-ID mit anschließender Anzeige des Namens ~~des~~Inhabers der ~~LEI~~Telematik-ID 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 ~~des~~Inhabers der ~~LEI~~Telematik-ID.

3. **Verantwortung für QR-Code-Inhalte**

Der statische QR-Code wird im PS erzeugt und in ~~einer LEI~~den Räumlichkeiten des Inhabers der Telematik-ID aufgestellt bzw. ~~positioniert. Die LEI~~präsentiert. ~~Der Inhaber der Telematik-ID~~ trägt die Verantwortung für die Richtigkeit der im gezeigten QR-Code enthaltenen Inhalte sowie dafür unbekannte oder als fehlerhaft gemeldete 2D-Codes zu entfernen.

4. **Minimierung der zu verarbeitenden Daten in der App**

Für den Online ~~-~~Check-in benötigt das PoPP-Modul in der Kassen-App ~~selbst~~ lediglich die Telematik-ID, ~~weder. Beispielsweise~~ die Krankenversicherungsnummer (KVN) ~~noch~~oder andere persönliche Daten der ~~VER~~Versicherten werden nicht benötigt.

5. **Unterscheidung und Sperrbarkeit von PoPP-Modulen**

Eine Unterscheidung der ~~verschiedenen~~verschiedenen Kassen-Apps die PoPP-Module beinhalten ~~kann~~ist auf Basis der ZETA-Guard-Client-Registry ~~erfolgen~~möglich. Kassen-Apps mit PoPP-Modul ~~können somit~~lassen sich so, falls notwendig auch nachträglich, vom PoPP ~~ausgeschlossen werden~~ausschließen.

6. **Information über die Authentifizierung**

Der PoPP-Token enthält die Information, ob der Online ~~-~~Check-in über ein App mit PoPP-Modul ~~von der VER~~vom Versicherten durchgeführt wurde und auf welche Weise ~~sich~~die Identität ~~der VER~~des Versicherten 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 des Inhabers der Telematik-ID

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

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

2.4.1 Verarbeitung Telematik-ID

1. Die Telematik-ID wird vom PoPP-Modul für die VZD-Suche benutzt (Consent-Dialog).
2. Die Telematik-ID wird ~~vom PoPP-Modul~~ an den PoPP-Service übergeben, ~~um~~ ~~ein~~damit der PoPP-Service darüber informiert ist, für welchen Inhaber der Telematik-ID ein PoPP-Token ~~für die zugehörige LEI zu erstellen~~auszustellen ist.

3. Der PoPP-Service prüft anhand der Telematik-ID, ob ~~dieser~~ zugehörige ~~LEI~~Inhaber der Telematik-ID authentisiert ist, und verwendet die Informationen zur Erstellung eines PoPP-Tokens.
4. Der ~~erstellte~~ PoPP-Token wird an das Primärsystem ~~desInhabers~~ der ~~zur~~ Telematik-ID ~~zugehörigen LEI~~ übermittelt.

2.4.2 Verarbeitung WorkplaceID

1. Die WorkplaceID wird lediglich im Primärsystem ~~einer LEI~~desInhaber der Telematik-ID verwendet. Daher wird die WorkplaceID als (transparenter) Parameter durch den PoPP-Service geschleust.
2. Die WorkplaceID darf weder im PoPP-Modul noch durch den PoPP-Service verändert werden.
- ~~2.3.~~ Die Übergabe der WorkplaceID erfolgt gemeinsam mit der Telematik-ID als Parameter des HTTP-Requests ~~vom PoPP-Modul~~ an den PoPP-Service.
- ~~3.4.~~ Der PoPP-Service bewahrt die Information WorkplaceID gemeinsam mit der Telematik-ID auf.
- ~~4.5.~~ Bei der Übermittlung des PoPP-Tokens an ~~eine LEI~~denInhaber einer Telematik-ID 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.
- ~~5.6.~~ Der PoPP-Service ~~muss~~übermittelt die WorkplaceID ~~übermitteln an das~~ Primärsystem, wenn er sie zuvor vom PoPP-Modul erhalten hat.
- ~~6.7.~~ Das Primärsystem prüft, ob eine WorkplaceID in der ~~Übermittlungsnachricht eines~~Nachricht mit dem PoPP-Tokens enthalten ist, ~~und~~. Das Primärsystem benutzt ~~die Information~~eine vorhandene WorkplaceID, um das PoPP-Token an den richtigen Arbeitsplatz zu übermitteln oder eine Zuordnung zwischen Aktionen in einer App der ~~VER~~Versicherten und dem PoPP-Token herzustellen.

2.5 Nicht Bestandteil des Dokuments

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

3 Einordnung in die Telematikinfrastruktur

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

Im Primärsystem ~~desInhaber~~ der ~~LEI~~Telematik-ID wird ein statischer QR-Code erzeugt und vom Versicherten über ~~die~~~~Versicherten~~eine Kassen-App (PoPP-Modul) gescannt. Der QR-Code stellt hierbei u.a. ~~die~~~~Information~~Informationen bereit, um welche ~~LEI~~~~(Telematik-ID)~~ es sich handelt, bei der sich die ~~VER~~~~Versicherten~~ einchecken möchte. Die Kommunikation ~~der~~ Kassen-App 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~~desInhabers der Telematik-ID und des Versicherten. DerInhaber der Telematik-ID authentifiziert sich mit seiner SM(C)-B. Ein Versicherter, bzw. dessen eGK, wird ebenfalls authentifiziert. Dieser Authentifizierungsprozess wird als Check-in bezeichnet.

~~Die LEI authentifiziert sich mit ihrer SMC-B. Für den Eine Möglichkeit zur Authentifizierung der Versicherten wird seine eGK authentifiziert. Dieser Authentifizierungsprozess wird als Check-in bezeichnet. Der Versicherte präsentiert seine~~ ist, dass sie ihre eGK an einem geeigneten Lesegerät ~~der LEI demInhaber der Telematik-ID präsentiert oder übergibt die eGK an LEI das Personal des Inhabers der Telematik-ID übergibt.~~ Alles Weitere führt der PoPP-Client durch.

Für den Online –Check-in am ~~GerätSmartphone~~ der VER ~~hat authentifiziert sich die VER die Wahl und authentifiziert sich entweder~~ mittels GesundheitsID ~~oder die eGK wird authentifiziert.~~ Beim Online –Check-in kommt auf dem ~~Gerät des Smartphone~~ der 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)Inhaber der Telematik-ID~~ 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~~~~der Inhaber der Telematik-ID~~ 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 2: PoPP-Use Cases (Business Sicht)

ID	Anwendungsfälle
UC_PoPP_1a	Vor-Ort in Versorgungseinrichtung mit <u>eGK</u>: bspw. Praxisbesuch Ein Versicherter möchte eine Versorgung eines Telematik-ID-Inhabers in einer LEIdessen Räumlichkeiten in Anspruch nehmen. Die LEIDer Inhaber der Telematik-ID 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 LEIdes Telematik-ID-Inhabers präsentiert. Nachdem der Versichertedie VER den Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und die LEIdas PS des Telematik-ID-Inhabers erhält im PS den notwendigen Nachweis des Versorgungskontexts.
UC_PoPP_1b	Vor-Ort in Versorgungseinrichtung mit <u>GesundheitsID</u>: bspw. Praxisbesuch Ein Versicherter möchte eine Versorgung eines Telematik-ID-Inhabers in einer LEIdessen Räumlichkeiten in Anspruch nehmen. Die LEIDer Inhaber der Telematik-ID benötigt für den Zugriff auf die Daten des physisch anwesenden Versicherten einen Nachweis des Versorgungskontexts. Dazu startet der Versichertedie VER den Online – Check-in-Prozess in einer <u>Kassen-App</u> mit integriertem PoPP-Modul, scannt den von der LEIvom Telematik-ID-Inhaber für den Check-in bereitgestellten QR-Code, bestätigt die LEINutzung der Daten durch den Inhaber der Telematik-ID und authentifiziert sich anschließend mittels GesundheitsID. Nachdem der Versichertedie VER den Online – Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und die LEIdas PS des Telematik-ID-Inhabers erhält im PS den notwendigen Nachweis des Versorgungskontexts.

ID	Anwendungsfälle
UC_PoPP_2a	In mobiler Versorgung mit <u>eGK</u>: bspw. Haus-/Heimbesuch Ein Versicherter möchte eine Versorgung außerhalb einer LEIder Räumlichkeiten eines Telematik-ID-Inhabers in Anspruch nehmen. Dazu kommt das Personal der LEIdes Telematik-ID-Inhabers zum Versicherten. Die LEIDer Inhaber der Telematik-ID 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 LEIdes Telematik-ID-Inhabers präsentiert. Nachdem das LEI-Personal des Telematik-ID-Inhabers die eGK eingelesen hat, ist der Check-in-Vorgang abgeschlossen und die LEIdas PS des Telematik-ID-Inhabers erhält im PSden notwendigen Nachweis des Versorgungskontexts.
UC_PoPP_2b	In mobiler Versorgung mit <u>GesundheitsID</u>: bspw. Haus-/Heimbesuch Ein Versicherter möchte eine Versorgung außerhalb einer LEIder Räumlichkeiten eines Telematik-ID-Inhabers in Anspruch nehmen. Dazu kommt das Personal der LEIdes eines Telematik-ID-Inhabers zum Versicherten. Die LEIDer Inhaber der Telematik-ID benötigt für den Zugriff auf die Daten des physisch anwesenden Versicherten einen Nachweis des Versorgungskontexts. Dazu startet der Versichertedie VER den Online -Check-in-Prozess in einer Kassen-App mit integriertem PoPP-Modul, scannt den von der LEIvom Telematik-ID-Inhaber für den Check-in bereitgestellten QR-Code, bestätigt die LEINutzung der Daten durch den Inhaber der Telematik-ID und authentifiziert sich anschließend mittels GesundheitsID. Nachdem der Versichertedie VER den Online -Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und die LEIdas PS des Telematik-ID-Inhabers erhält im PSden notwendigen Nachweis des Versorgungskontexts.
UC_PoPP_3a	In Fernversorgung mit <u>GesundheitsID</u>: bspw. Videosprechstunde <i>Online -Check-in über Krankenversicherungs-App oder DrittanbieterKassen-App mit PoPP-Modul</i> Ein Versicherter möchte virtuell eine Versorgung durch den Inhaber einer LEITelematik-ID in Anspruch nehmen. Die LEIDer Inhaber der Telematik-ID benötigt für den Zugriff auf die Daten des Versicherten den Nachweis des Versorgungskontexts. Dazu startet der Versichertedie VER zuvor den Online -Check-in-Vorgang in einer der Kassen-App mit integriertem PoPP-Modul, bestätigt die LEINutzung der Daten durch den Inhaber der Telematik-ID und authentifiziert sich anschließend mittels GesundheitsID. Nachdem der Versichertedie VER den Online -Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und die LEIdas PS des Telematik-ID-Inhabers erhält im PSden notwendigen Nachweis des Versorgungskontexts.

ID	Anwendungsfälle
UC_PoPP_3b	In Fernversorgung mit <u>GesundheitsID</u>: bspw. Videosprechstunde <i>Online -Check-in über DrittanbieterAnbieter-App, die das PoPP-Modul einer Krankenversicherungs-App nachnutzt (App2App)</i> Ein Versicherter möchte virtuell eine Versorgung durch den Inhaber einer LEITelematik-ID in Anspruch nehmen. Die LEIDer Inhaber der Telematik-ID benötigt für den Zugriff auf die Daten des Versicherten den Nachweis des Versorgungskontexts. Dazu startet der Versichertedie VER zuvor den Online -Check-in-Vorgang Prozess in einer Anbieter-App ohne integriertes PoPP-Modul. Anschließend öffnet sich die Kasen-App der Krankenversicherung-mit PoPP-Modul, der Versichertebestätigt die LEIdie VERbestätigt die Nutzung der Daten durch den Inhaber der Telematik-ID und authentifiziert sich mittels GesundheitsID. Nachdem der Versichertedie VER den Online -Check-in -Prozess durchgeführt hat, ist dieser abgeschlossen und die LEIdas PS des Telematik-ID-Inhabers erhält im PSden notwendigen Nachweis des Versorgungskontexts.
UC_PoPP_3e	In Fernversorgung mit <u>eGK</u>: bspw. Videosprechstunde <i>Online-Check-in über Krankenversicherungs-App oder Drittanbieter-App mit PoPP-Modul</i> 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.
UC_PoPP_3d	In Fernversorgung mit <u>eGK</u>: bspw. Videosprechstunde <i>Online-Check-in über Drittanbieter-App, die PoPP-Modul einer Krankenversicherungs-App nachnutzt (App2App)</i> 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.

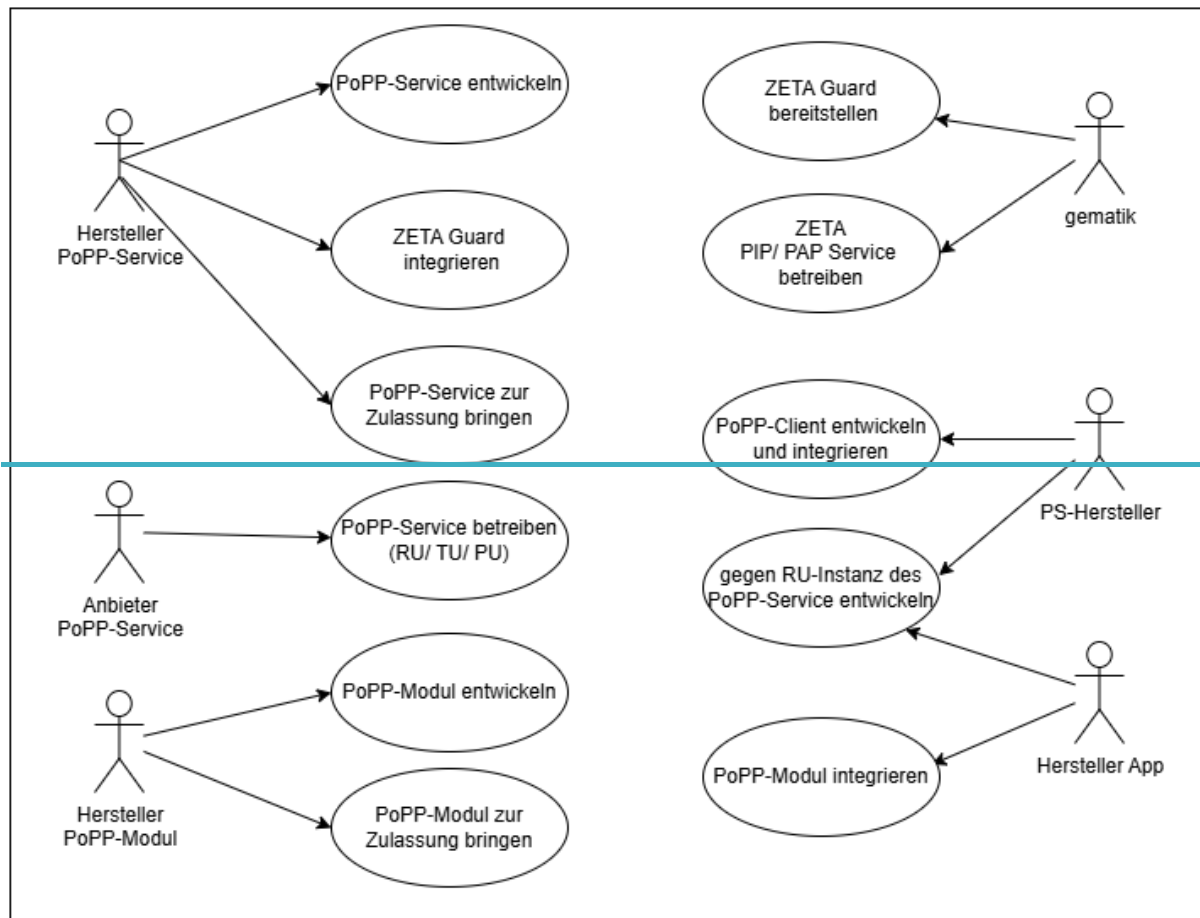
Hinweis: Das vom PoPP-Service erstellte PoPP-Token enthält die Information, mit welcher Methode (siehe proofMethod im Kapitel "PoPP-Token-Erstellung") der Versorgungskontext nachgewiesen wurde. Somit ist es den PoPP-Token nutzenden Anwendungen und

*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



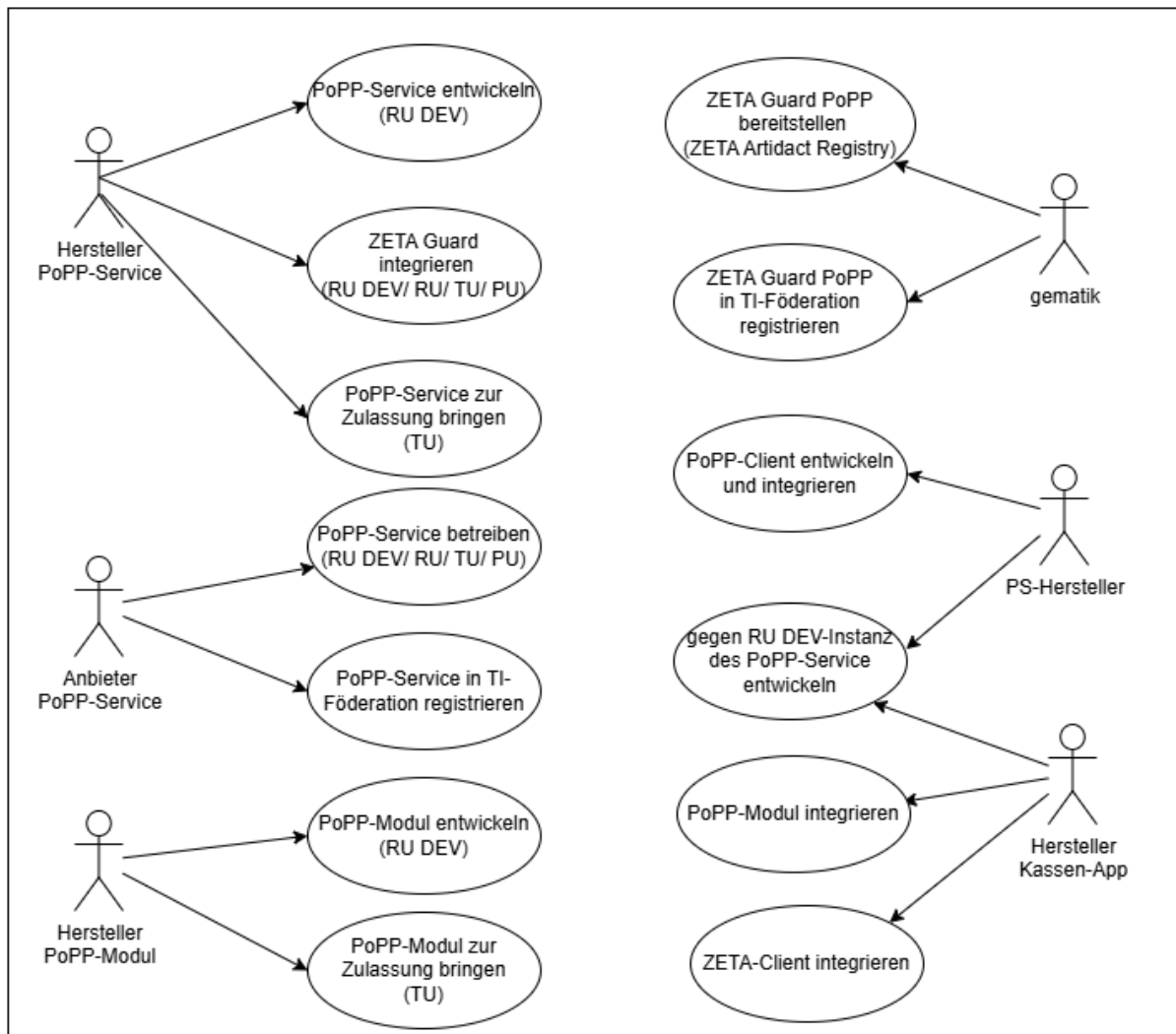


Abbildung 1: Rollen und Akteure bei Herstellung und Betrieb des PoPP-Service

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-VER~~ mit dem PoPP-Service interagieren und das für den Online -Check-in verwendet wird. Das PoPP-Modul ~~kann-ist bei Verwendung der GesundheitsID als Modul in einer Krankenversicherungs-App oder in einer DrittanbieterKassen-App integriert sein. Je nach Ausprägung sind Anforderungen an.~~ Das PoPP-Modul ~~zu erfüllen~~ erfüllt die Anforderungen in [gemSpec_PoPP_Modul].

