

Telematikinfrastruktur 2.0

Feature: PoPP Stufe 2 - Online Check-in

Version: 1.0.0 CC4
Revision: 1713069
Stand: 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	26.01.202 6		initiale Einarbeitung	gematik
1.0.0 CC2	11.05.202 6			gematik
1.0.0 CC3	05.08.202 6		zur Abstimmung	gematik
1.0.0 CC4	03.09.202 6		zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments.....	6
1.1 Einordnung Konzeptsdokumente.....	6
1.2 Zielsetzung.....	6
1.3 Zielgruppe.....	6
1.4 Abgrenzungen.....	7
1.5 Methodik.....	7
1.5.1 Epic und User Story.....	7
1.5.2 Anforderungen.....	7
2 Konzept.....	9
2.1 Komponenten und Rollen.....	10
2.1.1 Anwendungen und Zusammenspiel der Komponenten.....	10
2.1.2 Authentifizierung.....	11
2.1.3 Ermittlung der Telematik-ID.....	11
2.1.4 PoPP-Modul.....	12
2.1.5 Informationen zum Inhaber der Telematik-ID: QR-Code / WorkplaceID.....	12
2.1.6 PoPP-Client.....	13
2.1.7 PoPP-Service.....	13
2.2 Abläufe (Workflows).....	13
2.2.1 Vor-Ort in Versorgungseinrichtung.....	15
2.2.2 Mobile Versorgung (beispielsweise Haus-/Heimbesuch).....	16
2.2.3 Fernversorgung (beispielsweise Videosprechstunde).....	16
2.2.3.1 <i>Online Check-in über eine Anbieter-App mit Nutzung einer Kassen-App</i> <i>(App2App).....</i>	16
2.3 Sicherheit.....	16
2.4 Technischer Workflow: Verarbeitung von Daten des Inhabers der Telematik-ID.....	17
2.4.1 Verarbeitung Telematik-ID.....	17
2.4.2 Verarbeitung WorkplaceID.....	18
2.5 Nicht Bestandteil des Dokuments.....	18
3 Einordnung in die Telematikinfrastruktur.....	19
4 Spezifikation.....	20
4.1 Änderungen in [gemSpec_Popp_Service].....	20
4.1.1 [gemSpec_PoPP_Service#2.1]: Überblick zum Ablauf eGK und GesundheitsID aus Versichertensicht.....	20
4.1.2 [gemSpec_PoPP_Service#2.2]: Überblick der Anwendungsfälle für die Ausstellung von PoPP-Token.....	20
4.1.3 [gemSpec_PoPP_Service#2.3]: Akteure und Rollen.....	23
4.1.3.1 [gemSpec_PoPP_Service#2.3.1.6]: Hersteller PoPP-Modul.....	23
4.1.3.2 [gemSpec_PoPP_Service#2.3.1.7]: Hersteller App.....	24
4.1.4 [gemSpec_PoPP_Service#3]: Systemkontext PoPP-Service.....	24

80	4.1.5 [gemSpec_PoPP_Service#3.1]: Produktzerlegung und Außenschnittstellen.....	24
81	4.1.6 [gemSpec_PoPP_Service#3.2]: Systemkontext.....	26
82	4.1.7 [gemSpec_PoPP_Service#3.3]: Nachbarsysteme.....	29
83	4.1.8 [gemSpec_PoPP_Service#4]: Funktionale Anwendungsfälle des PoPP-Service..	30
84	4.1.9 [gemSpec_PoPP_Service#4.1]: Übersicht der Systemanwendungsfälle für die	
85	Ausstellung des PoPP-Token.....	30
86	4.1.10 Neues Kapitel [gemSpec_PoPP_Service#4.5]: Online Check-in und Ausgabe	
87	des PoPP-Token.....	32
88	4.1.11 Neues Kapitel 4.5.1: Auswahl des Inhabers der Telematik-ID für den Online	
89	Check-in.....	34
90	4.1.11.1 Neues Kapitel 4.5.1.1: Zugang zum FHIR-VZD.....	34
91	4.1.11.2 Neues Kapitel 4.5.1.2: Ermittlung von Informationen zum Inhaber der	
92	Telematik-ID.....	35
93	4.1.12 Neues Kapitel 4.5.2: Online Check-in mit GesundheitsID.....	35
94	4.1.13 Neues Kapitel 4.5.3: PoPP-Token bei Online Check-in.....	42
95	4.1.14 Neues Kapitel 4.5.5: Status der PoPP-Token-Erstellung nach Online Check-in	
96	ermitteln.....	48
97	4.1.15 Änderungen [gemSpec_PoPP_Service#5.2]: 5.2 Datenschutz und Sicherheit.	51
98	4.1.16 Änderungen [gemSpec_PoPP_Service#5.4]: ZETA Guard im PoPP-Service....	51
99	4.1.17 Änderungen [gemSpec_PoPP_Service#5.4.1]: Bereitstellung, Konfiguration	
100	und Verwendung vom ZETA Guard.....	52
101	4.1.18 Neues Kapitel [gemSpec_PoPP_Service#5.4.2]: Versand von Push-Notification	
102	über ZETA Guard an das Smartphone des Versicherten.....	53
103	4.1.19 Änderungen [gemSpec_PoPP_Service#5.6]: Federation Entity Statement.....	53
104	4.1.20 Änderungen in [gemSpec_PoPP_Service#6.1.2]: Schnittstelle für Token-Abrufe	
105		56
106	4.1.20.1 PoPP-Token Abruf nach eGK-Anbindung durch LEI.....	57
107	4.1.20.2 PoPP-Token Abruf nach Online-Check-in.....	57
108	4.1.20.2.1 REST-Betrieb.....	57
109	4.1.20.2.2 WebSocket-Betrieb.....	57
110	4.2 Änderungen in [gemILF_PoPP_Client].....	58
111	4.2.1 Erzeugung und Verwendung statischer QR-Codes für PoPP.....	58
112	4.2.2 WorkplaceID.....	61
113	4.2.3 Verbindung zum PoPP-Service herstellen und PoPP-Token abrufen.....	61
114	4.3 Änderungen in [api-popp].....	63
115	4.4 Änderungen in [gemSpec_ZETA].....	64
116	4.5 Änderungen in [gemKPT_Test].....	64
117	4.5.1 Änderungen im Kapitel 7.4 Interoperabilität.....	64
118	4.6 Änderungen in [gemSpec_IDP_Sek].....	65
119	4.7 Änderungen in [gemSpec_Perf].....	66
120	4.8 Änderungen in [gemKPT_Betr].....	68
121	5 Dokumentenhaushalt.....	69
122	6 Anhang A - Verzeichnisse.....	70
123	6.1 Abkürzungen.....	70
124	6.2 Glossar.....	70
125	6.3 Abbildungsverzeichnis.....	73
126	6.4 Tabellenverzeichnis.....	74

127	6.5 Referenzierte Dokumente.....	74
128	6.5.1 Dokumente der gematik.....	74
129	6.5.2 Weitere Dokumente.....	75
130	7 Anhang B - Anforderungshaushalt.....	77
131	7.1 Umsetzungsanforderungen.....	77
132	7.2 Blattanforderungen/ spezifische Festlegungen.....	77
133	8 Anhang C - Offene Punkte, Fragen.....	78
134	8.1 Offene Punkte.....	78
135		
136		

1 Einordnung des Dokuments

Dieses Feature-Dokument beschreibt das Konzept und die Anforderungen von PoPP Service Stufe 2: Online Check-in. Neben diesem Feature-Dokument ist auch die 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.

1.2 Zielsetzung

Dieses Feature-Dokument dient Herstellern, Anbietern und Herstellern des PoPP-Services als Orientierung und bietet eine konsolidierte Übersicht über neue Anforderungen für den Online Check-in beim PoPP-Service. Dies betrifft alle Szenarien, in denen ein Versicherter sein 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).

1.3 Zielgruppe

Dieses Dokument richtet sich an:

1. 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 Fachdiensten, die PoPP-Token nutzen.

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 Spezifikation [gemSpec_PoPP_Service].

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

Die konzeptionellen Anteile dieses Feature-Dokuments (2- Konzept) verbleiben in [gemF_PoPP_Online_Check-in]. Dieses wird 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.

1.5 Methodik

1.5.1 Epic und User Story

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.

1.5.2 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, DiGA, Kostenträger) und Versicherten (VER). Neu eingeführt wird mit Stufe 2 der Online Check-in für PoPP, der direkt am Smartphone des Versicherten erfolgt. Dieser ermöglicht die Nutzung einer GesundheitsID in allen Versorgungsszenarien, also auch vor-Ort in einer Versorgungseinrichtung.

Ziel ist es, den Zugang zu Versichertendaten auch in allen Versorgungsszenarien für Inhaber einer Telematik-ID zu ermöglichen und zusätzlich den 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 [gemSpec_PoPP_Service] generiert wird und berechtigten Inhabern einer Telematik-ID den Zugriff auf die Versichertendaten in Fachdiensten ermöglicht.

Der Prozess für den Online Check-in wird vom 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 Telematik-ID via App bei dem sich VER einchecken möchte,
3. zum Ausweisen eine GesundheitsID.

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

1. Dies kann erfolgen durch
 - a. das Scannen eines statischen QR-Codes (beinhaltet die Telematik-ID) 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 die VER mithilfe seiner GesundheitsID aus.
3. Abschließend wird der PoPP-Token im PoPP-Service Resource Server erstellt und der PoPP-Service stellt dem Inhaber der Telematik-ID den PoPP-Token für den Zugriff auf die Versichertendaten in den Fachdiensten zur Verfügung.

Der Online Check-in vermittelt der verwendeten App keinen Zugriff auf Versichertendaten. Der Zugriff auf die Versichertendaten bleibt, wie bereits in Stufe 1, ausschließlich dem berechtigten Inhaber der vom Versicherten ausgewählten Telematik-ID vorbehalten. PoPP-Token gelangen zu keinem Zeitpunkt in den 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 GesundheitsID in verschiedenen Versorgungsszenarien sowie die Aufgaben, bzw. Rollen der unterschiedlichen 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 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. Die vollständigen Abläufe sowie die detaillierten Anforderungen werden in [gemSpec_PoPP_Service] und [gemSpec_PoPP_Modul] beschrieben.

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

2.1 Komponenten und Rollen

2.1.1 Anwendungen und Zusammenspiel der Komponenten

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 Krankenversicherungen,
2. Apps von Leistungserbringern, etwa Apotheken,
3. Videosprechstunden-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 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 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.

Online Check-in aus einer Webanwendung

Die VER startet den Online Check-in in einer Webanwendung, beispielsweise einem Patientenportal oder einer Videosprechstunden-App. Die Webanwendung übergibt die notwendigen Informationen an die Kassen-App. Der eigentliche Online Check-in wird anschließend durch das PoPP-Modul der Kassen-App durchgeführt. Sofern die Telematik-ID bereits durch die Webanwendung festgelegt wurde, kann eine erneute Auswahl des Inhabers einer Telematik-ID entfallen.

2.1.2 Authentifizierung

Die Authentifizierung für den Online Check-in erfolgt mit der GesundheitsID auf dem Smartphone.

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

2.1.3 Ermittlung der Telematik-ID

VER wählen den Inhaber einer Telematik-ID aus, bei der sie online einchecken wollen. Die Telematik-ID lässt sich auf verschiedene Weise durch einen Versicherten erfassen:

1. **Scannen eines QR-Codes:** Ein statischer QR-Code, der die Telematik-ID beinhaltet, wird vom Inhaber der Telematik-ID etwa als Aufsteller am Empfang bereitgestellt.
2. **Hinterlegung in Apps:** Die Telematik-ID wird vom Inhaber der Telematik-ID direkt in der Anbieter-App hinterlegt, beispielsweise in einem Patientenportal oder einer Apotheken-App.
3. **Manuelle Ermittlung über VZD-Suche in der App:** Der Inhaber der 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 Inhabers der 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

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 gemäß der Zero-Trust-Architektur der TI. Hierzu nutzt die Kassen-App mit integriertem PoPP-Modul einen ZETA Client, der die gesicherte Kommunikation mit dem ZETA Guard des PoPP-Service ermöglicht. Sämtliche Kommunikation zwischen PoPP-Modul und PoPP-Service Resource Server erfolgt über diese Sicherheitsarchitektur.