Der Hersteller PoPP-Modul erwirkt eine Produktzulassung für sein PoPP-Modul.

4.1.3.2 [gemSpec_PoPP_Service#2.3.1.7]: Hersteller App

~~App~~-Hersteller ~~von Kassen-Apps~~ integrieren das PoPP-Modul ~~eines PoPPin die Anwendung, welche auch das Authenticator-Modul~~ ~~Herstellers für einen Online-Check-in-Prozess~~ des sektoralen IDP bereitstellt. Sie entwickeln Funktionalität für die

Unterstützung des Online -Check-ins. Sie nutzen den PoPP-Service in der RU, um die Funktionalität zu testen. Sie registrieren jede App-Version bei der gematik, damit die ~~entsprechenden Attestierungsdaten im ZETA hinterlegt werden können~~ gematik in der Lage ist die entsprechenden Attestierungsdaten in der ZETA Client Registrierung des ZETA Guard zu hinterlegen.

4.1.4 [gemSpec_PoPP_Service#3]: Systemkontext PoPP-Service

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

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

4.1.5 [gemSpec_PoPP_Service#3.1]: Produktzerlegung und Außenschnittstellen

Das Produkt PoPP-Service besteht aus mehreren Komponenten. Die Komponenten für die Erstellung des PoPP-Token sind im Produkttyp PoPP-Service zusammengefasst. Die Kommunikation zwischen ~~LEI~~dem Primärsystem des Inhabers einer Telematik-ID und dem PoPP-Service Resource Server wird durch einen ZETA Guard abgesichert. Die Kommunikation für den Online -Check-in zwischen einem Versicherten und dem PoPP-Service Resource Server erfolgt über ein PoPP-Modul und ZETA Client ~~welche~~ welche bei Verwendung der GesundheitsID in einer Kassen-App auf dem ~~Gerät~~ Smartphone des Versicherten integriert ~~sein müssen~~ sind.

Der Produkttyp PoPP-Service besteht aus mehreren Komponenten, die unterschiedliche Aufgaben erfüllen.

Für die Bearbeitung von ~~Token~~ Requests, bei denen die elektronische Gesundheitskarte (eGK) verwendet wird, ~~gehören dazu~~ sind dies die Komponenten "eGK-Kommunikation, ~~die~~-" und "eGK-Hash-Datenbank ~~sowie Funktionen zur Unterstützung kontaktlos angebundener eGK-~~".

Für ~~Fälle~~ die Bearbeitung von Online Check-In Requests, in denen ~~Versicherte~~ VER die GesundheitsID nutzen, wird die Komponente "Online -Check-in - gID-~~& eGK in Fernversorgung~~" genutzt.

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

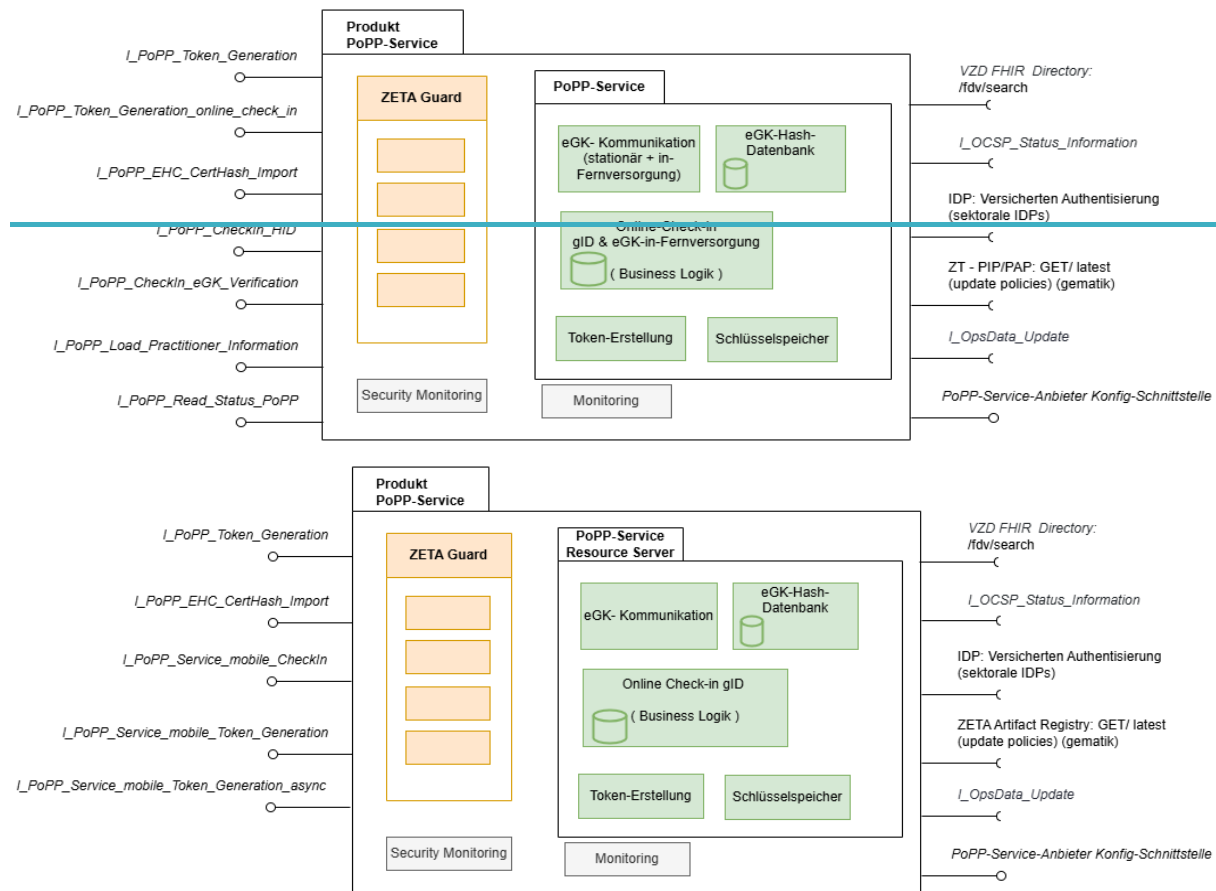


Abbildung 2: Produkttypzerlegung PoPP-Service

Der PoPP-Service stellt folgende Außenschnittstellen bereit:

1. **I_PoPP-Token-Generation** wird vom Primärsystem einer Telematik-ID Inhabers beim Stecken einer eGK verwendet, um vom PoPP-Service einen PoPP-Token zu erlangen.
2. **I_PoPP_EHC_CertHash_Import** wird von Lieferanten aufgerufen und dient der Befüllung der eGK-Hash-Datenbank.
- 2-3. **I_PoPP_Service_mobile_CheckIn-HID** wird vom PoPP-Modul in der APP auf dem Gerät Smartphone des Versicherten verwendet. Der PoPP-Service erstellt nach einer Authentifizierung des Versicherten mit seiner GesundheitsID einen PoPP-Token. Die Schnittstelle beinhaltet die Aufrufe
 - **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.
 - a. **I_PoPP_Load_Practitioner_Information** wird vom PoPP-Modul in der APP auf dem Gerät des Versicherten verwendet zur Ermittlung der Informationen zum Inhaber der Telematik-ID. 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.
 - b. zur Erstellung der PoPP-Daten. Der PoPP-Service erstellt nach einer Authentifizierung des Versicherten mit seiner GesundheitsID einen PoPP-Datensatz für die Erstellung eines PoPP-Token. Zusätzlich wird für die Benachrichtigungen zum Status des PoPP-Token Abrufs ein Nachrichten-Datensatz erstellt.
 - c. zur Statusabfrage es PoPP-Token Abrufs.
 - ~~**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.
- 3.4. ~~**I_PoPPService_mobile_Token_Generation_online_check_in**~~ wird vom Primärsystem einer LEI des Inhabers der Telematik-IDs verwendet, um vom PoPP-Service einen alle PoPP-Token abzurufen, zu erlangen nachdem denen ein gültiger unverarbeiteter PoPP-Datensatz aus einem Online-Check-in durch einen Nutzer stattgefunden hat, im PoPP-Service vorhanden ist.
5. **I_PoPP_Service_mobile_Token_Generation_async**: WebSocket-Schnittstelle für den Abruf und die Zustellung von PoPP-Token an PoPP-Clients.

Der PoPP-Service benutzt die folgenden Schnittstellen:

1. **ZETA PIP/PAPArtifact Registry**: 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].
2. **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.
3. **I_OpsData_Update**:
Wird vom PoPP-Service für die Lieferung von Betriebsdaten verwendet.
4. **VZD FHIR Directory: /fdv/search**
Wird vom PoPP-Service für die Ermittlung der Informationen ~~zum~~ **Inhaber** einer ~~LEI~~ **Telematik-ID** für eine bestimmte Telematik-ID oder bestimmte Suchkriterien ~~zum~~ **Inhaber** einer ~~LEI~~ **Telematik-ID** 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:

1. **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.

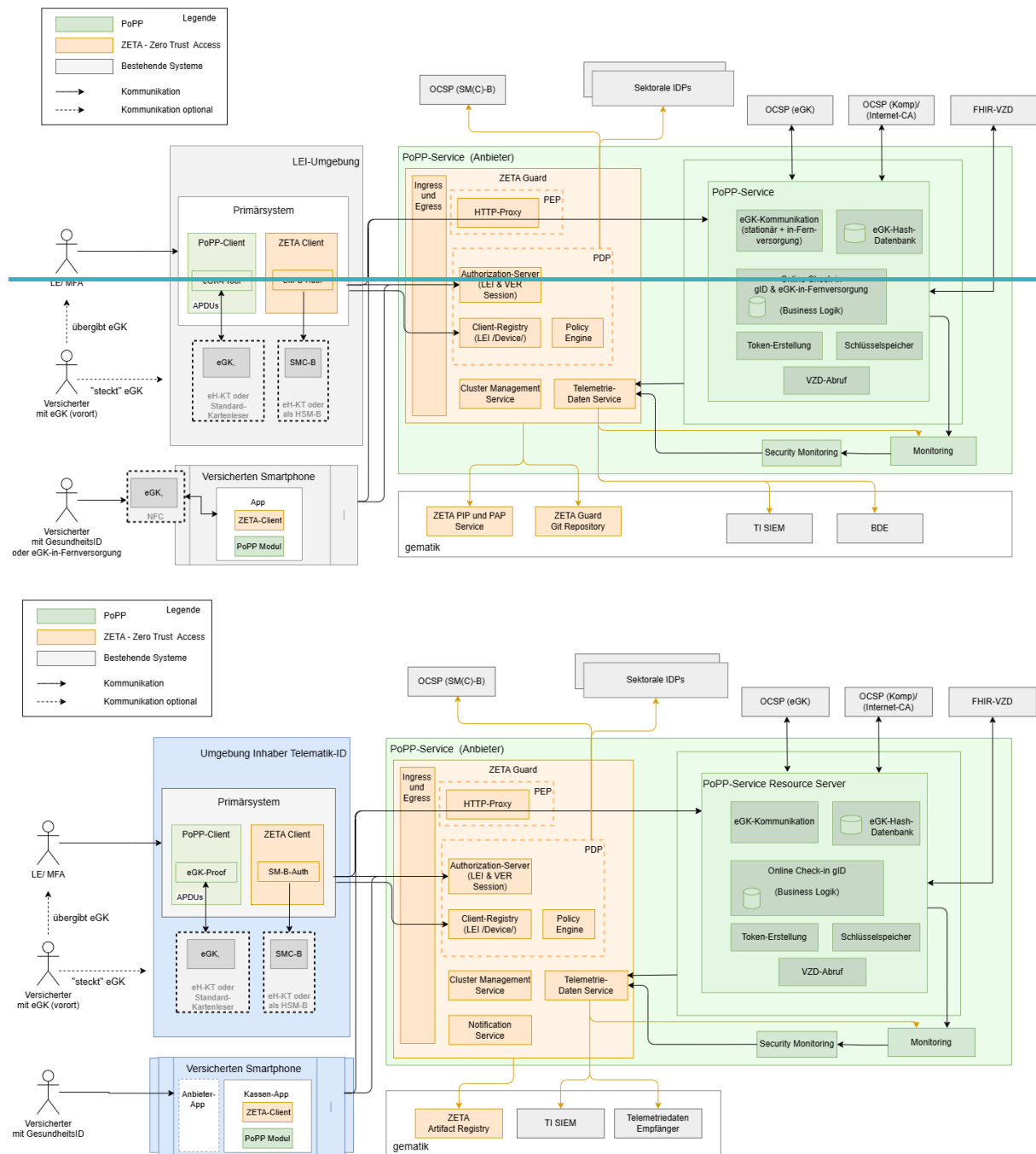


Abbildung 3: Systemkontext PoPP-Service

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.

grün dargestellt. Dargestellt sind zusätzlich heute bereits vorhandene und genutzte Komponenten und Dienste, die für die Nutzerauthentisierung (bspw. IDP) ~~bzw. oder~~ für die Betriebsüberwachung (~~bspw. mittels Betriebsdatenerfassung – kurz BDE~~) der gematik 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~~ der Inhaber einer Telematik-ID 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- ~~Resource Server~~. 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 3: Kurzbeschreibung der Komponenten in der PoPP-Lösung

Komponente	Kurzbeschreibung	Anforderungen
PoPP-Service	Der PoPP-Service umfasst folgende Komponenten der PoPP-Lösung: • ZETA Guard • PoPP-Service-Resource Server	

Komponente	Kurzbeschreibung	Anforderungen
ZETA Guard	Der Zero Trust Cluster ZETA Guard schützt die Kommunikation zwischen dem PoPP-Service Resource Server und den PoPP-Clients im Primärsystem des Inhabers der LEI Telematik-ID sowie die Kommunikation der Versicherten zwischen PoPP-Modul und PoPP-Service-Resource Server. Die Authentifizierung des Inhabers der LEI Telematik-ID erfolgt mittels SM(C)-B. Für die Kommunikation des PoPP-Modul mit dem PoPP-Service Resource Server stellt ZETA Guard ein Client Access Token auf Basis der Geräte- und App-Attestation aus der ZETA Client Registrierung aus. Für Nachrichten des PoPP-Service Resource Server an die PoPP-Module über Push-Notifications stellt ZETA Guard einen Notification Service zur Vefügung.	[gemSpec_ZETA]

Komponente	Kurzbeschreibung	Anforderungen
PoPP-Service <i>Resource Server</i>	Der PoPP-Service enthält die eigentliche Businesslogik des PoPP-Service für das Ausstellen von PoPP- Token an LEI- Systeme das Primärsystem eines Telematik-ID- Inhabers.	
eGK-Kartenkommunikation Kommunikation	In der Komponente eGK- Kartenkommunikation n enthält die Funktionalitäten für die Token-Erstellung in den Fällen enthalten, wenn ein Versicherter mittels seiner eGK beteiligt istfalls VER ihre eGK zur Authentisierung nutzen.	
eGK-Hash-DB Datenbank	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.	

Komponente	Kurzbeschreibung	Anforderungen
Token-Erstellung	Die Komponente Token-Erstellung enthält die Funktionalität zum Erstellen des PoPP-Token; hier werden die Daten von der LEI des Telematik-ID Inhabers 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 zum Inhaber einer LEI Telematik-ID. 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}[gemSpec_Perf]

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)[gemSpec_Perf]
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-Service.	[gemSpec_ZETA]
PoPP-Client	Der PoPP-Client ist der direkte Kommunikationspartner des PoPP-Service im PS des Inhabers einer LEI Telematik-ID.	[gemILF_PoPP_Client]
App	App ist eine Krankenversicherungskassen-App oder DrittanbieterAnbieter-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 Resource Server.	[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:

1. ~~Sektoraler IDP~~~~Sektorale IDPs~~:
verantwortlich für die Authentisierung eines Versicherten mit GesundheitsID,
2. FHIR-VZD:
im Internet verfügbar zum Abruf von ~~Informationen~~~~Informationen~~zum Inhaber einer ~~LEI~~~~Telematik-ID~~,
3. ~~OCSP-Responder des TSP für~~ (SM(C)-B):
im Internet verfügbar für die OCSP-Prüfung von SM(C)-B durch den ZETA Guard,
4. ~~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~~:OCSP (Komp)/(Internet CA):
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,
5. ~~OCSP-Responder Internet CA~~:
~~im Internet verfügbar~~ sowie für die OCSP-Prüfung des TLS-Internet-Zertifikats des PoPP-Service (für die Client-Schnittstelle),
6. Die gematik stellt folgende Dienste bereit:
~~PIP und PAP Service für Zero Trust~~, Git "ZETA Artifact Registry" als Repository für die ZETA Guard Images, ~~Überwachung und Betriebsdatenerfassung~~: BDEden "Telemetriedaten Empfänger" und Telematikinfrastruktur Security Information and Event Management (TI-SIEM).

Die für PoPP erforderlichen OCSP-Responder (~~eGK~~, SM(C)-B, ~~Komponenten PKI~~~~eGK~~, Komp, 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~~~~Service~~" sind folgende nutzende Systeme nicht dargestellt:

1. 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~~ konkret:
 - a. VSDM 2.0,
 - b. ePA für alle,
 - c. E-Rezept.
2. ~~TSP für eGK~~Lieferanten, 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 ~~verortet~~ vor-ort in ~~der LEI~~den Räumlichkeiten des Telematik-ID-Inhabers, in der Ausstellung eines PoPP-Token für die ~~LEI~~den Inhaber einer Telematik-ID.