2.1.5 Informationen 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 Erfassung der Telematik-ID. Dies erfolgt, indem ein QR-Code aus der App, in der der Online Check-in integriert ist, von den Versicherten abgescannt wird.

Zusätzlich kann der QR-Code weitere Informationen enthalten, etwa eine optionale WorkplaceID, die 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 eines Versicherten direkt dem richtigen Arbeitsplatz zugeordnet werden kann.
2. **SessionID:** Die WorkplaceID kann zusammen mit der Telematik-ID auch in Anbieter-Apps hinterlegt werden, um als SessionID eine richtige Zuordnung zwischen Aktionen in einer App des Versicherten und dem PoPP-Token nach dem erfolgreichen Online Check-in im PS des Inhabers der Telematik-ID zu gewährleisten.

Der Inhaber der Telematik-ID muss dazu einmalig einen QR-Code im Primärsystem (PS) generieren. Optional kann für jeden Arbeitsplatz ein separater QR-Code mit einer spezifischen WorkplacelD erstellt werden. QR-Codes können 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 Kassen-App aus dem Verzeichnisdienst (VZD), den Favoriten oder der Historie ohne eine dort hinterlegte WorkplacelD, so wird auch keine WorkplacelD übermittelt und entsprechend nicht verarbeitet.

2.1.6 PoPP-Client

Die grundlegende Aufgabe des PoPP-Clients bleibt im Vergleich zur Stufe 1 unverändert, nämlich die Verarbeitung und Verwaltung von PoPP-Token zum Zugriff des Inhabers der Telematik-ID auf 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 1 unverändert. Im PoPP-Service werden PoPP-Token erzeugt und nach erfolgreicher Authentifizierung des Inhabers der Telematik-ID sowie nach dem Ausweisen des Versicherten an das Primärsystem des Inhabers der Telematik-ID übermittelt.

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

2.2 Abläufe (Workflows)

Zunächst wird der Online Check-in mit Kassen-App, PoPP-Modul und GesundheitsID in einer Versorgungseinrichtung tabellarisch 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 Heimbesuch),
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 Heimbesuch) 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.

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=mZ0JER1Gw4OVpZoG-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=mZ0JER1Gw4OVpZoG-9&scaling=scale-down&content-scaling=fixed&starting-point-node-id=2535%3A5273)

Tabelle 1: Ablauf Online Check-in

ID	Beschreibung
Einstieg	VER öffnet Kassen-App auf einem Smartphone beim Betreten der Versorgungseinrichtung. Alternativ VER checkt über eine Anbieter-App ein, zum Beispiel zuhause mit einer Videosprechstunden-App.
Check-in	VER wählt die Funktion "Online Check-in" in der Kassen-App aus.
Auswahl desInhabers der Telematik-ID	DerInhaber der Telematik-ID stellt einen statischen QR-Code (etwa Zettel, Bildschirm) am Empfang sichtbar bereit. Der QR-Code enthält die Telematik-ID. VER scannt den QR-Code. Alternativ, wenn beispielsweise in der Fernversorgung kein QR-Code gescannt werden kann: VER wählt manuell denInhaber 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 Telematik-ID bereits in der Anbieter-App hinterlegt ist, beispielsweise bei einer Apotheken-App.
Einwilligungen	VER wird in der App der Name desInhabers der Telematik-ID inklusive Adresse angezeigt, welche zur ausgewählten Telematik-ID gehört; via VZD-Abruf VER bestätigt nach der Kontrolle den Online Check-in.
Authentifizierung	Falls noch keine Authentifizierung erfolgt ist, weist sich VER am Smartphone über die GesundheitsID in der Kassen-App (Authenticator Modul) 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 Informationen zur Art der durchgeführtenAuthentifizierung, an den PoPP-Service.
PoPP-Token-Erstellung und	PoPP-Service prüft die Daten und speichert diese in einem temporären Datensatz. Das Primärsystem desInhabers der

Abholung	Telematik-ID fragt bei PoPP-Service an, anschließend generiert dieser ein PoPP-Token und das Primärsystem 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 beim ausgewählten Inhaber der Telematik-ID bestätigt. Versicherten kann auch angezeigt werden, dass der Online Check-in noch ausstehend ist, beispielsweise wenn der Inhaber der Telematik-ID bei einer Fernversorgung noch nicht online ist. In diesem Fall kann eine Statusänderung auch nachträglich übermittelt und dem Versicherten angezeigt werden.
Abschluss	Der Inhaber der Telematik-ID erhält das PoPP-Token, um auf Versichertendaten in den Fachdiensten zuzugreifen.

2.2.1 Vor-Ort in Versorgungseinrichtung

Inhaber der Telematik-ID nutzt eGK (UC_PoPP_1a)

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

VER nutzt GesundheitsID (UC_PoPP_1b)

Für den Online Check-in vor Ort in einer Versorgungseinrichtung wird die GesundheitsID verwendet.

Der bevorzugte Weg in diesem Versorgungsszenario ist das Einchecken über eine Kassen-App und das Scannen eines QR-Codes durch die Versicherten, es lassen sich auch Anbieter-Apps verwenden. Die Nutzung der GesundheitsID erfordert bei Verwendung von Anbieter-Apps stets einen Wechsel in die Kassen-App mit Authentifizierungsmodul.

Abschließend übermittelt der PoPP-Service den PoPP-Token in das PS 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 Referenzpfad. Ablauf des Referenzpfad ist visuell als Click-Dummy aufrufbar: <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)

Inhaber der Telematik-ID nutzt eGK (UC_PoPP_2a)

Bereits mit 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 der Inhaber der Telematik-ID den QR-Code mit zum Versicherten nimmt.

2.2.3 Fernversorgung (beispielsweise Videosprechstunde)

2.2.3.1 Online Check-in über eine Anbieter-App mit Nutzung einer Kassen-App (App2App)

UC_PoPP_3b (GesundheitsID)

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

Im Anschluss übermittelt der PoPP-Service den PoPP-Token in das PS desInhabers der Telematik-ID und ermöglicht demInhaber der 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 dem Versicherten in der App und dem PoPP-Token im PS desInhabers der Telematik-ID ermöglichen (bspw. für Online-Dienste von Apotheken).

- Der Ablauf in einer Anbieter-App am Beispiel einer Videosprechstunden-App und mit Nutzung der GesundheitsID: [Link](#)

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

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

2.3 Sicherheit

Folgende Maßnahmen tragen dazu bei, dass genau derInhaber der Telematik-ID den PoPP-Token erhält, welche vom Versicherten für den Zugriff auf ihre Versichertendaten in 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. Diese erkennt falsche QR-Codes und warnt die Versicherten und verweist an das Personal des Inhabers der Telematik-ID.

2. Bestätigung für VER

Die VER muss vor dem eigentlichen Online Check-in zunächst denInhaber der Telematik-ID bestätigen. Hierzu erfolgt ein VZD-Abruf der erfassten Telematik-ID mit anschließender Anzeige des Namens desInhabers der 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 Telematik-ID.

3. Verantwortung für QR-Code-Inhalte

Der statische QR-Code wird im PS erzeugt und in den Räumlichkeiten des Inhabers der Telematik-ID aufgestellt bzw. präsentiert. DerInhaber 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 lediglich die Telematik-ID. Beispielsweise die Krankenversicherungsnummer (KVNR) oder andere persönliche Daten der Versicherten werden nicht benötigt.

5. Unterscheidung und Sperrbarkeit von PoPP-Modulen

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

6. Information über die Authentifizierung

Der PoPP-Token enthält die Information, ob der Online Check-in über ein App mit PoPP-Modul vom Versicherten durchgeführt wurde und auf welche Weise die Identität des Versicherten verifiziert wurde, also mittels GesundheitsID. Unter anderem wird diese Information von den Fachdiensten für die Zugriffsregelung genutzt.

**2.4 Technischer Workflow: Verarbeitung von Daten des Inhabers
der Telematik-ID**

Es gelten folgende Regelungen und Maßnahmen für die Verarbeitung von der Telematik-ID und WorkplacelID bei PoPP.

Die WorkplacelID ist nicht Teil des PoPP-Tokens und hat keinen Einfluss auf die Berechtigung des Inhabers der 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, damit der PoPP-Service darüber informiert ist, für welchen Inhaber der Telematik-ID ein PoPP-Token auszustellen ist.
3. Der PoPP-Service prüft anhand der Telematik-ID, ob der zugehörige Inhaber der Telematik-ID authentisiert ist, und verwendet die Informationen zur Erstellung eines PoPP-Tokens.
4. Der PoPP-Token wird an das Primärsystem desInhabers der Telematik-ID übermittelt.

2.4.2 Verarbeitung WorkplacelID

1. Die WorkplacelID wird lediglich im Primärsystem desInhaber der Telematik-ID verwendet. Daher wird die WorkplacelID als (transparenter) Parameter durch den PoPP-Service geschleust.
2. Die WorkplacelID darf weder im PoPP-Modul noch durch den PoPP-Service verändert werden.
3. Die Übergabe der WorkplacelID erfolgt gemeinsam mit der Telematik-ID als Parameter des HTTP-Requests vom PoPP-Modul an den PoPP-Service.

- 548 4. Der PoPP-Service bewahrt die Information WorkplaceID gemeinsam mit der Telematik-
549 ID auf.
- 550 5. Bei der Übermittlung des PoPP-Tokens an denInhaber einer Telematik-ID übergibt der
551 PoPP-Service die Information zur WorkplaceID innerhalb der HTTP-Nachricht, mit der
552 der PoPP-Token übermittelt wird. Die WorkplaceID ist nicht Teil des PoPP-Tokens.
- 553 6. Der PoPP-Service übermittelt die WorkplaceID an das Primärsystem, wenn er sie zuvor
554 vom PoPP-Modul erhalten hat.
- 555 7. Das Primärsystem prüft, ob eine WorkplaceID in der Nachricht mit dem PoPP-Tokens
556 enthalten ist. Das Primärsystem benutzt eine vorhandene WorkplaceID, um das PoPP-
557 Token an den richtigen Arbeitsplatz zu übermitteln oder eine Zuordnung zwischen
558 Aktionen in einer App der Versicherten und dem PoPP-Token herzustellen.

559 **2.5 Nicht Bestandteil des Dokuments**

560 Die weitere Verwendung des PoPP-Tokens im Primärsystem ist nicht Gegenstand dieses
561 Dokumentes. Die Regelungen zum Zugriff mittels PoPP-Token auf die Versichertendaten
562 erfolgen durch den jeweiligen Fachdienst.

3 Einordnung in die Telematikinfrastruktur

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

Im Primärsystem des Inhabers der Telematik-ID wird ein statischer QR-Code erzeugt und vom Versicherten über eine Kassen-App (PoPP-Modul) gescannt. Der QR-Code stellt hierbei u.a. Informationen bereit, um welche Telematik-ID es sich handelt, bei der sich die 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 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.

Eine Möglichkeit zur Authentifizierung der Versicherten ist, dass sie ihre eGK an einem geeigneten Lesegerät demInhaber der Telematik-ID präsentiert oder die eGK an das Personal des Inhabers der Telematik-ID übergibt. Alles Weitere führt der PoPP-Client durch.

Für den Online Check-in am Smartphone der VER authentifiziert sich die VER mittels GesundheitsID. Beim Online Check-in kommt auf dem 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 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 Inhaber der Telematik-ID wird zudem unterschieden, ob der Versorgungskontext während der physischen Anwesenheit von Versicherten entsteht (vor Ort in einer Versorgungseinrichtung oder bei mobiler Versorgung wie Praxisbesuchen oder Haus-/Heimbesuchen) oder ob derInhaber der Telematik-ID virtuell anwesend ist (bei Fernversorgung wie Videosprechstunden).