Neben der Erstellung eines PoPP-Token wird auch die Registrierung [des Primärsystems](#) und Anmeldung [des Inhabers](#) der [LEI-Telematik-ID](#) 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.

1. Anwendungsfall AF_10402* zur Authentisierung [des Inhabers](#) einer [LEI-Telematik-ID](#):
 - a. AF_10402* ist immer Voraussetzung für die Ausgabe eines PoPP-Token
2. Anwendungsfälle, ~~wie sich ein zur Authentisierung Versicherter für die Ausstellung des PoPP-Token authentisiert:~~
 - a. AF_10393* - PoPP-Token mittels eGK im eH-KT
 - b. AF_10387* - PoPP-Token mittels eGK im Standard-Kartenterminal
 - c. AF_10386* - Online -Check-in mit GesundheitsID
 - ◆ ~~AF_10389* - Online Check-in mit eGK~~
3. Anwendungsfälle, ~~die beschreiben, wie die zur Ausgabe eines PoPP-Token~~ Tokens an das PS ~~einer LEI erfolgte~~ eines Telematik-ID-Inhabers:
 - a. AF_10393* - PoPP-Token mittels eGK im eH-KT
 - b. AF_10387* - PoPP-Token mittels eGK im Standard-Kartenterminal
 - c. AF_10390* - PoPP-Token Erstellung bei Online -Check-in

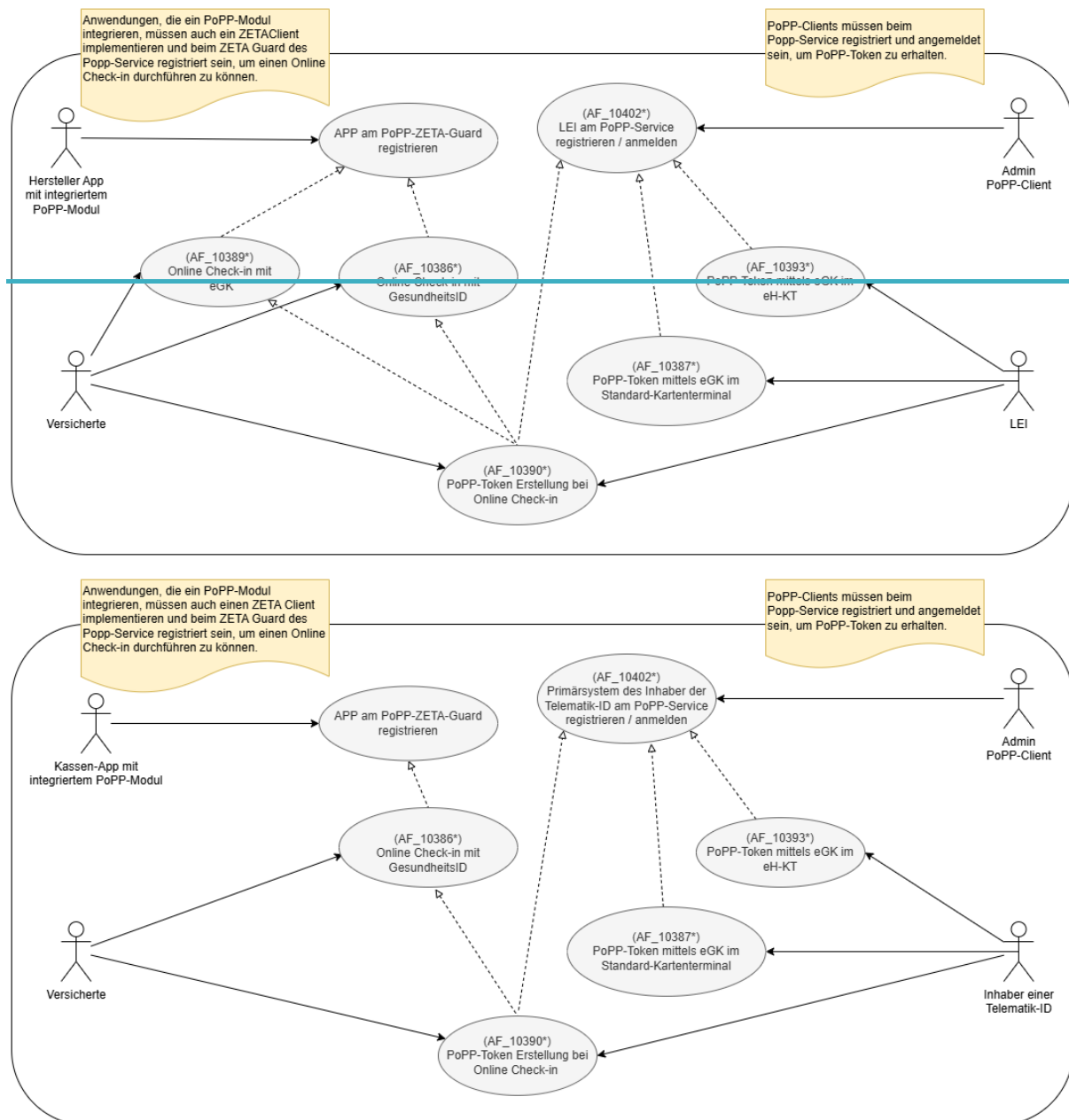


Abbildung 4: Anwendungsfälle zur Attestierung des Versorgungskontexts

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

Tabelle 4: Zuordnung der Anwendungsfälle zu den Use Cases

Anwendungsfall	Kurzbeschreibung	technische Anwendungsfälle
UC_PoPP_1a	PoPP-Token bei physischer Anwesenheit in beim Inhaber der LEI Telematik-ID / vor Ort-eGK	1. zunächst AF_10402*- LEIPrimärsystem des Inhaber der Telematik-ID 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_1b	PoPP-Token bei physischer Anwesenheit in beim Inhaber der LEI Telematik-ID / vor Ort - GesundheitsID	1. zunächst AF_10402*- LEIPrimärsystem des Inhaber der Telematik-ID 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_2a	PoPP-Token bei physischer Anwesenheit außerhalb der LEI Umgebung des Inhabers der Telematik-ID / Hausbesuch - eGK	Identisch zu UC_PoPP_1a 1.- zunächst AF_10402*-LEI am PoPP-Service registrieren/ anmelden und dann 2.- entweder AF_10393*- PoPP-Token mittels eGK im eH-KT oder AF_10387*- PoPP-Token mittels eGK im Standard-Kartenleser
UC_PoPP_2b	PoPP-Token bei physischer Anwesenheit außerhalb der LEI Umgebung des Inhabers der Telematik-ID / Hausbesuch - GesundheitsID	Identisch zu UC_PoPP_1b 1.- zunächst AF_10402*-LEI am PoPP-Service registrieren/ anmelden und dann 2.- AF_10386*- Online-Check in mit GesundheitsID, dann AF_10390*- PoPP-Token-Erstellung bei Online-Check in

Anwendungsfall	Kurzbeschreibung	technische Anwendungsfälle
UC_PoPP_3a	PoPP-Token ohne physische Anwesenheit in beim Inhaber der LEI/ in Fernversorgung-Telematik-ID / GesundheitsID - Check-in mit Drittanbieter Anbieter-App oder Browser-Anwendung	1.- zunächst AF_10402* - LEI am PoPP-Service registrieren/ anmelden und dann 2.- AF_10386* - Online-Check-in mit GesundheitsID, dann AF_10390* - PoPP-Token-Erstellung bei Online-Check-in-Identisch zu UC_PoPP_1b
UC_PoPP_3b	PoPP-Token ohne physische Anwesenheit in beim Inhaber der LEI/ in Fernversorgung-Telematik-ID / GesundheitsID - Check-in mit KrankenversicherungsKassen- App	Identisch zu UC_PoPP_3a, 1.- zunächst AF_10402* - LEI am PoPP-Service registrieren/ anmelden und dann 2.- AF_10386* - Online-Check-in mit 1bGesundheitsID, dann 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	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 Fernversorgung - eGK in Fernversorgung - Check-in mit Krankenversicherungs-App	Identisch zu UC_PoPP_3c 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 [gemSpec_PoPP_Service#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~~ **den Inhaber einer Telematik-ID** im PoPP-Service **Resource Server** initiiert.

Starten ~~die Versicherten~~ **VER** den Check-in-Prozess über das in eine **Kassen-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 **Kassen-App** integrierte PoPP-Modul ist eine Auswahl ~~der des Inhabers einer Telematik-ID einer LEI~~ für den Online ~~-~~Check-in möglich. Die Auswahl ~~der LEI des Inhabers einer Telematik-ID~~ kann über das Auswerten ~~des von der LEI eines~~ 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~~ **zum Inhaber einer Telematik-ID an das PoPP-Modul** zu ermitteln.

Nach erfolgreicher Authentisierung der ~~VER Versicherten~~ mit GesundheitsID ~~oder Authentifizierung der eGK in Fernversorgung~~ wird vom PoPP-Service **Resource Server** ein Datensatz zur Erstellung eines PoPP-Token erzeugt. Ist ~~das Primärsystem des betroffenen LEI Inhabers der Telematik-ID~~ online (d.h. sie ist zu dem Zeitpunkt authentifiziert), so wird das PoPP-Token erstellt und ~~der LEI dem Primärsystem~~ zugestellt. Ist ~~die LEI das Primärsystem des Inhabers der Telematik-ID~~ nicht online, so wird das PoPP-Token erstellt und zugestellt, sobald ~~dieses~~ online ist ~~und PoPP-Token abfragt~~. Spätestens nach einem festgelegten Zeitraum (72h) wird der aus dem Online ~~-~~Check-in erstellte Datensatz vom PoPP-Service **Resource Server** gelöscht.

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

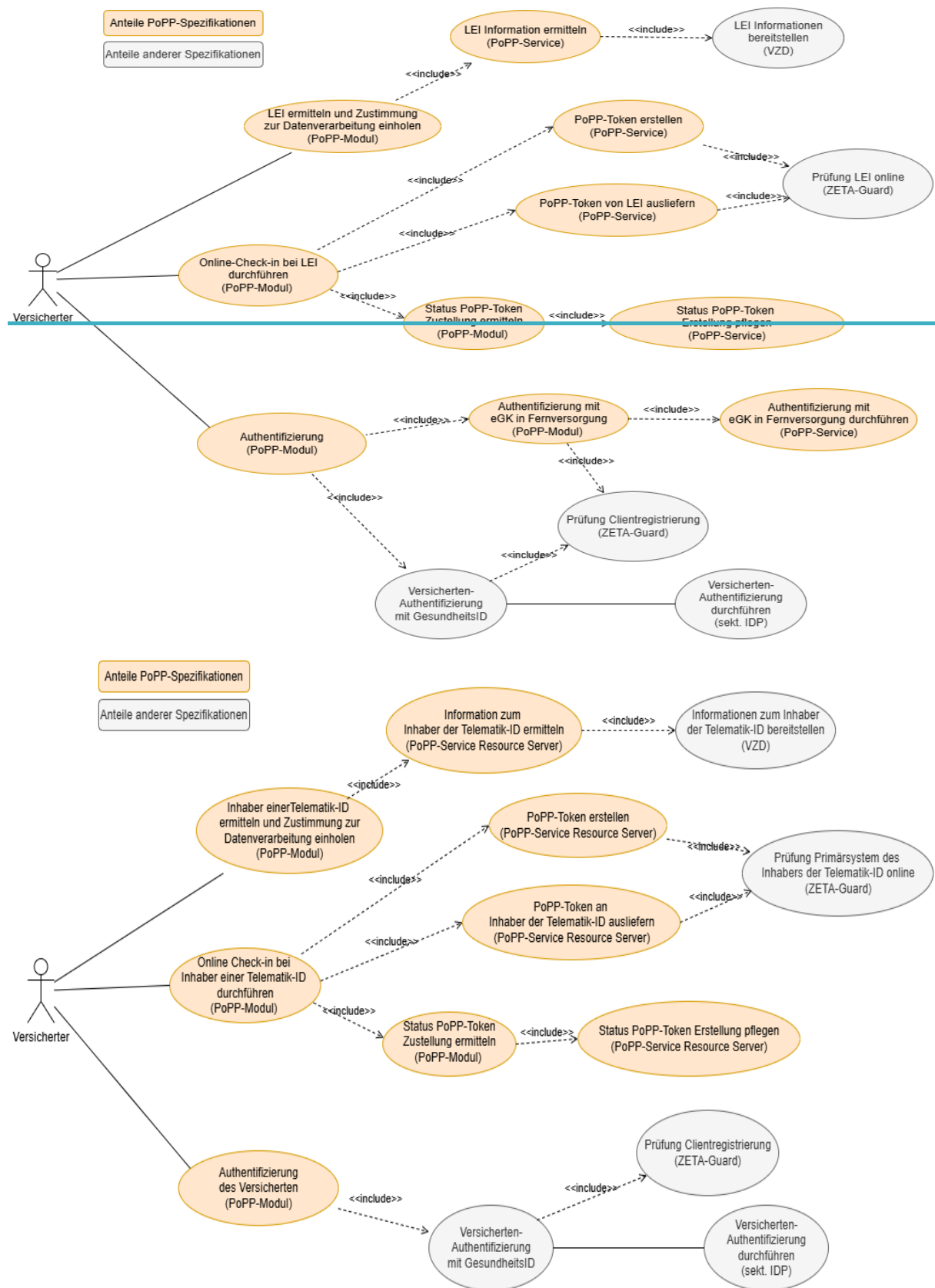


Abbildung 5: Use-Case-Übersicht Online –Check-in aus einer App mit integriertem PoPP-Modul

Tabelle 5: 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 Die VER startet in mit der Kassen-App mit PoPP-Modul (Krankenversicherungs-App, Drittanbieter-App) über einen Eintrag in der UX GUI den "Online –Check-in" Prozess
" LEI Inhaber der Telematik-ID ermitteln und Zustimmung zur Datenverarbeitung	Der Online –Check-in startet mit der Auswahl einer LEIdes Inhabers der Telematik-ID. Die Auswahl des Inhabers der LEITelematik-ID kann z.B. erfolgen durch: 1. Scannen eines QR-Code durch dendie Versicherten über eine Funktion in der App 2. Darstellen einer Auswahlliste in der App und Auswahl einer LEIdes Inhabers der Telematik-ID durch den Versicherten 3. Visualisierung einereines fest zugeordneten LEIInhabers einer Telematik-ID durch die App Der Versicherte muss zustimmenDie VER stimmt zu, dass seine KVNR an die LEIdem Inhaber der Telematik-ID übermittelt werden darfwird.
" LEI Information zum Inhaber der Telematik-ID ermitteln"	Die Prüfung einer Telematik-ID und die Ermittlung der Informationen zu einer LEI zum Inhaber der Telematik-ID (Name, Adresse, ..) wird durch den PoPP-Service Resource Server über eine Abfrage am VZD durchgeführt.

Anwendungsfall Online -Check-in App mit PoPP-Modul	Kurzbeschreibung
"Check-in bei LEI beim Inhaber der Telematik-ID durchführen"	Der Online Check-in umfasst 1. die Erstellung eines PoPP-Datensatzes im PoPP-Service Resource Server mit allen Informationen zur PoPP-Token Erstellung, 2. die Auskunft zum Status der PoPP-Token Erstellung, 3. die Erstellung eines PoPP-Token im PoPP-Service Resource Server, wenn die LEI der Inhaber der Telematik-ID online ist, 4. die Übertragung des PoPP-Token an die LEI des Inhabers der Telematik-ID, wenn dieser online ist 5. Die Auskunft zum Status der PoPP-Token Erstellung.
"Authentifizierung"	Die Authentifizierung kann erfolgen über: • die Authentifizierung des Versicherten über seine GesundheitsID • die Authentifizierung einer eGK (eGK in Fernversorgung) 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. 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.

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

4.1.11 Neues Kapitel 4.5.1: Auswahl einer LEI des Inhabers der Telematik-ID für den Online -Check-in

Die Abläufe zur Auswahl der Telematik-ID einer LEI, einer Suche im FIHR-VZD, der Aufbereitung der LEI-Informationen zum Inhaber der Telematik-ID 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 Neues Kapitel 4.5.1.1: 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 ~~kannist anschließend in der Lage~~ unter Angabe der Client-Credentials Zugangstoken für den Zugang zum FHIR-VZD abrufen. [$\leq$]

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

Der PoPP-Service ~~MUSS mindestens alle 24h das~~DARF Zugangstoken für den Zugang zum FHIR-VZD ~~NICHT verwenden, wenn diese älter als 24 Stunden sind.~~ [$\leq$ erneuern. [$\leq$]

4.1.11.2 Neues Kapitel 4.5.1.2: Ermittlung von Informationen ~~zu einer LEI~~zum Inhaber der Telematik-ID

~~A_28659 -PoPP-Service -Entgegennahme des HTTP-Request zur Ermittlung von Informationen zu einer LEI~~PoPP-Service - Entgegennahme des HTTP-Request zur Ermittlung von Informationen zum Inhaber der Telematik-ID

Der PoPP-Service MUSS eine Schnittstelle gemäß [I_PoPP_Load_Practitioner_InformationService_mobile_CheckIn.yaml] zur Ermittlung von Informationen ~~zuzumInhaber~~ einer ~~LEI~~-Telematik-ID 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 Schnittstellenaufruf zurückzugeben. [$\leq$]

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

A_30076 -Vorhalten VZD-Daten im PoPP-Service

Der PoPP-Service KANN auf den VZD-Abruf nach A_28659* verzichten, wenn die VZD-Daten im PoPP-Service bereits vorliegen (z.B. als VZD-Cache) und nicht älter als 24h sind.

Hinweis: Wird ein Caching von VZD-Daten umgesetzt gilt auch diesbezüglich A_26603. [$\leq$]*

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

~~Ist die~~Dieses Kapitel beschreibt den Online Check-in mit GesundheitsID innerhalb oder außerhalb der Umgebung eines Telematik-ID ~~der LEI-Inhabers~~ bzw. innerhalb oder außerhalb der Räumlichkeiten eines Telematik-ID-Inhabers (bspw. für eine Videosprechstunde).

Wurde die Telematik-ID ermittelt, bei welcher ~~der Versicherte-VER~~ einen Online Check-in durchführen möchte und ~~hat der Versicherte~~ nachdem VER der Datennutzung durch ~~die LEI~~ zugestimmt, so kann er den Inhaber der Telematik-ID zustimmte, authentifiziert sich VER mit ~~seiner~~ihrer GesundheitsID ~~authentifizieren~~, um sich ~~innerhalb oder außerhalb einer LEI (bspw. für eine Videosprechstunde)~~ bei einem Inhaber der Telematik-ID anzumelden. (innerhalb oder außerhalb (bspw. für eine Videosprechstunde).

Als Ergebnis einer erfolgreichen Authentifizierung wird im PoPP-Service Resource Server ein Datensatz zur Ausstellung eines PoPP-Token und ein Nachrichtendatensatz zum Status der PoPP-Token Erstellung angelegt. Das PoPP-Token selbst wird erstellt, wenn die LEI der Inhaber der Telematik-ID sich beim PoPP-Service authentifiziert hat und das PoPP-Token abrufen. Der Status zur PoPP-Token-Erstellung wird dem Versicherten präsentiert.

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

AF_10386-01 - ~~Online-Check-in mit GesundheitsID~~ Online Check-in mit
GesundheitsID

Attribute	Bemerkung
-----------	-----------

Beschreibung	Ist Zunächst wird die Telematik-ID der LEI ermittelt, bei welcher der Online -Check-in erfolgen soll, ermittelt und hat der Versicherte geplant ist. Dann stimmt VER der Datennutzung durch die LEI zugestimmt, den Inhaber der Telematik-ID zu. Anschließend bietet das PoPP-Modul dem Versicherten VER diverse Möglichkeiten zur Authentisierung an, über welche die Versichertenidentität verifiziert werden kann. Eine Möglichkeit ist die Authentifizierung mit. Im hier betrachteten Fall wählt VER "GesundheitsID-Bei diesem Verfahren" aus. Dabei wird der Versicherte VER durch den sektoralen IDP seiner Krankenversicherung authentifiziert. Dem Versicherten Der VER stehen dafür unterschiedliche Authentisierungsmittel zur Verfügung [gemSpec_IDP_Sek]. Nach erfolgreicher Authentifizierung durch den sektoralen IDP stellt dieser ein ID-Token aus, welches u.a. unter anderem die KVNR des der authentifizierten Versicherten VER und die IK-Nummer seiner der Krankenkasse enthält. Außerdem liefert das ID-Token Informationen über die Vertrauenswürdigkeit der Authentifizierung (Vertrauensniveau) und über das eingesetzte Authentisierungsmittel. Der für den PoPP-Service bereitgestellte ZETA Guard Authorization-Server des PoPP-Service erstellt daraufhin ein Access-Token für das PoPP-Modul und speichert die folgende Informationen zur späteren Verwendung: 1. KVNR des Versicherten der VER 2. IK-Nummer der Krankenversicherung 3. Vertrauensniveau der durchgeführten Authentifizierung 4. Durchgeführte Authentisierungsmethode ZETA Guard übermittelt das Access-Token an den ZETA Client im Smartphone der VER worauf der eigentliche Request für den Online Check-in über den ZETA Guard HTTP-Proxy am PoPP-Service Resource-Server erfolgt. Der PoPP-Service Resource Server erstellt in diesem Aufruf einen Nachrichten-Datensatz mit 1. dem Status der PoPP-Token-Generierung 2. einer eindeutigen ID für die Zuordnung einen PoPP-Datensatzes Der PoPP-Service Resource Server erstellt in diesem Aufruf des weiteren einen PoPP-Datensatz mit 1. KVNR des Versicherten der VER - diese wurde im Request durch den ZETA Guard HTTP-Proxy als Headerattribut ergänzt 2. IK-Nummer der Krankenversicherung - diese wurde im Request durch den ZETA Guard HTTP-Proxy als Headerattribut ergänzt
---------------------	---

Attribute	Bemerkung
	3. Durchgeführte Authentisierungsmethode (amr) - diese wurde im Request durch den ZETA Guard HTTP-Proxy als Headerattribut ergänzt 4. Telematik-ID - Query-Parameter des HTTP-Request 5. WorkplaceID - Query-Parameter des HTTP-Request 6. ID des zugehörigen Nachrichte-Datensatzes und speichert diesen zusammen mit einem Zeitstempel einem eindeutigen Identifier und einer Statusinformation zur PoPP-Token-Erstellung.
Vorbedingungen	1. Der VersicherteVER hat einer Datennutzung (KVNR) durch die LEIden Inhaber der Telematik-ID zugestimmt. 2. Im PoPP-Modul wurde ein HTTP-Request an den PoPP-Service mit folgenden Query-Parametern formuliert: a. Telematik-ID der LEI(mandatory) b. WorkplaceID (optional) 3. Die Authentifizierung des Versichertender VER mit GesundheitsID wurde von den ZETA-Komponenten und den Komponenten des sektoralen IDP seiner Krankenversicherung erfolgreich durchgeführt. a. Zum Zeitpunkt der Authentisierung des Versichertender VER muss dieser einen Internetzugang haben. b. Der VersicherteVER verwendet eine Kassen-App mit integrierten PoPP-Modul und ZETA Client. c. Gerät und Kassen-App sind in der ZETA Guard Client-Registry registriert. d. Die GesundheitsID ist für den Versichertendie VER im sektoralen IDP seiner Krankenversicherung eingerichtet und der VersicherteVER kann sich über sein Smartphone gegenüber dem sektoralen IDP seiner Krankenversicherung authentifizieren. 4. Der ZETA Guard HTTP-Proxy hat den PoPP-Service Resource Serve aufgerufen mit a. dem vom PoPP-Modul erstellten HTTP-Reguest a. demden im vom ZETA-Guard ausgestellten Access-Token b. den zum Access-Token gespeicherten Informationen c. den Informationen zum aufrufenden Client

Ablauf	1. Der PoPP-Service Resource Server nimmt den HTTP-Request vom ZETA Guard HTTP-Proxy entgegen. 2. Der PoPP-Service Resource Server extrahiert a. KVNR des Versicherten VER (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 f. client_id (mandatory) - aus dem Header des HTTP-Request 1. Der PoPP-Service erzeugt Resource Server prüft, ob für die KVNR und speichert einen Telematik-ID bereits ein PoPP-Datensatz mit extrahierten Daten (KVNR, IK-Nummer, Telematik-ID, WorkplaceID) existiert und der zugehörige Nachrichten-Datensatz den Status "pending" hat. Ist dies der erzeugten proofMethod=" und einem aktuellen Zeitstempel. 3. Fall antwortet der PoPP-Service Resource Server dem eingegangenen Request mit der Statusnachricht "pending". Der Ablauf ist beendet, es wird kein weiterer Datensatz angelegt. 3.4. Existiert noch kein PoPP-Datensatz zu KVNR und Telematik-ID erstellt und speichert der PoPP-Service Resource Server einen Nachrichten-Datensatz zum Status der PoPP-Token-Erstellung mit a. id- eindeutiger Identifier zur Identifikation der Nachricht bei asynchronem Abruf b. status - repräsentiert den Status der PoPP-Token-Erstellung (<i>success, pending, cancelled canceled</i>). Bei Erstellung ist der status immer "pending". a. message enthält Detailinformationen zu Status c. client_id- ID des anfragenden Clients für späteren Abgleich bei Statusabfragen 5. Der PoPP-Service Resource Server erzeugt und speichert einen PoPP-Datensatz mit extrahierten Daten (KVNR, IK-Nummer, Telematik-ID, WorkplaceID), der erzeugten proofMethod=" und einem aktuellen Zeitstempel. 4.6. Der PoPP-Service Resource Server speichert den Identifier (id) der Nachricht des Nachrichten-Datensatz
--------	---

Attribute	Bemerkung
	zum Status der PoPP-Token-Erstellung zusätzlich im PoPP-Datensatz. 5.7. Der PoPP-Service Resource Server hat den eingegangenen Request mit der Statusnachricht zur PoPP-Token-Erstellung beantwortet
Nachbedingung	1. Erfolgsfall a. Der PoPP-Service Resource Server hat einen PoPP-Datensatz mit allen Daten angelegt, die zur Erstellung eines PoPP-Token notwendig sind. b. Der PoPP-Service Resource Server hat einen Nachrichten-Datensatz zum Status der PoPP-Token-Erstellung angelegt. - b.c. Der PoPP-Service Resource Server hat dem ZETA Guard HTTP-Proxy mit HTTP-200201 und der Statusnachricht zur PoPP-Token-Erstellung geantwortet. 2. Fehlerfall ◆ Es ist ein Fehler aufgetreten a. Der PoPP-Service Resource Server hat dem ZETA Guard HTTP-Proxy mit einem Fehler Code und der Statusnachricht zur PoPP-Token-Erstellung geantwortet.

Akzeptanzkriterien	1.  ML-184424 - AF 10386 - Bereitsstellung einer Schnittstelle für die Erzeugung eines PoPP-Token nach Authentifizierung mit GesundheitsID a. Der PoPP-Service Resource Server 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. b. Der PoPP-ServiceServiceResource Server hat geantwortet mit einem i. HTTP-200 (OK)201 (CREATED), wenn die Bearbeitung des Requests fehlerfrei abgearbeitetabgearbeitet werden konnte ii. HTTP-400 (Bad Request}),}), wenn nicht alle mandatory Attribute extrahiert werden konnten iii. HTTP-500 in allen anderen FehlerfällenFehlerfällen 2.  ML-198839 - AF 10386 - Prüfung auf bereits bestehenden PoPP-Datensatz 2-3.  ML-184338 - AF 10386 - Erstellung und Speicherung PoPP-Datensatz GesundheitsID a. Der PoPP-Service Resource Server hat einen PoPP-Datensatz angelegt, bestehend aus i. KVNR des Versichertender VER ii. IK-Nummer der Krankenversicherung iii. Telematik-IDder LEI iv. WorkplaceIDder LEI v. proofMethod="" vi. Zeitstempel vii. Identifier der Nachricht zur PoPP-Token-Generierung 3-4.  ML-184339 - AF 10386-10389 - Erstellung und Speicherung eines Nachrichten-Datensatz a. Der PoPP-Service Resource Server hat einen Nachrichten-Datensatz mit der Nachricht zum Status der PoPP-Token-Generierung angelegt, bestehend aus i. Identifier der Nachricht ii. Status der PoPP-Token-Generierung ◆ Message zum PoPP-Token-Status iii. client_id des anfragenden Clients 4-5.  ML-185491 - AF 10386 - Response an ZETA Guard HTTP-Proxy zum eingegangenen Request
--------------------	---

Attribute	Bemerkung
	a. Der PoPP-Service Resource Server hat den eingegangenen Request mit der Statusnachricht zur PoPP-Token-Erstellung beantwortet i. "success", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token erstellt und dem Inhaber der LEITelematik-ID zugestellt wurde. ii. "pending", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token noch nicht erstellt und dem Inhaber der LEITelematik-ID zugestellt wurde iii. "cancelledcanceled", wenn der Inhaber der Telematik-ID den PoPP-Token nicht innerhalb von 72h abgeholt hat oder wenn ein Fehler aufgetreten ist. message mit Informationen im Initial ist der Status immer "pending". Fehlerfall
Fehlerfälle	1. Die Prüfung-GerätGeräte- und/oder App-Prüfung durch ZETA ist fehlgeschlagen. 2. Die Prüfung der übergebenübergebenen Parameter zum AnlagenAnlegen des PoPP-Datensatzes ist fehlgeschlagen. 3. Die Authentifizierung des Nutzers über ZETA und sektoralensektorale IDP ist fehlgeschlagen. 4. Das Anlegen des Datensatzes im PoPP-Service Resource Server ist fehlgeschlagen.
Alternativen	Alternativ zur GesundheitsID kann der Versicherte den Versorgungskontext mit seiner eGK (eGK in Fernversorgung) attestieren.

[<=]

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

Der PoPP-Service implementiert eine Schnittstelle gemäß [I_PoPP_Service_mobile_CheckIn-~~HID~~.yaml] für die Entgegennahme eines HTTP-Requests zur Erzeugung eines PoPP-Token, nachdem ~~der Versicherte~~**VER** über seine GesundheitsID authentifiziert wurde.

[<=]

ML-198839 -AF_10386 - Prüfung auf bereits bestehenden PoPP-Datensatz

Der PoPP-Service hat geprüft, ob zur KVNR und Telematik-ID im eingegangenen Request bereits ein PoPP-Datensatz existiert und im dazu gehörenden Nachrichten-Datensatz den

Status auf "pending" gesetzt ist. Ist das der Fall, hat der PoPP-Service auf den eingegangenen Request gemäß [I_PoPP_Service_mobile_CheckIn.yaml] eine Response an den ZETA Guard HTTP-Proxy zurück gesendet und damit den Ablauf beendet. Dabei MUSS der Status in der die Statusnachricht den Wert "pending" enthalten.

[<=]

ML-184338 -AF_10386 - Erstellung und Speicherung PoPP-Datensatz GesundheitsID

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: ^[\^V:]*?"<> }{: ^[\^V:]*?"<> }{1,64}\$
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	Identifizier des Nachrichten Datensatz-Datensatzes zur PoPP-Token-Generierung	UUID

[<=]

ML-184339 ~~AF_10386_10389 - Erstellung und Speicherung eines Nachrichten-Datensatz~~ AF_10386 - Erstellung und Speicherung eines Nachrichten-Datensatz

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 "success" - PoPP-Token wurde erstellt und erfolgreich, dem Primärsystem zugestellt "pending" - PoPP-Datensatz ist angelegt, PoPP-Token wurde noch nicht erstellt "cancelledcanceled" - Erstellung des PoPP-Token wurde abgebrochen	string Wertebereich: ["success", "pending", " cancelled ", "canceled"]
messageclient_id	Detailinformationen zum Status ZETA-Identifier des anfragenden Clients, wie er im HTTP Header vom ZETA Guard PEP http Proxy mitgegeben wird.	String (max. 128 Zeichen) Wertebereich: ^[\ÄÖÜäöüß\w\-\.\&\+*V]{1,128}\$ ZETA-spezifisch

[<=]

Initial ist der Status immer "pending". [<=]

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

Der PoPP-Service hat auf den eingegangenen Request gemäß

[I_PoPP_Service_mobile_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~~ aber das PoPP-Token noch nicht erstellt und ~~der LEI~~ dem Primärsystem zugestellt wurde.

3. "~~cancelled~~canceled", wenn die Erstellung des PoPP-Token abgebrochen wurde.

[<=]

~~Hinweis: Nach der initialen Erstellung des Nachrichten-Datensatzes ein Fehler aufgetreten ist, der Status immer "pending".~~

~~Im Fehlerfall muss die "message" der Statusnachricht Informationen zum aufgetretenen Fehler enthalten.~~

[<=]

A_30107 -PoPP-Service - Unveränderte Datenübernahme und sichere Speicherung (GesundheitsID)

Der PoPP-Service MUSS

- die Telematik-ID und die WorkplaceID (wenn vorhanden) aus dem Request des PoPP-Moduls unverändert übernehmen und im PoPP-Datensatz abspeichern
- die KVNR und IK-Nummer aus dem HTTP Header vom ZETA Guard PEP http Proxy unverändert übernehmen und im PoPP-Datensatz abspeichern
- die client_id aus dem HTTP Header vom ZETA Guard PEP http Proxy unverändert übernehmen und im Nachrichten-Datensatz abspeichern.

Für die Speicherung gilt A_26603*.

Für die Übernahme von Daten von Clients gilt A_26470*.

[<=]

4.1.13 Neues Kapitel 4.5.3: PoPP-Token bei 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 Angang 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 eGKAttribute	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 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 • 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 und speichert diesen zusammen mit einem Zeitstempel einem eindeutigen Identifier und einer Statusinformation zur PoPP-Token Erstellung.

AF_10389-01- Online-Check-in mit-eGKAttribute	Bemerkung
Vorbedingung	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: • 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 a. dem vom PoPP-Modul erstellten HTTP-Request b. dem vom ZETA-Guard ausgestellten Client Access-Token

Ablauf	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 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 APDU Commands entgegen 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. 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 a. KVN-R 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-R, 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 a. id — eindeutiger Identifier zur Identifikation der Nachricht bei asynchronem Abruf b. status — repräsentiert den Status der PoPP Token Erstellung (success, pending, cancelled) c. message — enthält Detailinformationen zu Status
--------	--

Gelöscht

	8. Der PoPP-Service speichert den Identifier (<i>id</i>) der Nachricht zum Status der PoPP-Token-Erstellung im PoPP-Datensatz Der PoPP-Service hat den eingegangenen Request mit der Statusnachricht zur PoPP-Token-Erstellung beantwortet Offener Punkt: OP-PoPP-1 (zusätzliche Push-Notification für PS) <i>Für PoPP Stufe 2 ist noch nicht festgelegt, ob und wie Primärsysteme über neu bereitgestellte PoPP-Token aktiv informiert werden oder diese ausschließlich durch regelmäßige Abrufe ermitteln. Die hierfür notwendigen Festlegungen befinden sich derzeit in Abstimmung.</i> Vorgehen zur Auflösung: <i>Klärung innerhalb der gematik gemeinsam mit den verantwortlichen ZETA-Teams parallel zur Kommentierung. Das Ergebnis wird über einen Eigenkommentar der gematik veröffentlicht und in die Spezifikationen eingearbeitet.</i>
Nachbedingung	• Erfolgsfall • 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 • Der PoPP-Service hat dem ZETA-Guard HTTP-Proxy mit einem Fehler-Code und der Statusnachricht zur PoPP-Token-Erstellung geantwortet

Akzeptanzkriterien	 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 hat den HTTP-Request vom ZETA Guard HTTP-Proxy entgegengenommen und die Zugriffsberechtigung geprüft. - Der PoPP-Service hat geantwortet mit einem - 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 - Der PoPP-Service hat die Daten der eGK ausgelesen und geprüft  ML 184341 AF 10389 Erstellung und Speicherung PoPP-Datensatz eGK in Fernversorgung - Der PoPP-Service hat einen PoPP-Datensatz angelegt bestehend aus - KVNR des Versicherten - IK-Nummer der Krankenversicherung - Telematik-ID der LEI - WorkplaceID der LEI - proofMethod=" - Zeitstempel - Identifizier des Nachrichten-Datensatz zur PoPP-Token-Generierung  ML 184339 AF 10386 10389 Erstellung und Speicherung eines Nachrichten-Datensatz - Der PoPP-Service hat einen Nachrichten-Datensatz mit der Nachricht zum Status der PoPP-Token-Generierung angelegt bestehend aus - Identifizier der Nachricht - Status der PoPP-Token-Generierung - Message zum PoPP-Token-Status
--------------------	---

	• ML 185492 AF 10389 Response an ZETA Guard HTTP Proxy zum eingegangenen Request • 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 • "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	• Die Prüfung Gerät und/oder App durch ZETA ist fehlgeschlagen • Die Prüfung der übergeben Parameter zum Anlagen 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: $\wedge[\wedge\vee:*\?"<>]{64}\$$
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	Identifizier 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 de eGK~~
- ~~nach Abschluss des Auslesen 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.