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 dessen Räumlichkeiten in Anspruch nehmen. Der 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 des Telematik-ID-Inhabers präsentiert. Nachdem die VER den Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und das PS des Telematik-ID-Inhabers erhält 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 dessen Räumlichkeiten in Anspruch nehmen. Der Inhaber der Telematik-ID benötigt für den Zugriff auf die Daten des physisch anwesenden Versicherten einen Nachweis des Versorgungskontexts. Dazu startet die VER den Online Check-in-Prozess in einer Kassen-App mit integriertem PoPP-Modul, scannt den vom Telematik-ID-Inhaber für den Check-in bereitgestellten QR-Code, bestätigt die Nutzung der Daten durch den Inhaber der Telematik-ID und authentifiziert sich anschließend mittels GesundheitsID. Nachdem die VER den Online Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und das PS des Telematik-ID-Inhabers erhält den notwendigen Nachweis des Versorgungskontexts.
UC_PoPP_2a	In mobiler Versorgung mit <u>eGK</u>: bspw. Haus-/Heimbesuch Ein Versicherter möchte eine Versorgung außerhalb der Räumlichkeiten eines Telematik-ID-Inhabers in Anspruch nehmen. Dazu kommt das Personal des Telematik-ID-Inhabers zum Versicherten. Der 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 des Telematik-ID-Inhabers präsentiert. Nachdem das Personal des Telematik-ID-Inhabers die eGK eingelesen hat, ist der Check-in-Vorgang abgeschlossen und das PS des Telematik-ID-Inhabers erhält den notwendigen Nachweis des Versorgungskontexts.
UC_PoPP_2b	In mobiler Versorgung mit <u>GesundheitsID</u>: bspw. Haus-/Heimbesuch Ein Versicherter möchte eine Versorgung außerhalb der Räumlichkeiten eines Telematik-ID-Inhabers in Anspruch nehmen. Dazu kommt das Personal des Telematik-ID-Inhabers zum Versicherten. Der Inhaber der Telematik-ID benötigt für den Zugriff auf die Daten des physisch anwesenden Versicherten einen Nachweis des Versorgungskontexts. Dazu startet die VER den Online Check-in-Prozess in einer Kassen-App

	mit integriertem PoPP-Modul, scannt den vom Telematik-ID-Inhaber für den Check-in bereitgestellten QR-Code, bestätigt die Nutzung der Daten durch den Inhaber der Telematik-ID und authentifiziert sich anschließend mittels GesundheitsID. Nachdem die VER den Online Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und das PS des Telematik-ID-Inhabers erhält den notwendigen Nachweis des Versorgungskontexts.
UC_PoPP_3a	In Fernversorgung mit <u>GesundheitsID</u>: bspw. Videosprechstunde <i>Online Check-in über Kassen-App mit PoPP-Modul</i> Ein Versicherter möchte virtuell eine Versorgung durch den Inhaber einer Telematik-ID in Anspruch nehmen. Der Inhaber der Telematik-ID benötigt für den Zugriff auf die Daten des Versicherten den Nachweis des Versorgungskontexts. Dazu startet die VER zuvor den Online Check-in-Vorgang in der Kassen-App mit integriertem PoPP-Modul, bestätigt die Nutzung der Daten durch den Inhaber der Telematik-ID und authentifiziert sich anschließend mittels GesundheitsID. Nachdem die VER den Online Check-in-Prozess durchgeführt hat, ist dieser abgeschlossen und das PS des Telematik-ID-Inhabers erhält den notwendigen Nachweis des Versorgungskontexts.
UC_PoPP_3b	In Fernversorgung mit <u>GesundheitsID</u>: bspw. Videosprechstunde <i>Online Check-in über Anbieter-App, die das PoPP-Modul einer Krankenversicherungs-App nachnutzt (App2App)</i> Ein Versicherter möchte virtuell eine Versorgung durch den Inhaber einer Telematik-ID in Anspruch nehmen. Der Inhaber der Telematik-ID benötigt für den Zugriff auf die Daten des Versicherten den Nachweis des Versorgungskontexts. Dazu startet die VER zuvor den Online Check-in Prozess in einer Anbieter-App ohne integriertes PoPP-Modul. Anschließend öffnet sich die Kassen-App mit PoPP-Modul, die VER bestätigt die Nutzung der Daten durch den Inhaber der Telematik-ID und authentifiziert sich mittels GesundheitsID. Nachdem die VER den Online Check-in Prozess durchgeführt hat, ist dieser abgeschlossen und das PS des Telematik-ID-Inhabers erhält 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

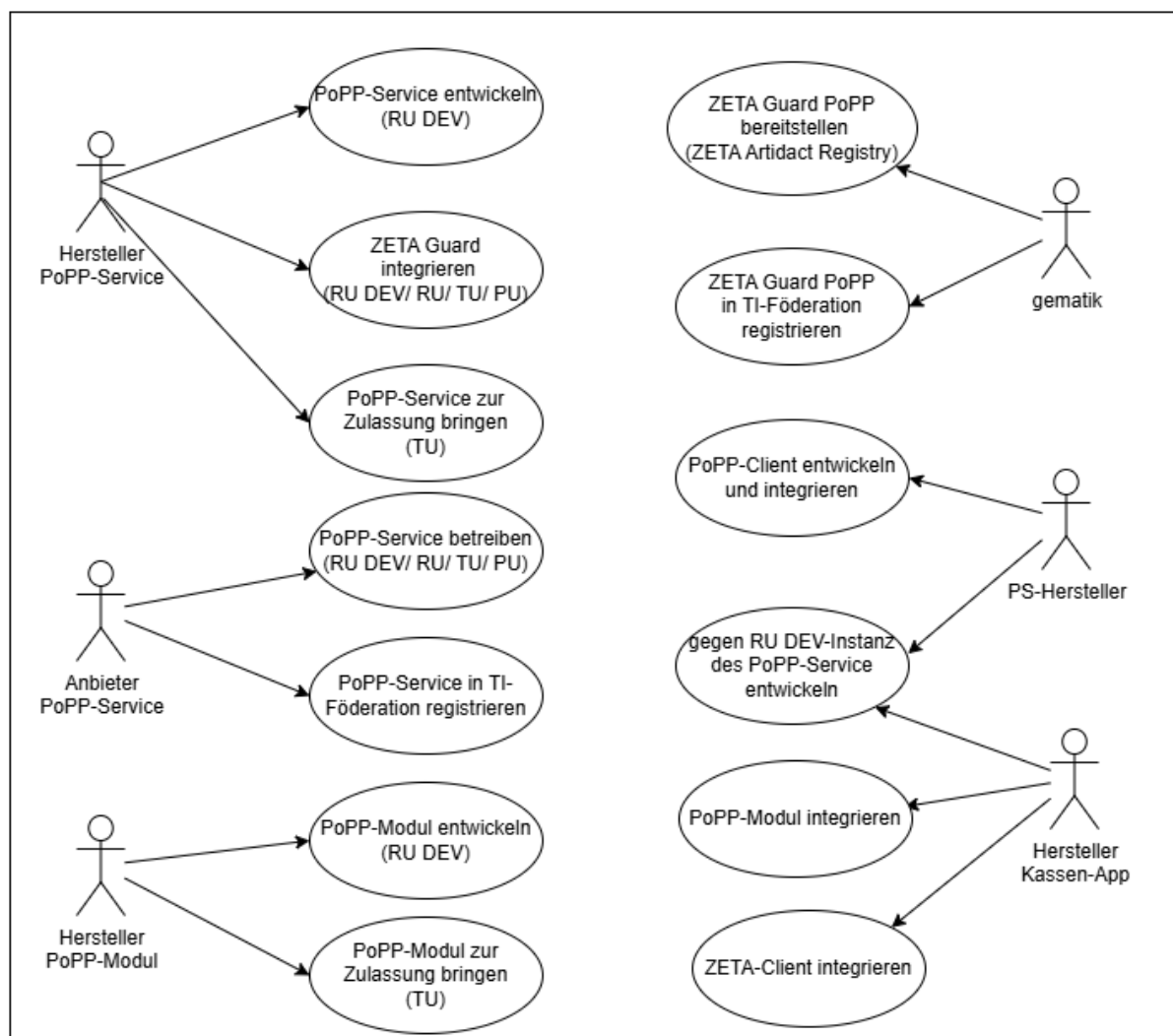


Abbildung 1: Rollen und Akteure bei Herstellung und Betrieb des PoPP-Service

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 VER mit dem PoPP-Service interagieren und das für den Online Check-in verwendet wird. Das PoPP-Modul ist bei Verwendung der GesundheitsID als Modul in einer Kassen-App integriert. Das PoPP-Modul 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

Hersteller von Kassen-Apps integrieren das PoPP-Modul in die Anwendung, welche auch das Authenticator-Modul 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

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 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 bei Verwendung der GesundheitsID in einer Kassen-App auf dem Smartphone des Versicherten integriert sind.

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

Für die Bearbeitung von Requests, bei denen die elektronische Gesundheitskarte (eGK) verwendet wird, sind dies die Komponenten "eGK-Kommunikation" und "eGK-Hash-Datenbank".

Für die Bearbeitung von Online Check-In Requests, in denen VER die GesundheitsID nutzen, wird die Komponente "Online Check-in - glID" 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 zum Inhaber einer 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.

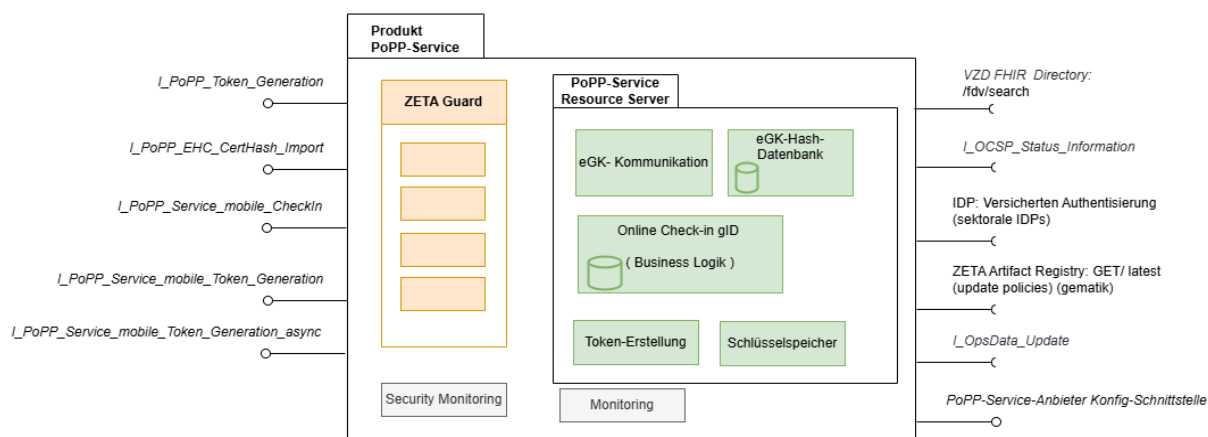


Abbildung 2: Produkttypzerlegung PoPP-Service

Der PoPP-Service stellt folgende Außenschnittstellen bereit:

1. **I_PoPP-Token_Generation** wird vom Primärsystem eines 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.
3. **I_PoPP_Service_mobile_CheckIn** wird vom PoPP-Modul in der APP auf dem Smartphone des Versicherten verwendet. Die Schnittstelle beinhaltet die Aufrufe
 - a. 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.
 - 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 des PoPP-Token Abrufs.
4. **I_PoPP_Service_mobile-Token_Generation** wird vom Primärsystem des Inhabers der Telematik-IDs verwendet, um vom PoPP-Service alle PoPP-Token abzurufen, zu denen ein gültiger unverarbeiteter PoPP-Datensatz aus einem Online Check-in 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 Artifact 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 Telematik-ID für eine bestimmte Telematik-ID oder bestimmte Suchkriterien zum Inhaber einer 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.