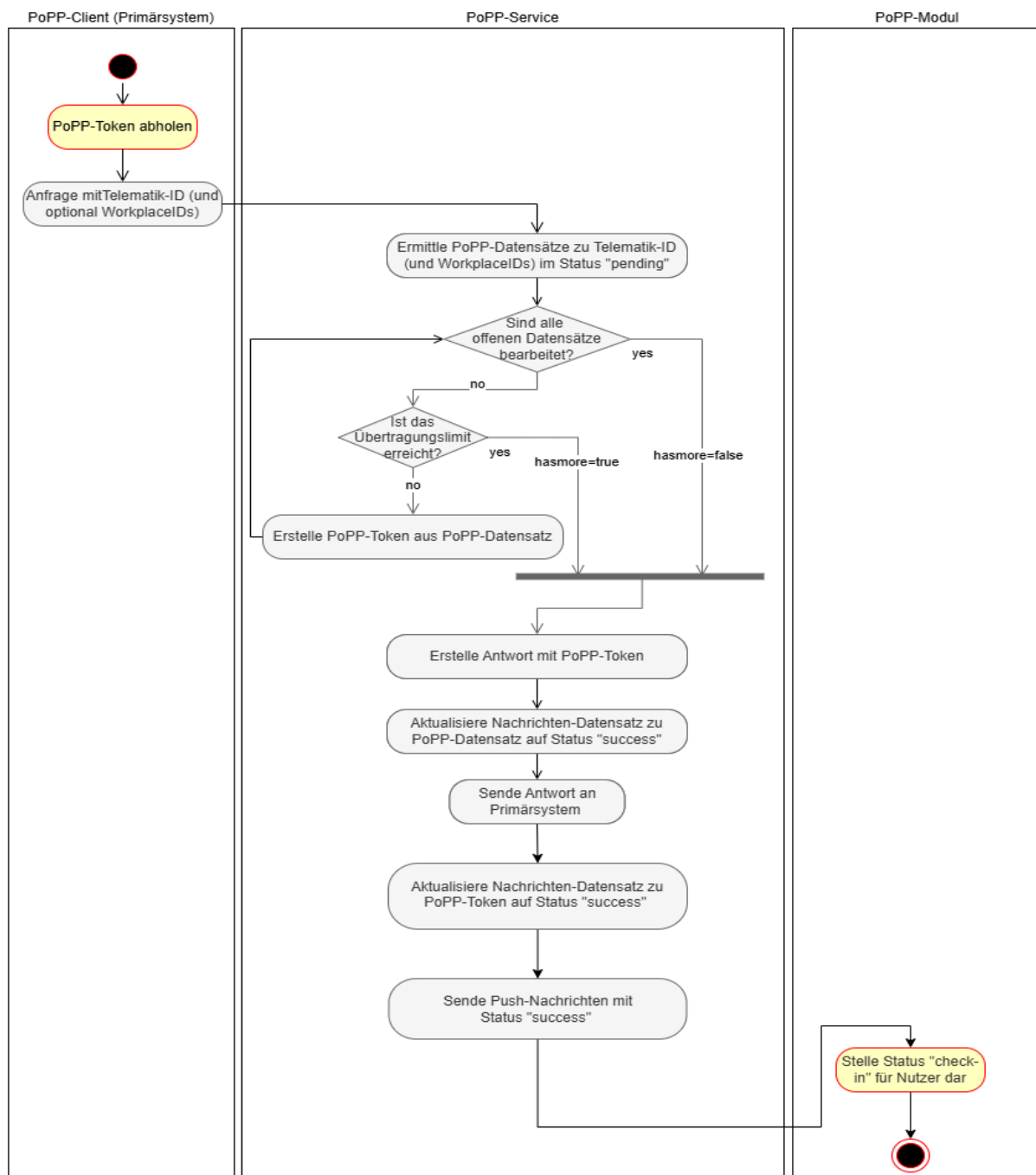


Abbildung 6 : Ablauf Abholen der PoPP-Token bei Online Check-in (auf die beteiligten ZETA-Komponenten wurde in der Abbildung verzichtet)

Das Abholen der PoPP-Token bei Online Check-in wird durch das Primärsystem gestartet. Dieses sendet einen Request gemäß [I_PoPP_Service_mobile_Token_Generation.yaml] an den PoPP-Service. Der PoPP-Service ermittelt die Daten der zu erstellenden PoPP-Token. Der PoPP-Service generiert die PoPP-Token und sendet sie an das Primärsystem zurück.

Der PoPP-Service setzt im Nachrichten-Datensatz den Status auf "success" setzen und löscht den PoPP-Datensatz.

Der folgende Anwendungsfall beschreibt den Ablauf und die einzuhaltenden Akzeptanzkriterien.

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

Attribute	Bemerkung
Beschreibung	Nach einem durch den Versicherten initiierten Online -Check-in ist ein Datensatz für die Erstellung eines PoPP-Token und ein Nachrichten-Datensatz mit dem Status zur PoPP-Token-Generierung angelegt. Erst wenn sich die LEIder Inhaber der Telematik-ID gegenüber dem ZETA-Guard (mit SMC-SM(C)-B) authentifiziert hat, wird aus diesem Datensatz ein PoPP-Token erzeugt. Über ZETA-Guard erhält das Primärsystem eine Nachricht, dass PoPP-Token abrufbar im (AF_10425*). Der PoPP-Service liegen. Dieses Resource Server übermittelt PoPP-Token kann vom Primärsystem der LEI abgerufen werden. Der Abruf von an den PoPP-Token kann auch ohne vorherige Benachrichtigung manuell oder automatisiert durch das Primärsystem der LEI erfolgen. Client. Der PoPP-Service generiert eine Nachricht, welche Resource Server übermittelt den Status der PoPP-Token-Erstellung-Generierung an das PoPP-Modul mit folgendem Inhalt enthält. • id = eindeutiger Identifier der Nachricht • status • success – PoPP-Token wurde erzeugt und der LEI zugestellt • pending – PoPP-Token wurde erzeugt und noch nicht zugestellt, da die LEI nicht online ist. Die Zustellung wird weiter versucht. • cancelled – Prozess wurde aufgrund eines Fehlers oder wegen Überschreitung der maximalen Wartezeit (z.B. 72h) abgebrochen • message = Detailinformationen zum jeweiligen Status 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*).

Attribute	Bemerkung
Vorbedingung	1. Der PoPP-Datensatz für die PoPP-Token-Generierung ist im PoPP-Service Resource Server erstellt und gespeichert. 2. Die LEIDer Nachrichten-Datensatz zum Status der PoPP-Token-Generierung ist im PoPP-Service Resource Server erstellt und gespeichert. 2.3. Das Primärsystem desInhabers der Telematik-ID ist als PoPP-Client am ZETA-Guard registriert. 3.4. Die LEIDer Inhaber der Telematik-ID hat sich gegenübersich gegenüber dem ZETA-Guard (mit SMC-SM(C)-B) authentifiziert.

Ablauf	Information an LEIInhaber der Telematik-ID 1. Der PoPP-Service Resource Server erstellt eine NachrichtPush-Notification für die LEIdas Primärsystem zum Abholen des PoPP-Token. 2. Der PoPP-Service Resource Server sendet die NachrichtPush-Notification an ZETA-Guard zur Weiterleitung an das Primärsystem. <i>Hinweis: Wie die NachrichtPush-Notification erstellt (1) und über ZETA-Guard versendet wird (2) ist im Moment noch ein offener Punkt (OP-PoPP-1)</i> Das Abholen der PoPP-Token durch Primärsysteme ist unabhängig davon, ob der PoPP-Service Resource Server ein Primärsystem darüber informiert hat, dass PoPP-Token zur Generierung vorliegen. Abholen des PoPP-Token durch Primärsystemder LE: 1. Das Primärsystem sendet einen HTTP-Request(über die ZETA-Komponenten) einen HTTP-Request gemäß [I_PoPP_Service_mobile_Token_Generation.yaml] an den PoPP-Service Resource Server. ZETA prüft in diesem Ablauf die Vertrauenswürdigkeit des anfragenden Primärsystems und validiert dessen Identität (SMCSM(C)-B). 2. Der PoPP-Service Resource Server sucht alle PoPP-Datensätze zur Telematik-ID a. mit der LEIWorkplaceID, wenn diese als Suchparameter im Request übermittelt wurde, b. zu denen noch kein PoPP-Token erstellt und ausgegeben wurde. Der Status im Nachrichten-Datensatz zum PoPP-Datensatz ist "pending". c. die innerhalb der letzten 72 Stunden erstellt wurden. 2.3. Der PoPP-Service signiert dasResource Server geniert PoPP-Token. 3.4. Der PoPP-Service Resource Server antwortet auf den HTTP-Request mit demden ausgestellten PoPP-Token und, wenn vorhanden, der zugeteilten WorkplaceIDs und dem Identifier des zugehörigen Nachrichten-Datensatzes. 4.5. Der PoPP-Service Resource Server ändert den Status der Nachrichtzumin den Nachrichten-Datensätzen zu den PoPP-Datensatz-Datensätzen auf <i>status = success</i>. 5.6. Der PoPP-Service Resource Server stellt demPoPP-ModulModulen über die ZETA-Komponenten dieeine Nachricht zur Statusänderung zu. Die Zustellung der Nachricht zuerfolgt a. im synchronen Fall als Antwort auf den jeweiligen HTTP-Request (AF_10386*, AF_10389*)z.B.
--------	--

Attribute	Bemerkung
	Anwendungsfall "Online Check-in mit GesundheitsID"), oder b. asynchron auf Anfrage des PoPP-Moduls an den PoPP-Service Resource Server zu einem PoPP-Token, oder b-c. asynchron als Push-Notification für alle neu verarbeiteten PoPP-Token.
Nachbedingung	- Der PoPP-Service Resource Server löscht alle PoPP-Datensätze - zu denen ein PoPP-Token erstellt und ausgeliefert und zu denen eine Nachricht an das PoPP-Modul erfolgreich zugestellt wurde. - die älter als 72h sind. Der Status der Nachricht zu diesem Datensatz wird auf status = cancelled und message auf message = "Der Check-in wurde nach 72h erfolglos abgebrochen" canceled gesetzt. - Der PoPP-Service Resource Server löscht alle Nachrichten-Datensätze mit status = cancelled oder status = success sobald sie zugestellt wurden, spätestens jedoch nach 5 Tagen.
Akzeptanzkriterien	 ML-184426 - AF 10390 - PoPP-Token erstellt und übermittelt oder Abbruch des Check-in - Der PoPP-Service Resource Server 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 Nachrichten-Datensätzen zu gesendeten PoPP-Token - Der PoPP-Service Resource Server hat eine Nachricht zum Status der PoPP-Token-Erstellung aktualisiert.  ML-184427 - AF 10390 - Löschung zugestellter oder abgelaufener Nachrichten - Der PoPP-Service Resource Server hat zugestellte Nachrichten-Datensätze gelöscht. - Der PoPP-Service Resource Server hat abgelaufene Nachrichten-Datensätze gelöscht.
Fehlerfälle	Die Zustellung der Benachrichtigung ist fehlgeschlagen Das PoPP-Token wurde nicht innerhalb von 72h abgeholt
Alternativen	keine

[<=]

ML-184426 -AF_10390 - PoPP-Token erstellt und übermittelt oder Abbruch des Check-in

Der PoPP-Service hat gemäß [I_PoPP-Token_Generation.yaml] ~~ein~~ PoPP-Token erstellt. ~~Das~~ Die PoPP-Token wurde dem Primärsystem zugestellt. ~~Konnte~~ Wurde innerhalb von 72h nach Erstellung ~~deseines~~ 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~~ AF_10390 - Aktualisierung der Nachrichten-Datensätzen zu gesendeten PoPP-Token

Der PoPP-Service hat ~~den Nachrichtendatensatz~~ aktualisiert

- ~~status = success, wenn dem Primärsystem für die Nachrichten-Datensätze gesetzt, für die ein PoPP-Token zugestellt werden konnte.~~

~~status = cancelled, wenn der Check-in Prozess nach 72h abgebrochen~~ an ein Primärsystem übertragen wurde. [≤]

[≤]

ML-184427 -AF_10390 - Löschung zugestellter oder abgelaufener Nachrichten

Der PoPP-Service hat alle ~~Nachrichtendatensätze~~ Nachrichten-Datensätze gelöscht, die

1. den status "success" oder "~~cancel~~ ~~cancelled~~" haben und erfolgreich dem PoPP-Modul zugestellt werden konnten.
2. die älter als 5 Tage sind.

[<=]

A_30040 -PoPP-Service - Bereitstellung der Schnittstelle zum Abruf der PoPP-Token zu Online Check-ins

Der PoPP-Service MUSS die Schnittstelle I_PoPP_Service_mobile-Token_Generation [I_PoPP_Service_mobile-Token_Generation.yaml] für den Abruf der PoPP-Token zu Online Check-ins bereitstellen. [≤]

A_30106 -PoPP-Service - Abgleich der Telematik-ID PoPP-Datensatz und Nutzer-Anfrage

Der PoPP-Service MUSS durchsetzen, dass ausschließlich solche PoPP-Token für das Primärsystem eines Telematik-ID Inhabers erzeugt und an diesen ausgeliefert werden, die für genau die Telematik-ID bestimmt sind, die bei der Nutzer-Authentifizierung im Rahmen der Anfrage aus dem Primärsystem durch ZETA Guard anhand der SM-B des Nutzers verifiziert wurde. Ein Inhaber einer Telematik-ID bekommt also genau nur PoPP-Token, die für genau diese Telematik-ID vorgesehen sind. [≤]

A_30105 -PoPP-Service - Löschen von Datensätzen nach deren Ablaufzeit

Der PoPP-Service MUSS PoPP-Datensätze löschen, wenn diese älter als 72 h sind und Nachrichtendatensätze löschen, wenn diese älter als 5 Tage sind. [≤]

Offener Punkt: OP-PoPP-8 (Berücksichtigung der WebSocket-Schnittstelle in AF_10390)

Mit Einführung der Schnittstelle

[I_PoPP_Service_mobile_Token_Generation_async.yaml] steht neben REST auch eine WebSocket-basierte Zustellung von PoPP-Token zur Verfügung. Der Anwendungsfall AF_10390 beschreibt bislang den REST-basierten Abruf.

Zu prüfen ist, ob AF_10390 um die WebSocket-Nutzung erweitert werden kann oder ein eigener Anwendungsfall erforderlich ist. Dabei sind insbesondere die Token-Zustellung über bestehende Verbindungen, die Zuordnung von Telematik-ID und WorkplaceID sowie das Zusammenspiel von REST und WebSocket zu betrachten.

Vorgehen:

Erstellung eines neuen Anwendungsfalls oder Erweiterung von AF-10390 parallel zur Kommentierung. Das Ergebnis wird über einen Eigenkommentar der gematik veröffentlicht und in die Spezifikationen eingearbeitet.

4.1.154.1.14 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~~ den Inhaber der Telematik-ID ausgeliefert wurde ("LEI offline").

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

Attribute	Bemerkung
Beschreibung	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 LEIder Inhaber der Telematik-ID, für die das PoPP-Token erstellt werden soll, zum Zeitpunkt des Online -Check-in nicht am ZETA Guard authentifiziert ist (z.B. weil die LEIdas Primärsystem des Inhabers der Telematik-ID nicht online ist). In diesem Fall erhält das PoPP-Modul als Ergebnis des Online -Check-in eine Statusnachricht mit dem Status "pending". KannWird zu einem späteren Zeitpunkt die LEIder Inhaber der Telematik-ID authentifiziert werden und ruft diesdas zugehörige PoPP-Token am PoPP-Service Resource Server ab, so wird beim Abruf des PoPP-Token der Status der Nachricht im PoPP-Service auf "success" gesetzt. Kann die LEI auch zu einem späteren ZeitpunktSolange der Inhaber der Telematik-ID nicht authentifiziert werden (z.B. innerhalb vonist, bleibt der Status "pending". Wurde auch nach 72h);, das PoPP-Token nicht generiert, so wird der PoPP-Datensatz gelöscht und der Status der Nachricht auf "cancelledcanceled" geändert. Das PoPP-Modul kann nun zu späteren Zeitpunktennach dem Online -Check-in beim PoPP-Service Resource Server den aktuellen Status der PoPP-Token-Generierung anfragen und den VersichertenVER informieren, ob sein Online -Check-in beibeimInhaber der LEITelematik-ID erfolgreich war oder abgebrochen wurde.

Attribute	Bemerkung
Vorbedingung	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". Der Identifier des Nachrichten-Datensatzes ist im PoPP-Datensatz hinterlegt. 3. Im PoPP-Modul wurde ein HTTP-Request zur Abfrage des Status zur PoPP-Token-Erstellung an den PoPP-Service Resource Server mit dem Identifier (id) des Nachrichten-Datensatzes Query-Parametern formuliert. 4. Zum Zeitpunkt der Authentisierung des Versichertender VER muss dieser einen Internetzugang haben. 5. Der VersicherteVER verwendet eine Kassen-App mit integrierten PoPP-Modul und ZETA-Client. 6. Gerät und Kassen-App sind in der ZETA Guard Client-Registry registriert. ZETA Guard hat ein Client Access-Token erstellt. a. Der ZETA Guard HTTP-Proxy hat den PoPP-Service aufgerufenResource Server mit dem vom PoPP-Modul erstellten HTTP-Request 7. dem vom ZETA-Guard ausgestellten Client Access-Token aufgerufen.
Ablauf	1. Der PoPP-Service Resource Server nimmt den HTTP-Request vom ZETA Guard HTTP-Proxy entgegen. 1. Der PoPP-Service prüft die Berechtigung der Anfrage (Client Access-Token) 2. Der PoPP-Service-Resource Server extrahiert den Identifier (id) des Nachrichten-Datensatzes aus dem HTTP-Request. 3. Der PoPP-Service Resource Server ermittelt die aktuellen Informationen zur PoPP-Token-Erzeugung aus dem Nachrichten-Datensatz. 4. Der PoPP-Service Resource Server hat den eingegangenen Request mit der Statusnachricht zur PoPP-Token-Erstellung beantwortet.

Attribute	Bemerkung
Nachbedingung	- Erfolgsfall - Der PoPP-Service Resource Server hat dem ZETA Guard HTTP-Proxy mit HTTP-200 und der Statusnachricht zur PoPP-Token-Erstellung geantwortet. - Es ist ein Fehler aufgetreten - Der PoPP-Service Resource Server 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 einem Online -Check-in Der PoPP-Service hat den HTTP-Request vom ZETA Guard HTTP-Proxy entgegengenommen und die Zugriffsberechtigung geprüft Der PoPP-ServiceResource Server hat geantwortet mit einem - 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 FehlerfallFehlerfällen  ML-185507 - AF 10425 - Response an ZETA Guard HTTP-Proxy zum eingegangenen Request Der PoPP-Service Resource Server hat den eingegangenen Request mit der Statusnachricht zur PoPP-Token-Erstellung beantwortet "success", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token erstellt und demInhaber der LEITelematik-ID zugestellt wurde "pending", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token noch nicht erstellt und demInhaber der LEITelematik-ID zugestellt wurde "cancelledcanceled", wenn ein Fehler aufgetreten ist. message mit Informationen im Fehlerfal
Alternativen	Keine

[<=]

ML-185508 ~~-AF_10425 - Bereitsstellung einer Schnittstelle zur Abfrage des aktuellen Status der PoPP-Token-Erstellung nach einem Online-Check-in~~
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_PoPPService_mobile_CheckIn.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_PoPPService_mobile_CheckIn.yaml] eine Response an den ZETA Guard HTTP-Proxy zurück gesendet. Dabei MUSS die Response im Responsebody die Statusnachricht zur PoPP-Token-Erzeugung enthalten:

1. "success", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token erstellt und demInhaber der LEITelematik-ID zugestellt wurde.
2. "pending", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token noch nicht erstellt und demInhaber der LEITelematik-ID zugestellt wurde.
3. ~~"cancelled", wenn ein Fehler aufgetreten ist. Im Fehlerfall muss die "message" der Statusnachricht Informationen zum aufgetretenen Fehler enthalten~~ "canceled", wenn das PoPP-Token nicht zugestellt werden konnte.[<=]

[<=]

A_30100 -PoPP-Service - Abgleich client_id bei Statusabfrage

Der PoPP-Service MUSS durchsetzen, dass bei Status-Abfragen die ZETA Guard PEP http-Proxy client_id abgeglichen wird und der Status nur zurückgegeben wird, wenn die für den Nachrichten-Datensatz Identifier passende client_id angefragt hat (client_id der aktuellen Status-Abfrage = im passenden Nachrichten-Datensatz gespeicherte client_id). In den anderen Fällen (client_id nicht identisch) MUSS mit dem Fehler, dass der Identifier für diesen Client unbekannt ist, geantwortet werden.[<=]

~~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.

~~4.1.174.1.15 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 ausgestellt2]: 5.2 Datenschutz 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. Sicherheit~~

Neu:

A_30118 -PoPP-Service - Berücksichtigung OWASP-Top-10-Risiken

Der Anbieter des PoPP-Service Provider MUSS Maßnahmen zum Schutz vor den zum Zulassungszeitpunkt aktuellen OWASP-Top-10-Risiken umsetzen und dokumentieren, wie es vorgesehen ist, ebenfalls auf die nach dem Zulassungszeitpunkt aktuellen OWASP-Top-10-Risiken zu reagieren.

Hinweis: Die Nichtanwendbarkeit eines OWASP-Top-10-Risikos ist zu begründen. Für Informationen zum Umgang mit den OWASP-Top-10-Risiken wird auf den aktuellen [OWASP-Top-10-Risiken] und die darin enthaltenen Vorgehensweisen für z. B. Entwickler und Tester verwiesen.[<=]

A_30143 -PoPP-Service - Rate-Limit Online Check-in pro Versichertem

Der PoPP-Service MUSS durchsetzen, dass pro Versichertem nicht mehr als 100 laufende Check-in-Vorgänge bestehen - also Vorgänge im Status "pending".[<=]

4.1.184.1.16 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~~-VER 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~~**Versicherten-Smartphone**, 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~~**Smartphone** des Versicherten und den Komponenten im Backend, u.a. auch zwischen PoPP-Modul und PoPP-Service **Resource Server**.

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

ZETA Notification Service

Nach [gemSpec_ZETA] ist der ZETA Notification Service die zentrale Fassade vor den Push Gateways und übernimmt innerhalb der Telematikinfrastruktur die Aufgabe, Benachrichtigungen eines Fachdienstes (Resource Server) an die zugehörigen Endgeräte der Versicherten zuzustellen. Er baut auf dem Push-Notification-Konzept der gematik [gemF_PushNotification].

Fachlich ordnet sich der Notification Service als Bindeglied zwischen dem Fachdienst und der plattformspezifischen Push-Infrastruktur der Betriebssystemhersteller (Apple APNs, Google FCM) ein. Er entkoppelt den Fachdienst von den Details der Push-Zustellung, verwaltet die Push-Konfigurationen und Pusher der Clients und stellt sicher, dass Nachrichteninhalte und Nutzeridentifikatoren geschützt verarbeitet werden.

Der Dienst wird in zwei Betriebsvarianten betrieben: mit VAU, bei der Notification Service und Resource Server gemeinsam in einer Vertrauenswürdigen Ausführungsumgebung laufen und HSM-Anbindung sowie At-rest-Verschlüsselung und Pseudonymisierung aktiv sind, sowie ohne VAU, bei der diese HSM-gestützten Schutzmaßnahmen entfallen. Die Verschlüsselung der Nachrichten ist ein pro ZETA-Guard-Instanz zentral konfigurierbares Feature; ist es nicht aktiv, werden Nachrichten unverschlüsselt weitergegeben.

4.1.17 Änderungen [gemSpec_PoPP_Service#5.4.1]: Bereitstellung, Konfiguration und Verwendung vom ZETA Guard

A_30099 -PoPP-Service - Konfiguration des PEP HTTP Proxy

Der PEP HTTP Proxy des PoPP-Service MUSS so konfiguriert sein, dass gemäß A_26590* die Request-Weiterleitung an den PoPP-Service mit den Client-Daten angereichert wird. [<=]

4.1.18 Neues Kapitel [gemSpec_PoPP_Service#5.4.2]: Versand von Push-Notification über ZETA Guard an das Smartphone des Versicherten

Der PoPP-Service kann über das PoPP-Modul VER über Ereignisse zu einem Online Check-in durch den Versand von Push-Notifications informieren. Für den Versand der Push-Notifikation muss der PoPP-Service Resource Server lediglich die relevanten Schnittstellen am ZETA Notification Service aufrufen.

todo: Zuweisung A_29969 nach Freigabe gemSpec_ZETA (Verwendung der OpenAPI Schnittstelle)

A_30067 -PoPP-Service - Push-Notification an PoPP-Modul nach Statuswechsel

Der PoPP-Service MUSS jeden Statuswechsel per Push-Notification an das PoPP-Modul gemäß [\[OpenApi Spezifikation der Schnittstelle zwischen ZETA Guard Notification Service und Resource Server\]](#) übermitteln. Die zu sendende Payload ist dabei nach dieser Regel zu setzen.

- Wenn dasPoPP-Token dem Inhaber der Telematik-ID zugestellt wurde:
 - "trigger_id": "<ID des Nachrichten-Datensatzes zum PoPP-Token-Datensatz>"
 - "message": "Der Check-in ist abgeschlossen."
 - "status": "success"
- Wenn das PoPP-Token dem Inhaber der Telematik-ID nicht innerhalb von 72h zugestellt wurde:
 - "trigger_id": "<ID des Nachrichten-Datensatzes zum PoPP-Token-Datensatz>"
 - "message": "Der Check-in wurde abgebrochen."
 - "status": "canceled"

[<=]

4.1.19 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 [\[OpenID Federation 1.01\]](#) unter <Identifizier-URL>/ .well-known/openid-federation verfügbar macht.

Das Entity Statement beauskunftet 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 in Kapitel 5.6 werden hinzugefügt

- Allgemeine Anforderungen an die Inhalte des Teilnehmer der TI-Föderation - Zuweisung A_28848, A_28857, A_28879 (neu mit Release IDP 26.1)

A_28848 -Validierung der Vertrauenskette eines TI-Föderation-Teilnehmers

Teilnehmer der TI-Föderation, welche mit anderen Teilnehmern der TI-Föderation kommunizieren wollen, MÜSSEN das Entity Statement des anderen TI-Föderation-Teilnehmers abrufen und gemäß der Regeln [OpenID Federation 1.1] ("Entity Statement Validation") validieren, sowie die Vertrauenskette gemäß [OpenID Federation 1.1] ("Resolving the Trust Chain and Metadata") prüfen. Der Abruf des Entity Statement sollte alle 12h und MUSS innerhalb von 24h erfolgen.

[<=]

gestellt:

A_28857 -Maximale Gültigkeitsdauer und regelmäßige Erneuerung des Entity Statement eines TI-Föderation-Teilnehmers

Teilnehmer der TI-Föderation MÜSSEN ihr Entity Statement bei Änderungen oder vor dem zeitlichen Ablauf neu ausstellen. Die maximale Gültigkeitsdauer - gegeben durch die Differenz der Attributwerte `exp-iat` - darf 24 Stunden nicht überschreiten. [<=]

A_28879 -Registrierung von Teilnehmern in der TI-Föderation durch organisatorischen Prozess

Ein Teilnehmer der TI-Föderation MUSS seinen öffentlichen Schlüssel für die Signatur des selbst-signierten Entity Statement (federation entity signing key) über einen organisatorischen Prozess bei der Superior Entity (Federation Master oder Intermediate) bekannt machen, bei welcher der Teilnehmer als Subordinate Entity registriert werden soll. Nach erfolgreicher Registrierung wird dem Teilnehmer der öffentliche Schlüssel übermittelt, mit dem das Entity Statement des Federation Master signiert ist (federation entity signing key). Der Teilnehmer MUSS diesen Schlüssel speichern und zur Validierung einer Vertrauenskette gemäß A_28848* verwenden. [<=]

~~Anforderungen aus dem Kapitel 5.6 werden aktualisiert:~~

~~Alt:~~

- ~~• A_27294, A_27295, A_27296 entfallen durch die Zuordnung von A_28911 zum PoPP-Service-Bereitstellung-well-known-für-PoPP-Service(neu mit Release IDP 26.1)~~

~~Der Anbieter eines PoPP-Service MUSS sicherstellen, dass unter `<Identifier-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, Identifier in der TI-Föderation
sub	URL	URL des PoPP-Service, (=iss)

Name	Werte	Beispiel / Beschreibung
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")

~~[<=]~~

A_28911 -Entity Statement eines TI-Fachdienstes als Protected Resource

TI-Fachdienste, die sich als Protected Resource in der TI-Föderation registrieren, MÜSSEN ein selbst-signiertes Entity Statement gemäß [OpenID Federation 1.1] ("Entity Statement") bereitstellen und im Internet verfügbar machen. Das Entity Statement MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

Tabelle 6: Header des Entity Statement des TI-Fachdienstes als Protected Resource

Name	Werte / Wertebereich
alg	string, zulässiger Wert "ES256"
kid	string, UUID7-Format [RFC9562#name-uuid-version-7]
typ	string, zulässiger Wert "entity-statement+jwt"

~~Neu:~~

~~A_27294-01-PoPP-Service-Bereitstellung-well-known-für-PoPP-Service~~

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

Tabelle 7+ : Allgemeine Attribute im well-known-document-Dokument des PoPP-ServiceTI-Fachdienstes als Protected Resource

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]
jwks	Set von JWK [RFC7517] zulässige Werte sind, gemäß [OpenID Federation "Claims that MUST or MAY Appear in both Entity Configurations and Subordinate Statements"] - jwks, nur die öffentlichen Schlüssel zu Schlüsseln, mit denen das Entity Statement signiert ist- (federation entity signing key)
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 JSON Object, erforderlicher Wert: "oauth_resource"

* Der claim authority_hints wird nur benötigt, wenn das 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-Statement oauth_resource veröffentlicht sind.
Das Metadaten-Statement MUSS mindestens die folgenden Werte enthalten:

Tabelle 8- : Attribute des ~~Metadatenblock~~Metadatenblocks `oauth_resource` im well-known-document des PoPP-Service-Dokument des TI-Fachdienstes als Protected Resource

Name	Werte	Beispiel
<code>resource</code>	string, URL nach [RFC1738] zulässiger Wert: identisch mit dem Wert des Claims <code>iss</code>	
<code>signed_jwks_uri(*)</code>	URLstring, URL nach [RFC1738]	<code>"https://popp-resource.de/jwks.jose"</code>
<code>organization_name</code>	string (gemäß [OpenID-Federation "Informational Metadata Extensions"] - <code>organization_name</code>) Wertebereich: <code>^[à-üÄ-Üß\w\ \-\.\+*V]{1,128}\$</code>	
<code>keywords</code>	[string] (gemäß [OpenID-Federation "Informational Metadata Extensions"] - <code>keywords</code>) erforderliche Werte: "product_type_version:<VERSION>" "product_type:<von der gematik zugelassener Produkttyp>"	
<code>contacts</code>	[string] (gemäß [OpenID-Federation "Informational Metadata Extensions"] - <code>contacts</code>) erforderlicher Wert in Liste: "<E-Mail-Adresse für Supportanfragen>"	

~~[<=]~~(*) - gemäß [OpenID Federation 1.1] - "Usage of `jwks`, `jwks_uri`, and `signed_jwks_uri` in Entity Metadata" darf der Metadatenblock nur entweder `signed_jwks_uri` oder `jwks` enthalten.

~~[<=]~~

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

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

Name	Werte
<code>organization_name</code>	string (gemäß [OpenID-Federation "Informational Metadata Extensions"] –organization_name) Wertebereich: △[ÄÖÜäöüß\w\ \ \. \& \+ * \/]{1,128}\$
<code>display_name</code>	string (gemäß [OpenID-Federation "Informational Metadata Extensions"] –display_name) Wertebereich: △[ÄÖÜäöüß\w\ \ \. \& \+ * \/]{1,128}\$
<code>keywords</code>	[JSON] (gemäß [OpenID-Federation "Informational Metadata Extensions"] –keywords) erforderlicher Wert: "product_type_version" : "<von der gematik zugelassene Produkttyp-Version>"
<code>contacts</code>	[JSON] (gemäß [OpenID-Federation "Informational Metadata Extensions"] –contacts) erforderlicher Wert: "support" : "<e-mail Adresse für Supportanfragen>"
<code>signed_jwks_uri</code>	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

4.1.20 Änderungen in [gemSpec_PoPP_Service#6.1] eGK-Handling.2]: Schnittstelle für Token-Abrufe

4.1.20.1 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.~~

~~Ein Versicherter nutzt beim~~ **Erster informativer Satz wird wie folgt geändert:**

Die technische Spezifikation der Schnittstellen **I_PoPP-Token-Generation** zum Abruf von PoPP-Token durch Clientsysteme veröffentlicht die gematik auf GitHub im OpenAPI-Format.

Die Anforderung A_26361 wird geändert und nach vorn direkt hinter den ersten informativen Teil gestellt:

alt:

A_26361 - PoPP-Service - Zero Trust Schutz des PoPP-

Interfaceshttps://gemspec.gematik.de/docs/gemSpec/gemSpec_PoPP_Service/latest/-A_26361

Der PoPP-Service MUSS sicherstellen, dass der Zugang zu den Schnittstellen I_PoPP-Token-Generation zum Abruf von PoPP-Token mittels des ZETA Guard [gemSpec_ZETA] vor unberechtigten Zugriffen geschützt ist. [**<=**]

neu:

A_26361-01 -PoPP-Service - Zero Trust Schutz des PoPP-Interfaces

Der PoPP-Service MUSS sicherstellen, dass der Zugang zu allen Schnittstellen zum Abruf von PoPP-Token mittels des ZETA Guard [gemSpec_ZETA] vor unberechtigten Zugriffen geschützt ist. [**<=**]

(I_PoPP-Token-Generation entfernt)

Es wird nach A_26361-01 folgende Zwischenüberschrift neu eingefügt:

4.1.20.1 PoPP-Token Abruf nach eGK-Anbindung durch LEI

Nach dieser neuen Überschrift wird ergänzt:

Bei der Schnittstelle I_PoPP-Token-Generation dient die WebSocket-Verbindung dem Austausch von APDU-Kommandos und APDU-Antworten zwischen PoPP-Service und eGK.

Die Verbindung besteht ausschließlich für die Dauer eines einzelnen Check-in-Vorgangs und wird nach erfolgreicher Ausstellung oder Ablehnung eines PoPP-Token beendet.

Es folgen die unveränderten Anforderungen A_26345 und A_26362

Danach wird das folgende Kapitel am Ende ergänzt.

4.1.20.2 PoPP-Token Abruf nach Online-Check-in ein Versichertenendgerät für

Für den Abruf von PoPP-Token, die Authentisierung im Zusammenhang mit einem Online Check-in erstellt wurden, stellt der eGK gegenüber dem PoPP-Service. Das Versichertenendgerät verfügt über einen Standard-Kartenleser mit dem zwei alternative Schnittstellen bereit.

Die Schnittstelle [I_PoPP_Service_mobile_Token_Generation.yaml] ermöglicht den Abruf von PoPP-Token über ein REST-Verfahren durch den PoPP-Client eines Primärsystems. Als Ergebnis werden die eGK zum Abruf berechtigten PoPP-Token einschließlich der zugehörigen Metadaten, beispielsweise WorkplaceID oder weiteren Zuordnungsinformationen, zurückgegeben.

Ergänzend stellt der PoPP-Service die Schnittstelle [I_PoPP_Service_mobile_Token_Generation_async.yaml] bereit. Diese WebSocket-Verbindung bleibt während der Sitzung aktiv und wird aus Sicherheitsgründen nach spätestens 60 Minuten automatisch beendet. Über diese Verbindung kann der PoPP-Service PoPP-Token unmittelbar an ein verbundenes Primärsystem übermitteln, sobald für die zugehörige Telematik-ID ein PoPP-Token zur Zustellung bereitsteht. Beide Schnittstellen dienen demselben fachlichen Zweck und unterstützen die Zustellung von PoPP-Token nach einem Online-Check-in. Die Wahl der verwendeten Schnittstelle liegt beim Hersteller des Primärsystems.

- c. kontaktbehaftet kommuniziert oder
- d. kontaktlos kommuniziert.

4.1.20.2.1 REST-Betrieb

A_30145 -PoPP-Service – StatusCodes

Der PoPP-Service MUSS sicherstellen, dass Antworten der REST-Schnittstelle die in der Schnittstellenbeschreibung [I_PoPP_Service_mobile_Token_Generation.yaml] definierten HTTP-Status-Codes verwenden. [$\leq$]

4.1.20.2.2 WebSocket-Betrieb

A_30170 -PoPP-Service - Status Code im WebSocket-Interface - 2

Der PoPP-Service MUSS sicherstellen, dass in der Beantwortung eingehender Request an den Schnittstellen I_PoPP_Service_mobile_Token_Generation_async zum Abruf von PoPP-Token ausschließlich die http-Status Code gemäß der Spezifikation auf [I_PoPP_Service_mobile_Token_Generation_async.yaml] verwendet werden. [$\leq$]

A_30146 -PoPP-Service – Zuordnung von Telematik-IDs zu WebSocket-Verbindungen

Der PoPP-Service MUSS für jede über die Schnittstelle [I_PoPP_Service_mobile_Token_Generation_async.yaml] aufgebaute WebSocket-Verbindung die zugehörige Telematik-ID verwalten.

Falls für eine WebSocket-Verbindung zusätzlich eine WorkplaceID übermittelt wird, MUSS der PoPP-Service die Zuordnung zwischen Telematik-ID, WorkplaceID und aktiver WebSocket-Verbindung verwalten

Der PoPP-Service MUSS die Zuordnung zwischen Telematik-ID, optionaler WorkplaceID und aktiver WebSocket-Verbindung während der gesamten Lebensdauer der Verbindung vorhalten.

[<=]

A_30147 -PoPP-Service – Auslieferung von PoPP-Token über bestehende WebSocket-Verbindungen

Wenn für die Telematik-ID eines Empfängers mindestens eine aktive WebSocket-Verbindung vorliegt, MUSS der PoPP-Service PoPP-Token, die für diese Telematik-ID erzeugt wurden, über diese Verbindung zustellen.