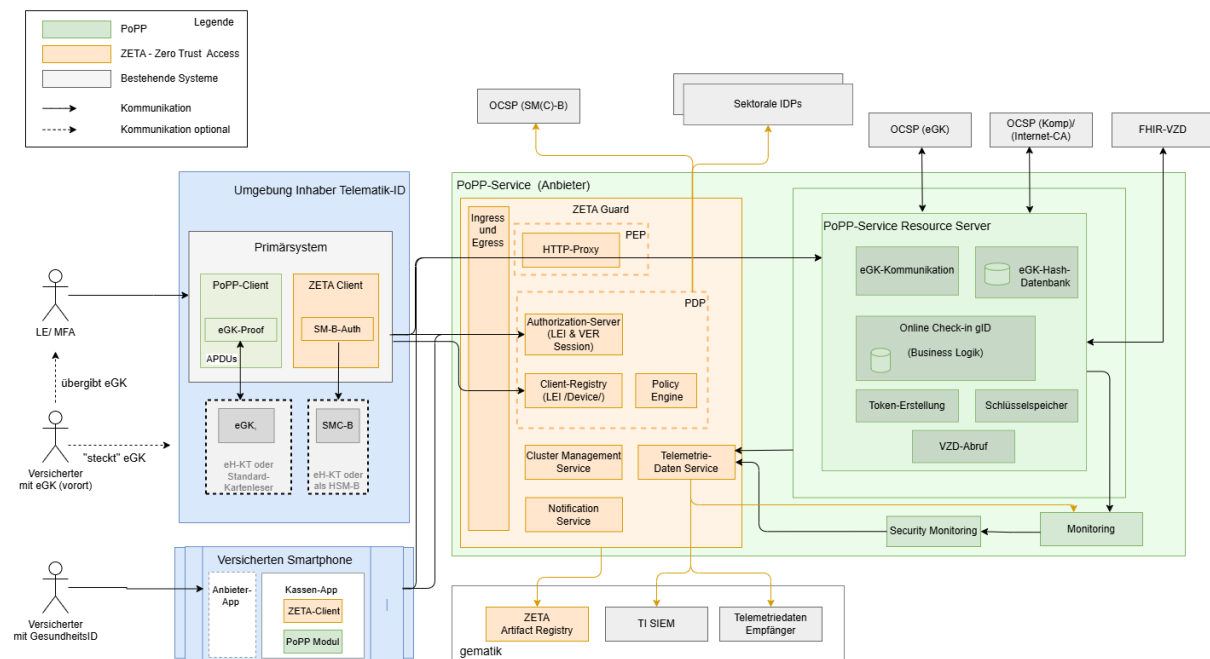


Abbildung 3: Systemkontext PoPP-Service

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

Das PS mit den integrierten Modulen PoPP-Client und ZETA Client triggert über verschiedene Aufrufwege die PoPP-Token-Erstellung, nachdem bspw. 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 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	umfasst folgende Komponenten der PoPP-Lösung:	

	• ZETA Guard • PoPP-Service Resource Server	
ZETA Guard	schützt die Kommunikation zwischen dem PoPP-Service Resource Server und den PoPP-Clients im Primärsystem des Inhabers der Telematik-ID sowie die Kommunikation zwischen PoPP-Modul und PoPP-Service Resource Server. Die Authentifizierung des Inhabers der 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 Verfügung.	[gemSpec_ZETA]
PoPP-Service Resource Server	enthält die eigentliche Businesslogik des PoPP-Service für das Ausstellen von PoPP-Token an das Primärsystem eines Telematik-ID-Inhabers.	
eGK-Kommunikation	enthält die Funktionalitäten für die Token-Erstellung falls VER ihre eGK zur Authentisierung nutzen.	
eGK-Hash-Datenbank	enthält die Datenbank und die steuernde Funktionalität für den Abgleich von anonymisierten eGK-Metadaten	
Online Check-in gID	enthält die steuernde Funktionalität, wenn ein Versicherter einen Online Check-in durchführt.	
Token-Erstellung	enthält die Funktionalität zum Erstellen des PoPP-Token; hier werden die Daten des Telematik-ID Inhabers und dem Versicherten im PoPP-Token zusammengefügt.	
Schlüsselspeicher	enthält die Funktionalität zur	

	sicheren Ablage der verwendeten Schlüssel und zur Speicherung von Daten.	
VZD-Abruf	enthält die Funktion zum Aufruf der FHIR-VZD-Schnittstelle zur Ermittlung von Informationen zum Inhaber einer Telematik-ID. Das Suchergebnis wird vom PoPP-Service dem PoPP-Modul zugestellt.	
Monitoring	sammelt Funktionalitäten für das Eigenmonitoring der verwendeten Systeme zur Überwachung und Analyse des Betriebszustands.	[gemSpec_Perf]
Security Monitoring	enthält Funktionen für das Sicherheits- und Event-Monitoring im PoPP-Service.	[gemSpec_Perf]
Primärsystem (PS)	Bestehende Primärsysteme werden für PoPP erweitert.	
ZETA Client	ist der direkte Kommunikationspartner der ZETA Guard Komponente des PoPP-Service.	[gemSpec_ZETA]
PoPP-Client	ist der direkte Kommunikationspartner des PoPP-Service im PS des Inhabers einer Telematik-ID.	[gemILF_PoPP_Client]
App	App ist eine Kassen-App oder Anbieter-App (Smartphone-App, Desktop-Anwendung, Browser-Anwendung), die von einem Versicherten mit GesundheitsID online genutzt wird.	
ZETA Client	ist der direkte Kommunikationspartner der ZETA Guard Komponente des PoPP-Service.	
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. Sektorale IDPs:
verantwortlich für die Authentisierung eines Versicherten mit GesundheitsID,
2. FHIR-VZD:
im Internet verfügbar zum Abruf von Informationen zum Inhaber einer Telematik-ID,
3. OCSP (SM(C)-B):
im Internet verfügbar für die OCSP-Prüfung von SM(C)-B durch den ZETA Guard,
4. OCSP (eGK):
im Internet verfügbar für die OCSP-Prüfung von eGK durch den PoPP-Service,
5. 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 APDU im eGK-Ablauf, sowie für die OCSP-Prüfung des TLS-Internet-Zertifikats des PoPP-Service (für die Client-Schnittstelle),
6. Die gematik stellt folgende Dienste bereit:
"ZETA Artifact Registry" als Repository für die ZETA Guard Images, den "Telemetriedaten Empfänger" und Telematikinfrastruktur Security Information and Event Management (TI-SIEM).