Die Zustellung MUSS alle zum PoPP-Token gehörenden Zusatzinformationen, wie WorkplaceID umfassen.[<=]

A_30148 -PoPP-Service – Entfernen ungültiger WebSocket-Verbindungen

Der PoPP-Service MUSS die Zuordnung zwischen Telematik-ID und WebSocket-Verbindung entfernen, wenn die zugehörige WebSocket-Verbindung beendet wurde oder nicht mehr erreichbar ist.

[<=]

A_30149 -PoPP-Service – Beenden von WebSocket-Verbindungen beim Wechsel von Verarbeitungskontexten

Der PoPP-Service MUSS beim Beenden eines Verarbeitungskontextes alle diesem Verarbeitungskontext zugeordneten WebSocket-Verbindungen ordnungsgemäß schließen.

[<=]

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

Für den Überblick zu den statischen QR-Codes siehe auch [gemF_PoPP_Online-Check-in] Kapitel 2.1.5. "Informationen zum Inhaber der Telematik-ID: QR-Code und WorkplaceID" sowie [gemSpec_PoPP_Modul] Kapitel 5.3.1 "QR-Code"

Der statische QR-Code dient im Online Check-in als einfacher und medienbruchfreier Einstiegspunkt zur Auswahl des Inhabers der Telematik-ID. Er ermöglicht Versicherten die eindeutige Identifikation der Einrichtung oder

Organisation, bei der ein Versorgungskontext nachgewiesen werden soll, ohne dass die Telematik-ID manuell erfasst werden muss. Der QR-Code kann in Versorgungseinrichtungen vor Ort, bei mobilen Versorgungsszenarien sowie in der Fernversorgung eingesetzt werden.

Der QR-Code wird durch das Primärsystem des Inhabers der Telematik-ID erzeugt. Zwingender Bestandteil ist die Telematik-ID. Optional kann zusätzlich eine WorkplaceID enthalten sein. Diese dient ausschließlich organisatorischen Zwecken innerhalb des Primärsystems, beispielsweise zur Zuordnung eines erfolgreichen Online Check-ins zu einem bestimmten Arbeitsplatz oder zu einer laufenden Sitzung. Die WorkplaceID begründet keine zusätzlichen Berechtigungen und wird nicht Bestandteil des PoPP-Tokens.

Die eigentliche Berechtigungsentscheidung wird nicht durch den QR-Code, sondern durch die Versicherten getroffen. Vor der Erteilung ihrer Einwilligung werden den Versicherten die zur Telematik-ID gehörenden Informationen aus dem Verzeichnisdienst angezeigt. Dadurch können sie überprüfen, ob der Online Check-in tatsächlich für die gewünschte Einrichtung oder Organisation durchgeführt wird. Der QR-Code dient somit ausschließlich als technischer Transportmechanismus für die Identifikation des vorgesehenen Empfängers eines späteren PoPP-Tokens.

Aus Sicherheitsgründen enthält der QR-Code keine URLs oder sonstige Informationen, die zu automatischen Weiterleitungen führen könnten. Die Durchführung des Online Check-ins erfolgt ausschließlich über die hierfür vorgesehenen Kassen-Apps mit integriertem PoPP-Modul. Primärsystem-Hersteller sollten den QR-Code zusammen mit den wesentlichen Klartextinformationen, insbesondere dem Namen der Einrichtung, der Telematik-ID und gegebenenfalls der WorkplaceID, darstellen. Dadurch wird die Erkennung von Manipulationen erleichtert.

Die Verwendung statischer QR-Codes ist bewusst einfach gehalten. Primärsysteme können denselben QR-Code über längere Zeiträume verwenden. Ein regelmäßiger Austausch oder eine kryptographische Signatur des QR-Codes sind nicht vorgesehen. Die Sicherheit des Verfahrens beruht stattdessen auf der nachgelagerten Prüfung der Telematik-ID über den Verzeichnisdienst, der ausdrücklichen Zustimmung der Versicherten sowie den Authentisierungs- und Autorisierungsmechanismen der PoPP- und ZETA-Komponenten.

A_28532 -PS - PoPP - Inhalt QR-Code

Das PS MUSS einen QR-Code für ~~eine LEI~~ den Inhaber der Telematik-ID 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. [$\leq$]

A_28533 -PS - PoPP - Format QR-Code

Das PS MUSS diesen QR-Code gemäß ISO/IEC 18004:2024 kodieren. [$\leq$]

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. [$\leq$]

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

Das PS MUSS neben dem Wird einer VER ein 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 Online Check-in-Vorgang verwendet wird, präsentiert, dann MÜSSEN für die VER zusätzlich im Klartext Hinweise hinzugefügt werden. Die Hinweise MÜSSEN mindestens die folgenden Informationen vermitteln:

1. Der Online Check-in ist nur mit einer gültigen GesundheitsID möglich.
2. QR-Codes sind ausschließlich mit der dafür vorgesehenen Kassen-App zu scannen. Beispiel: "Wir bitten Sie diesen QR-Code immer mit Ihrer Andere Apps auf dem Smartphone des Versicherten dürfen nicht verwendet werden.
3. Während des Online Check-in-AppVorgangs werden keine Links zur Eingabe weiterer Daten oder zur Navigation auf externe Webseiten bereitgestellt; entsprechende Aufforderungen können auf einen Phishing-Angriff hindeuten und sollen dem Personal der Institution gemeldet werden.
- 1-4. Während des Online Check-in werden am Smartphone des Versicherten Angaben zumInhaber der Telematik-ID präsentiert. Diese Angaben sind von der VER auf Richtigkeit zu prüfen.

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 desInhaber der-LEI-Name Telematik-ID, die (verkürzte) Telematik-ID und (optional) die Arbeitsplatzbezeichnung im Klartext aufdrucken.
Weitere Informationen über den Inhaber der Telematik-ID, die Versicherten den Abgleich mit den präsentierten VZD-Daten erleichtert, können ebenfalls dargestellt werden.
- Es ist ratsam,eine regelmäßige ÜberprüfungenÜberprüfung 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 bevor dieser gedruckt wird den Hinweis anzeigen, dass

- 1- QR-Codes innerhalb der LEIRäumlichkeiten des Telematik-ID Inhabers in einem gut durch LEI-das Personal frequentiert Bereich - idealerweise am Tresen - aufgestellt bzw. angebracht werden soll sowie regelmäßig auf Korrektheit geprüft werden soll.[<=]
1. , da der QR-Code grundsätzlich von einem Angreifer ausgetauscht werden könnte.
2. QR-Codes nicht auf Webseiten eingebracht werden sollen.
3. QR-Codes nicht per E-Mail versendet werden sollen.

[<=]

Hinweis:

Zur Prüfung der Korrektheit des QR-Codes kann das Personal des Inhaber der Telematik-ID den QR-Code mit der eigenen Kassen-App scannen und die darin enthaltene

Telematik-ID anhand der angezeigten VZD-Daten verifizieren. Ein tatsächlicher Check-in ist hierfür nicht erforderlich und kann abgebrochen werden.

Hinweis:

Die Darstellung des QR-Codes auf einem Display des Telematik-ID Inhabers ist möglich.

4.2.2 WorkplaceID

~~Für den ILF wird einleitend noch weiterer erklärender Text zur WorkplaceID
zugefügt, bzw. Hinweis auf den Konzept Teil dieser Feature Spezifikation.~~

~~Die optional vom~~Für den Überblick zur Verwendung der WorkplaceID siehe auch
[gemF_PoPP_Online-Check-in] Kapitel 2.1.5. "Informationen zum Inhaber der Telematik-
ID: QR-Code und WorkplaceID".

Neben großen Versorgungseinrichtungen wie MVZ mit vielen Check-in Arbeitsplätzen
können auch Online-Dienste wie bspw. Videosprechstunden Anbieter die WorkplaceID
verwenden. Ebenso ist die Verwendung als "SessionID" möglich, um auch in Anbieter-
Apps den Check-in einem VER Smartphone zuordnen zu können.

Falls der PoPP-Service ~~übertragen~~zusätzlich zum PoPP-Token auch eine WorkplaceID
übermittelt, dann dient ~~beispielsweise~~dieses beispielsweise der Zuordnung ~~eines~~des PoPP-
Token zu einem Arbeitsplatz ~~in der LEI~~im Primärsystem des Telematik-ID Inhabers, an
dem ein Online Check-in von einem Versicherten durchgeführt wurde.

Die WorkplaceID kann durch ~~die LEI~~den Inhaber der Telematik-ID 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~~Der Inhaber der Telematik-ID muss dabei
beachten, dass die in A_28629* beschriebenen Einschränkungen für die WorkplaceID
entsprechend genauso gelten.

A_28537 -PS - PoPP - WorkplaceID entnehmen

Das PS MUSS die optionale WorkplaceID 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_Ge
neration_online_check_in.yaml] aufgerufen wird. Im Zuge des Online -Check-in eines
Nutzers-Versicherten wird ein PoPP-Datensatz im PoPP-Service angelegt und für maximal
72h vorgehalten. Fragt ~~eindas~~ das Primärsystem ~~desInhabers~~ einer ~~LEI~~Telematik-ID während
dieser Zeit ~~die Schnittstelle nach~~ über die
Schnittstelle [I_PoPP_Service_mobile_Token_Generation.yaml] oder
[I_PoPP_Service_mobile_Token_Generation_async.yaml] PoPP-Token an, ~~wird aus dem~~
erstellt der PoPP-Service auf Basis des hinterlegten PoPP-Datensatz ein PoPP-Token
~~erstellt~~ und ~~der LEI~~liefert dieses an ~~der Schnittstelle~~ das Primärsystem 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.~~

Neben der REST-Schnittstelle `I_PoPP_Service_mobile_Token_Generation` stellt der PoPP-Service für den Abruf von PoPP-Token zusätzlich die WebSocket-Schnittstelle `I_PoPP_Service_mobile_Token_Generation_async` bereit. Beide Schnittstellen dienen demselben fachlichen Zweck, nämlich dem Abruf von PoPP-Token durch den im Primärsystem integrierten PoPP-Client. Die über die WebSocket-Schnittstelle ausgetauschten Nachrichten entsprechen fachlich den Informationen der bestehenden REST-Schnittstelle.

Die WebSocket-Schnittstelle ermöglicht es dem PoPP-Service, PoPP-Token unmittelbar über bereits bestehende Verbindungen an Primärsysteme zu übertragen. Dadurch muss ein Primärsystem nicht ausschließlich periodisch neue Abrufe initiieren, sondern kann eingehende PoPP-Token über eine bestehende Verbindung unmittelbar empfangen.

Da der PoPP-Service innerhalb einer Vertrauenswürdigen Ausführungsumgebung (VAU) betrieben wird und die Verarbeitungskontexte regelmäßig erneuert werden, besitzen WebSocket-Verbindungen nur eine begrenzte Lebensdauer.

Primärsysteme müssen daher davon ausgehen, dass bestehende Verbindungen spätestens nach dem Ablauf eines Verarbeitungskontextes beendet werden können. Die maximale Lebensdauer eines Verarbeitungskontextes beträgt eine Stunde. Nach einem Verbindungsabbruch ist eine neue WebSocket-Verbindung aufzubauen. Grundlage hierfür ist die VAU-Anforderung, Verarbeitungskontexte regelmäßig neu zu starten.

Für eine zuverlässige Zustellung von PoPP-Token empfiehlt es sich daher, dass Primärsysteme die bestehende WebSocket-Verbindung zyklisch überwachen und bei Bedarf automatisch erneut aufbauen. Die WebSocket-Verbindung sollte als persistente Kommunikationsverbindung zwischen Primärsystem und PoPP-Service betrachtet werden, deren Wiederaufbau Bestandteil des regulären Betriebs ist.

Auf Seiten des PoPP-Service ist eine Zuordnung zwischen der über die WebSocket-Verbindung angemeldeten Telematik-ID und der jeweils offenen Verbindung erforderlich. Dadurch kann der PoPP-Service ein im Zuge eines Online Check-in erzeugtes PoPP-Token einer bereits bestehenden Verbindung zuordnen und dies ohne zusätzliche Anmeldung oder erneute Verbindungsherstellung unmittelbar an das zugehörige Primärsystem ausliefern.

A_30039 -PS - Abruf von PoPP-Token nach Online Check-in

Der PoPP-Client MUSS zum Abruf von PoPP-Token zu Online Check-ins mindestens eine der folgenden Schnittstellen unterstützen:

- die REST-Schnittstelle `[I_PoPP_Service_mobile_Token_Generation.yaml]` oder

- die WebSocket-Schnittstelle[I_PoPP_Service_mobile_Token_Generation_async.yaml].

Der PoPP-Client KANN beide Schnittstellen unterstützen und KANN die verwendete Schnittstelle situationsabhängig auswählen.[<=]

A_30144 -PoPP-Client – Überwachung und Wiederaufbau einer WebSocket-Verbindung

Wenn der PoPP-Client die WebSocket-Schnittstelle [I_PoPP_Service_mobile_Token_Generation_async.yaml] verwendet, MUSS der PoPP-Client den Zustand der Verbindung zum PoPP-Service überwachen und bei einem Verbindungsabbruch selbstständig eine neue WebSocket-Verbindung aufbauen. Der PoPP-Client DARF NICHT davon ausgehen, dass eine bestehende WebSocket-Verbindung dauerhaft verfügbar bleibt. Der PoPP-Client MUSS insbesondere davon ausgehen, dass eine bestehende WebSocket-Verbindung spätestens nach einer Stunde seitens PoPP-Service beendet wird. Im Falle des Verbindungsabbaus MUSS der PoPP-Client den Abruf von PoPP-Token durch den erneuten Aufbau einer WebSocket-Verbindung fortsetzen.

Hinweis: Die maximale Lebensdauer einer WebSocket-Verbindung ergibt sich aus der maximalen Lebensdauer der Verarbeitungskontexte innerhalb der VAU des PoPP-Service, da die Verbindung direkt im Verarbeitungskontext terminiert.

[<=]

4.44.3 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:

Tabelle 9: Übersicht über die OpenAPI-Definitionen

Schnittstelle	Status	Änderungsbeschreibung
[I_PoPP_Token_Generation.yaml]	unverändert	ohne Änderung

Schnittstelle	Status	Änderungsbeschreibung
[I_PoPP_Service_mobile_Token_Generation_online_check_in.yaml]	neu	Neues REST 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, WorkplaceID, ...)

Schnittstelle	Status	Änderungsbeschreibung
[I_PoPP_Service_mobile_CheckIn_HID.yaml]	neu	Schnittstellen für die Kommunikation mit dem PoPP-Modul. Die OpenAPI-Definition umfasst: - Die Schnittstelle für zur Authentifizierung mit Gesundheits ID und Anlegen eines PoPP-Datensatzes - Die Schnittstelle für das Laden der Informationen zum Inhaber einer Telematik-ID vom FHIR-VZD - Die Schnittstelle für das Lesen des aktuellen Status zur PoPP-Token-Erstellung und Auslieferung
[I_PoPP_Modul_mobile_CheckIn_eGK_Verification.yaml]	neu	Schnittstelle für Authentifizierung einer eGK und Anlegen eines PoPP-Datensatzes Modul für den Aufruf aus anderen Apps.

Schnittstelle	Status	Änderungsbeschreibung
[I_PoPP_load_Practitioner_Information.yaml]	neu	Schnittstelle für das Laden der Informationen zu einer LEI vom FHIR-VZD
[I_PoPP_Read_Status_PoPPService_mobile_Token_Generation_async.yaml]	neu	Schnittstelle für das Lesen des aktuellen Status zur PoPP-Token-Erstellung und Auslieferung Neues WebSocket 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, WorkplaceID, ...)
[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

4.54.4 Änderungen in [gemSpec_ZETA]

~~Für die Authentisierung~~ Bei der Authentifizierung von Versicherten wird mit GesundheitsID werden in PoPP Stufe 2 ~~der u.a.~~ ZETA-Komponenten (ZETA-Client / ZETA Guard) verwendet. Die Festlegungen dazu stehen in [gemSpec_ZETA] Stufe 2.

~~IDPs aufgenommen werden~~ IDP in der TI-Föderation (iss) und eine PoPP spezifischen Pfaderweiterung.

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~~ Smartphone 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 Allgemeine Anforderungen an Teilnehmer**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. **[<=]**

TI-Föderation"

~~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.~~

~~A_28690~~ Authenticator Modul: Schnittstelle zur Abfrage des Status der GesundheitsID

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. **[<=]**

4.84.7 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

Tabelle: 10 Tab_gemSpec_Perf_PoPP_Service: Performancerelevante UseCases

UseCase	Fachdienstoperation	Beschreibung
←...→PoPP.ZT1	GET /.well-known	ZETA: Abruf gültiger Autorisierungsserver
PoPP.ZT2	GET /nonce	ZETA: Nonce abrufen
PoPP.ZT3	POST /token <JWT Client Assert>	ZETA: Autorisierung ohne Refresh Token
PoPP.ZT4	POST /token <Refresh Token>	ZETA: Autorisierung mit Refresh Token
PoPP.1	GET/popp/practitioner/api/v1/token-generation-ehc	Anweisung zur Erstellung eines PoPP-Token nach Authentifizierung des Versicherten in der Umgebung des Telematik-ID-Inhabers
PoPP.2	POST /httpLoadPractitionerInformationRequest	Anweisung zur Suche der Daten zum Inhaber einer Telematik-ID

UseCase	Fachdienstoperation	Beschreibung
PoPP.UC_03 3	I_PoPP_CheckIn_HIDPOST /httpCheckInGIDRequest	Anweisung zur Erstellung eines PoPP-Token nach Authentifizierung des Versicherten über seine GesundheitsID 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. Der UC Beginnt mit dem Aufruf CheckInGIDRequest im PoPP-ResourceServer und endet mit dem Absenden der Response StatusPoppTokenGeneration.
PoPP.4	(reserviert)	

UseCase	Fachdienstoperation	Beschreibung
PoPP UC_04 5	I_PoPP_CheckIn_eGK_VerificationPOST /httpReadStatusPoPPRequest	Anweisung für den Abruf des aktuellen Status zur PoPP-Token-Erstellung In diesem Aufruf erzeugt liest der PoPP-Service APDU-Kommandos für die eGK und liefert diese in der Response an das PoPP-Modul und führt folgende Schritte aus • 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 aktuellen Nachrichten-Datensatzes Datensatz. Der aktuelle Nachrichten-Datensatz wird vom PoPP-Service in der Response an das PoPP-Modul gesendet. Der UC beginnt mit dem Erhalt des Aufrufs ReadEgkRequest im PoPP-Dienst und endet mit dem Absenden der Response zum PoPP-Modul. Die Kommunikation über das PoPP-Modul zur eGK ist darin mit enthalten.

UseCase	Fachdienstoperation	Beschreibung
PoPP.UC_05 6	I_PoPP_Load_Practitioner_Information POST /popp/practitioner/api/v1/token-deliveries	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. Anweisung zur Erstellung eines PoPP-Token nach Authentifizierung des Versicherten mit Mobilgerät (Smartphone) (REST)
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_077	I-PoPP-Token-Generation-online-check-in POST (/popp/practitioner/api/v1/token-deliveries) (Hinweis: Link wird noch geändert)	In diesem Aufruf ruft das Primärsystem einen LEI-PoPP-Token zu Online-Check-in ab. Der PoPP-Service • ermittelt PoPP-Datensätze zur LEI • Erstellt PoPP-Token • Aktualisiert den Nachrichten-Datensatz zum PoPP-Datensatz Die erstellten PoPP-Token werden von dem PoPP-Service in der Response an das Primärsystem der LEI gesendet. Anweisung zur Erstellung eines PoPP-Token nach Authentifizierung des Versicherten mit Mobilgerät (Smartphone) (WebSocket)
-------------	--	--

Aktualisierung der Anforderung zu den Performance-Kenngrößen:

~~A_27030-04A_27030-01~~ -Performance - PoPP-Service - Bearbeitungszeit unter Last

Der PoPP-Service MUSS die Bearbeitungszeitvorgaben unter Last aus Tabelle "Tab_gemSpec_Perf_PoPP_Service: Last- und Bearbeitungszeitvorgaben" erfüllen.

Tabelle 11: Tab_gemSpec_Perf_PoPP_Service: Last- und Bearbeitungszeitvorgaben

Operation	Spitzenlast [1/sec]	Mittlere Bearbeitungszeit [msec]	Maximale Bearbeitungszeit [msec]	Erfüllungsquote [%]
PoPP.UC_011	1400	600	1500	99,99
PoPP.UC_022	-1400	-600	-1500	-99,99

Operation	Spitzenlast [1/sec]	Mittlere Bearbeitungszeit [msec]	Maximale Bearbeitungszeit [msec]	Erfüllungsquote [%]
PoPP. UC_033	1400	1400+800 (600+1200 PoPP. UC_05)	1800 3500	99,99
PoPP. UC_044	350 1400	1700 (500+1200 PoPP. UC_05)800	1200 3250	99,99
PoPP. UC_055	2000 350	1200 200	350 2000	99,99
PoPP. UC_066	1400	600	1500	99,99
PoPP. UC_077	1400	600	1500	99,99

[<=]

4.94.8 Änderungen in [gemKPT_Betr]

Anpassung Tabelle:

Tabelle 12: 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
BDE	Betriebsdatenerfassung
GUI	Graphical User Interface (graphische Bedienoberfläche)
IDP	Identity Provider
LE	Leistungserbringer
LEI	Leistungserbringerinstitution
LEPS	LeistungserbringerPrimärsystem
SM(C)-B	Secure Module (Card) - Typ B
VER	versicherte Person oder dessen Vertreter
VZD	Verzeichnisdienst
eGK	elektronische Gesundheitskarte
eH-KT	eHealth-Kartenterminal
gID	GesundheitsID

6.2 Glossar

Tabelle 13: 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.

Begriff	Erläuterung
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 Krankenversicherungskassen -Apps (1-App-Strategie), andere halten Krankenversicherungskassen -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.
Anbieter-App	Der Begriff Anbieter-App verallgemeinert Apps, die kein PoPP-Modul implementieren. Das können andere Apps der Krankenkassen oder Drittanbieter-Anwendungen für VER sein.

Begriff	Erläuterung
Drittanbieter-AppAnwendung	Eine Drittanbieter-App bieten den Versicherten Anwendung ist eine Anwendung im Kontext des Gesundheitswesens, die Personen digitale Service zur Unterstützung medizinischer Anwendungsfälle an. Beispiele für Gesundheitsdienste bereitstellt und nicht von einer gesetzlichen oder privaten Krankenversicherung angeboten wird. Drittanbieter-Apps Anwendung können insbesondere von Leistungserbringern, deren Verbänden oder sonstigen Anbietern für Leistungen im Gesundheitswesen bereitgestellt werden. Beispiele sind Apotheken-Apps, Videosprechstunden-Apps oder DiGA-Apps. Die Apps von Krankenkassen aka Krankenversicherungskassen-Apps sind von keine Anbieter-Apps im Sinne dieser Spezifikation. Drittanbieter-Apps verschieden. Drittanbieter App können für beliebige Smartphone Betriebssysteme wie Android oder iOS sowie für unterschiedliche Desktop Betriebssysteme wie Windows oder Linux verfügbar Anwendungen können als native mobile Anwendungen oder browserbasierte Webanwendungen umgesetzt 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.
Telematik-ID	Die Telematik-ID ist die eindeutige elektronische Identität von Leistungserbringern und medizinischen Institutionen in der TI. Sie wird von den Sektoren des Gesundheitswesens zugewiesen und verwaltet. Inhaber oder Inhaberinnen einer Telematik-ID werden in diesem Dokument "Inhaber einer Telematik-ID" oder "Telematik-ID Inhaber" genannt.

Begriff	Erläuterung
Krankenversicherungskassen-App	Mit einer Krankenversicherungs-App bieten Krankenversicherungen ihren Versicherten digitale Service zur Unterstützung medizinischer Anwendungsfälle an. Eine Kassen-App ist eine App, die von einer Krankenversicherung oder einem Dienstleister einer Krankenversicherung für VER bereitgestellt wird. Dazu zählen Apps wie das ePA-FdV, die Authenticator-App für die GesundheitsID sowie weitere Apps für digitale Serviceleistungen von Krankenversicherungen.
Leistungserbringer (LE)	Ein Leistungserbringer gehört zu einem zugriffsberechtigten Personenkreis nach § 352 SGB V und erbringt Leistungen des Gesundheitswesens für Versicherte VER. Nach § 339 SGB V darf er auf Versichertendaten in Anwendungen der TI zugreifen.
Leistungserbringerinstitution (LEI)	Die in organisatorischen Einheiten oder juristischen Personen zusammengefassten Leistungserbringer (bspw. Arztpraxen, Krankenhäuser).
Mobiles PS	Mobiles Endgerät, auf dem ein PS-Client des Inhabers einer LEI Telematik-ID 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 DrittanbieterKassen-App , welche beim für Online-Check-in-Anwendungsfälle die Kommunikation mit dem PoPP-Service ServiceResource Server übernimmt. Das PoPP-Modul verwaltet TAN, initiiert die es vom PoPP-Service im Rahmen eines Online-Check-ins erhält und hilft bei der Übertragung Authentifizierung einer TAN an das Primärsystem VER mit GesundheitsID.
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 dem Inhaber einer LEI Telematik-ID.

Begriff	Erläuterung
Proof of Patient Presence (PoPP)	PoPP ist ein Nachweis, der belegt, dass ein Versicherter sich zu einem bestimmten Zeitpunkt in einem Versorgungskontext mit dem Inhaber einer bestimmten Telematik-ID befindet.
Versorgungskontext (VK)	Der Versorgungskontext beschreibt die sichere und kryptografisch belegte Verbindung zwischen einem berechtigten Versicherten und einem authentifizierten Inhaber einer Telematik-ID . 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	31
Abbildung 2: Produkttypzerlegung PoPP-Service	33
Abbildung 3: Systemkontext PoPP-Service	35
Abbildung 4: Anwendungsfälle zur Attestierung des Versorgungskontexts	43

Abbildung 5: Use-Case-Übersicht Online-Check-in aus einer App mit integriertem PoPP-Modul	48
Abbildung 1: Rollen und Akteure bei Herstellung und Betrieb des PoPP-Service	31
Abbildung 2: Produkttypzerlegung PoPP-Service	33
Abbildung 3: Systemkontext PoPP-Service	35
Abbildung 4: Anwendungsfälle zur Attestierung des Versorgungskontexts	43
Abbildung 5: Use-Case-Übersicht Online Check-in aus einer App mit integriertem PoPP-Modul	48
Abbildung 6 : Ablauf Abholen der PoPP-Token bei Online Check-in (auf die beteiligten ZETA-Komponenten wurde in der Abbildung verzichtet)	71

6.4 Tabellenverzeichnis

Tabelle 1: PoPP-Use Cases (Business Sicht)	26
Tabelle 2: Kurzbeschreibung der Komponenten in der PoPP-Lösung	36
Tabelle 3: Zuordnung der Anwendungsfälle zu den Use Cases	44
Tabelle 4: Kurzbeschreibung technische Use Cases Online-Check-in aus einer App mit integriertem PoPP-Modul	48
Tabelle 5: Attribute im well-known document des PoPP-Service	85
Tabelle 6: Attribute im well-known document des PoPP-Service	87
Tabelle 7: Attribute des Metadatenblock oauth_resource im well-known document des PoPP-Service	88
Tabelle 8: Attribute des Metadatenblock oauth_resource im well-known document des PoPP-Service	89
Tabelle 9 Tab_gemSpec_Perf_PoPP_Service: Last- und Bearbeitungszeitvorgaben	108
Anpassung Tabelle 10: Tab_gemKPT_Betr_Produkttypen	109
Tabelle 11: Glossar der explizit im Dokument verwendeten Begriffe	112
Tabelle 1: Ablauf Online Check-in	18
Tabelle 2: PoPP-Use Cases (Business Sicht)	26
Tabelle 3: Kurzbeschreibung der Komponenten in der PoPP-Lösung	36
Tabelle 4: Zuordnung der Anwendungsfälle zu den Use Cases	44
Tabelle 5: Kurzbeschreibung technische Use Cases Online Check-in aus einer App mit integriertem PoPP-Modul	48
Tabelle 6: Header des Entity Statement des TI-Fachdienstes als Protected Resource	86
Tabelle 7 : Allgemeine Attribute im well-known-Dokument des TI-Fachdienstes als Protected Resource	86
Tabelle 8 : Attribute des Metadatenblocks oauth_resource im well-known-Dokument des TI-Fachdienstes als Protected Resource	87

Tabelle 9: Übersicht über die OpenAPI-Definitionen	97
Tabelle:10 Tab_gemSpec_Perf_PoPP_Service: Performancerelevante UseCases	104
Tabelle 11: Tab_gemSpec_Perf_PoPP_Service: Last- und Bearbeitungszeitvorgaben ...	108
Tabelle 12: Tab_gemKPT_Betr_Produkttypen	109
Tabelle 13: Glossar der explizit im Dokument verwendeten Begriffe	112

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
[gemKPT_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/ Technisches Konzept Proof of Patient Presence (PoPP) https://gemspec.gematik.de/docs/gemKPT/gemKPT_PoPP (Version 1.0.0 vom 20.08.2024)
[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/
[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-CC2</i> gematik Spezifikation "Proof of Patient Presence (PoPP)-Service" https://gemspec.gematik.de/docs/gemSpec/gemSpec_PoPP_Service/gemSpec_PoPP_Service_V1.1.0/ (Version 1.1.0 vom 22.04.2026)

[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]	Spezifikation PoPP (Proof of Patient Presence)-Modul ... (Version: Vorab-Veröffentlichung im gleichen Dok-Paket)
[gemSpec_ZETA]	gematik Spezifikation Zero Trust Access (ZETA) https://gemspec.gematik.de/docs/gemSpec/gemSpec_ZETA/ bzw. https://gemspec.gematik.de/prereleases/Draft_ZETA_26_2/gemSpec_ZETA_V2.0.0_CC/ (Vorab-Veröffentlichung vom 09.07.2026 - ZETA Stufe 2)
[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) https://github.com/gematik/api-popp/tree/US-2_CC2 (vom 22.01.2026)
[I_PoPP_Service_mobile_CheckIn_HID.yaml]	OpenAPI Schnittstellenspezifikation für Authentifizierung mit GesundheitsID und - den Aufruf des VZD-Suche am PoPP-Service - den Aufruf zum Anlegen eines PoPP-Datensatzes https://github.com/gematik/api-popp/blob/US-2_CC1/src/openapi/I_PoPP_CheckIn_HID.yaml am PoPP-Service - den Aufruf zur Statusabfrage am PoPP-Service I_PoPP_Service_mobile_CheckIn.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_Service_mobile_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

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

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[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

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](#) VER 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](#) das Primärsystem des [Inhabers der Telematik-ID](#) 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 [6.24 Spezifikation](#) von diesem Dokument enthalten.

8 Anhang C – Offene Punkte, Fragen

8.1 Offene Punkte

OP-PoP P-1	Kap 4.1.14 (13 [gemSpec_PoPP-Service]) Kap #4.25.3 (ILF): PoPP-Client)-Token bei Online Check-in	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. OP-PoPP-1 (zusätzliche Push-Notification für PS) Für PoPP Stufe 2 ist noch nicht festgelegt, ob und wie Primärsysteme über neu bereitgestellte PoPP-Token aktiv informiert werden oder diese ausschließlich durch regelmäßige Abrufe ermitteln. Die hierfür notwendigen Festlegungen befinden sich derzeit in Abstimmung. Vorgehen zur Auflösung: Klärung innerhalb der gematik gemeinsam mit den verantwortlichen ZETA-Teams parallel zur Kommentierung. Das Ergebnis wird über einen Eigenkommentar der gematik veröffentlicht und in die Spezifikationen eingearbeitet.	

Gelösch

OP-PoP P-2	[gemSpec_Popp_Modul#3.2.1.3]	Offener Punkt: OP-PoPP-2 Für die Authentisierung eines Versicherten mit GesundheitsID müssen Informationen zum verwendeten sektoralen Identity Provider der Krankenversicherung an die ZETA-Komponenten übergeben werden. Die Ausgestaltung dieser Übergabe und die hierfür verwendeten Schnittstellenparameter sind derzeit noch nicht abschließend festgelegt. (Stichwort: idp_iss via authorization_details,) Vorgehen: Klärung innerhalb der gematik gemeinsam mit den verantwortlichen ZETA-Teams parallel zur Kommentierung. Das Ergebnis wird über einen Eigenkommentar der gematik veröffentlicht und in die Spezifikationen eingearbeitet.
OP-PoP P-3	[gemSpec_Popp_Modul#3.2.2.2]	Offener Punkt: OP-PoPP-3 (DeepLink) Die derzeit spezifizierte Übergabe von Informationen zwischen Anbieter-App und Kassen-App mittels HTTP-POST über Deep Links ist hinsichtlich ihrer technischen Umsetzbarkeit noch nicht abschließend geklärt. Insbesondere ist offen, ob die vorgesehene Übergabeform durch die relevanten mobilen Betriebssysteme und die hierfür vorgesehenen Mechanismen zuverlässig unterstützt wird. Für die Umsetzung des Online Check-in wird gegebenenfalls eine alternative Lösung auf Basis von App-Links und einer parameterbasierten Übergabe innerhalb der Ziel-URL erforderlich. Vorgehen: Prüfung und Abstimmung innerhalb der gematik parallel zur Kommentierung. Die betroffenen Spezifikationsstellen werden identifiziert und konsistent angepasst. Das Ergebnis wird über einen Eigenkommentar der gematik veröffentlicht und in die betroffenen Spezifikationen eingearbeitet.

			
OP-PoP P-4	[gemSpec_Popp_Modul#5.6.3]	Offener Punkt: OP-PoPP-4 (2-Geräte-Flow) Wie der 2-Geräte-Flow abzubilden ist, ist derzeit noch offen. Vorgehen: Prüfung und Abstimmung innerhalb der gematik parallel zur Kommentierung. Das Ergebnis wird über einen Eigenkommentar der gematik veröffentlicht und in die betroffenen Spezifikationen eingearbeitet.	
OP-PoP P-25	Kap 4.7 (Testkonzept)[gemSpec_Popp_Modul#5.6.4]	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. Offener Punkt: OP-PoPP-5 - (Anforderungen an Anbieter-App) Im Zusammenspiel mit dem PoPP-Token-Abruf ergeben sich Anforderungen an die Anbieter-Apps - das sind zum Beispiel Videosprechstunden-Apps, die PoPP nutzen und selbst kein PoPP-Modul integrieren. Es ist noch offen, ob es hierfür einen eigenen Steckbrief gibt, bzw. an wen und wie dieses Anforderungen im Anforderungsmanagement geführt werden. Vorgehen: Prüfung und Abstimmung innerhalb der gematik parallel zur Kommentierung. Das Ergebnis wird über einen Eigenkommentar der gematik veröffentlicht und in die betroffenen Spezifikationen eingearbeitet.	

OP-PoP P-6	[gemSpec_Popp_Modul#8.2]	Offener Punkt: OP-PoPP-6 (Bezeichnung von Kassen-Systemen als Primärsysteme) Die Erläuterung zum Eintrag Primärsystem bezeichnet auch die Systeme der Kassen, die einen PoPP-Client zum PoPP-Token-Abruf implementiert haben, als Primärsysteme. Konkret: "Primärsystem- Primärsystem im Kontext der Spezifikation umfasst alle Systeme, die ein PoPP-Token vom PoPP-Service erhalten. Unter Primärsystem fallen demnach PVS, AVS und KIS sowie Systeme von Kostenträgern." Vorgehen: Wenn es im Rahmen der Kommentierung keinen Widerspruch -von Kostenträgern- dazu gibt, würde der offene Punkt geschlossen werden und die aktuell gewählte Formulierung verwendet.
OP-PoP P-7	[gemSpec_Popp_Modul#9.5.3]	Offener Punkt: OP-PoPP-7 (PoPP-Token Abruf -Step 16: Push Notification) Die aktuelle ZETA-Spezifikation (in Kommentierung) legt fest, dass der ZETA Client bzw. das ZETA SDK die Push-Nachricht verarbeitet und den Klartext-Payload an die aufrufende App übergibt. Dazu gibt es auf Detailebene noch offene Punkte, bspw. kann das PoPP-Modul den Inhalt der Nachricht modifizieren? Z.B. kommt die MessageID und der Status zu einem Online Check-in, angezeigt soll aber ein Text, z.B. "Der Check-in bei <LEI> war erfolgreich", wenn status = success zurück kommt. Vorgehen: Prüfung und Abstimmung innerhalb der gematik parallel zur Kommentierung. Das Ergebnis wird über einen Eigenkommentar der gematik veröffentlicht und in die betroffenen Spezifikationen eingearbeitet

OP-PoP P-8	4.1.13 [gemSpec_PoPP-Service#4.5.3]: PoPP-Token bei Online Check-in	Offener Punkt: OP-PoPP-8 (Berücksichtigung der WebSocket-Schnittstelle in AF_10390) Mit Einführung der Schnittstelle [I_PoPP_Service_mobile_Token_Generation_async.yaml] steht neben REST auch eine WebSocket-basierte Zustellung von PoPP-Token zur Verfügung. Der Anwendungsfall AF_10390 beschreibt bislang den REST-basierten Abruf. Zu prüfen ist, ob AF_10390 um die WebSocket-Nutzung erweitert werden kann oder ein eigener Anwendungsfall erforderlich ist. Dabei sind insbesondere die Token-Zustellung über bestehende Verbindungen, die Zuordnung von Telematik-ID und WorkplaceID sowie das Zusammenspiel von REST und WebSocket zu betrachten. Vorgehen: Erstellung eines neuen Anwendungsfalls oder Erweiterung von AF-10390 parallel zur Kommentierung. Das Ergebnis wird über einen Eigenkommentar der gematik veröffentlicht und in die Spezifikationen eingearbeitet.	

Gelöscht