Die für PoPP erforderlichen OCSP-Responder (SM(C)-B, 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-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, konkret:
 - a. VSDM 2.0,
 - b. ePA für alle,
 - c. E-Rezept.
2. 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 GesundheitsID resultieren, wie der Anwendungsfall eines Check-in mit eGK vor-ort in den Räumlichkeiten des Telematik-ID-Inhabers, in der Ausstellung eines PoPP-Token für die den Inhaber einer Telematik-ID.

Neben der Erstellung eines PoPP-Token wird auch die Registrierung des Primärsystems und Anmeldung des Inhabers der 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 Telematik-ID:
 - a. AF_10402* ist immer Voraussetzung für die Ausgabe eines PoPP-Token
2. Anwendungsfälle zur Authentisierung Versicherter:
 - 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
3. Anwendungsfälle zur Ausgabe eines PoPP-Tokens an das PS 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

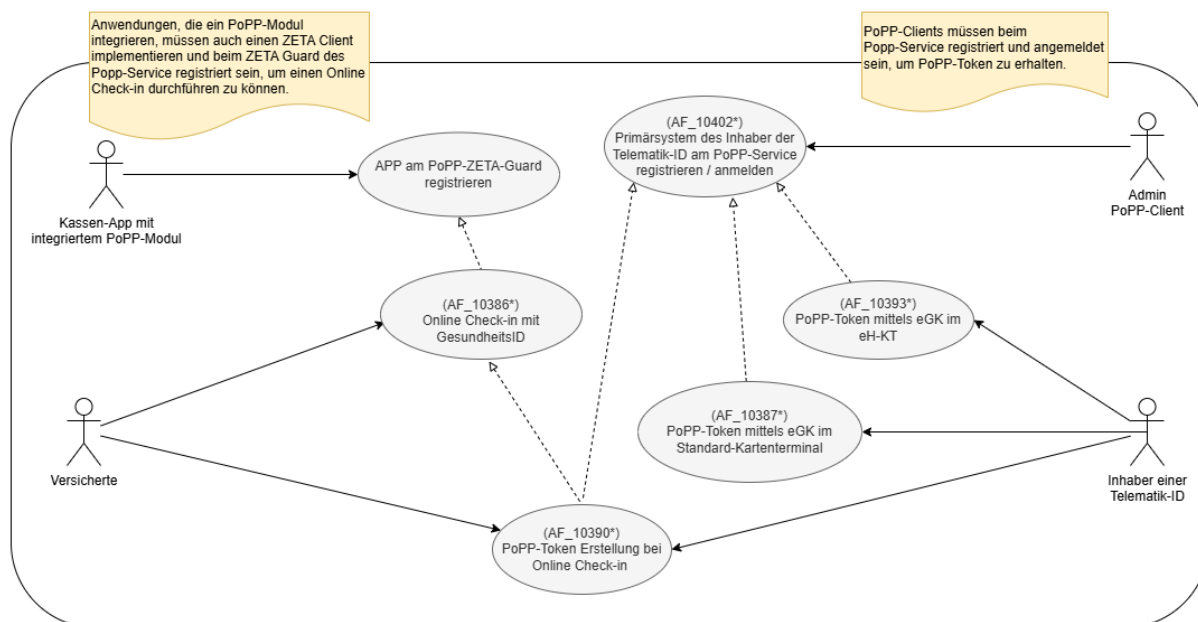


Abbildung 4: Anwendungsfälle zur Attestierung des Versorgungskontexts

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

810 **Tabelle 4: Zuordnung der Anwendungsfälle zu den Use Cases**

Anwendungs-fall	Kurzbeschreibung	technische Anwendungsfälle
UC_PoPP_1a	PoPP-Token bei physischer Anwesenheit beim Inhaber der Telematik-ID / vor Ort - eGK	1. zunächst AF_10402*- Primärsystem 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 beim Inhaber der Telematik-ID / vor Ort - GesundheitsID	1. zunächst AF_10402*- Primärsystem 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 Umgebung des Inhabers der Telematik-ID / Hausbesuch - eGK	Identisch zu UC_PoPP_1a
UC_PoPP_2b	PoPP-Token bei physischer Anwesenheit außerhalb der Umgebung des Inhabers der Telematik-ID / Hausbesuch - GesundheitsID	Identisch zu UC_PoPP_1b
UC_PoPP_3a	PoPP-Token ohne physische Anwesenheit beim Inhaber der Telematik-ID / GesundheitsID - Check-in mit Anbieter-App oder Browser-Anwendung	Identisch zu UC_PoPP_1b
UC_PoPP_3b	PoPP-Token ohne physische Anwesenheit beim Inhaber der Telematik-ID / GesundheitsID - Check-in mit Kassen-App	Identisch zu UC_PoPP_1b

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

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 einen Inhaber einer Telematik-ID im PoPP-Service Resource Server initiiert.

Starten VER den Check-in-Prozess über das in eine Kassen-App integrierte PoPP-Modul, so ist eine Authentisierung mit GesundheitsID möglich.

Über das in eine Kassen-App integrierte PoPP-Modul ist eine Auswahl des Inhabers einer Telematik-ID für den Online Check-in möglich. Die Auswahl des Inhabers einer Telematik-ID kann über das Auswerten 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 zum Inhabers einer Telematik-ID an das PoPP-Modul zu ermitteln.

Nach erfolgreicher Authentisierung der Versicherten mit GesundheitsID wird vom PoPP-Service Resource Server ein Datensatz zur Erstellung eines PoPP-Token erzeugt. Ist das Primärsystem des betroffenen Inhabers der Telematik-ID online (d.h. sie ist zu dem Zeitpunkt authentifiziert), so wird das PoPP-Token erstellt und dem Primärsystem zugestellt. Ist 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 Smartphone des Versicherten darstellen. Sollte der Check-in nicht erfolgreich sein, wird die VER auch darüber informiert.

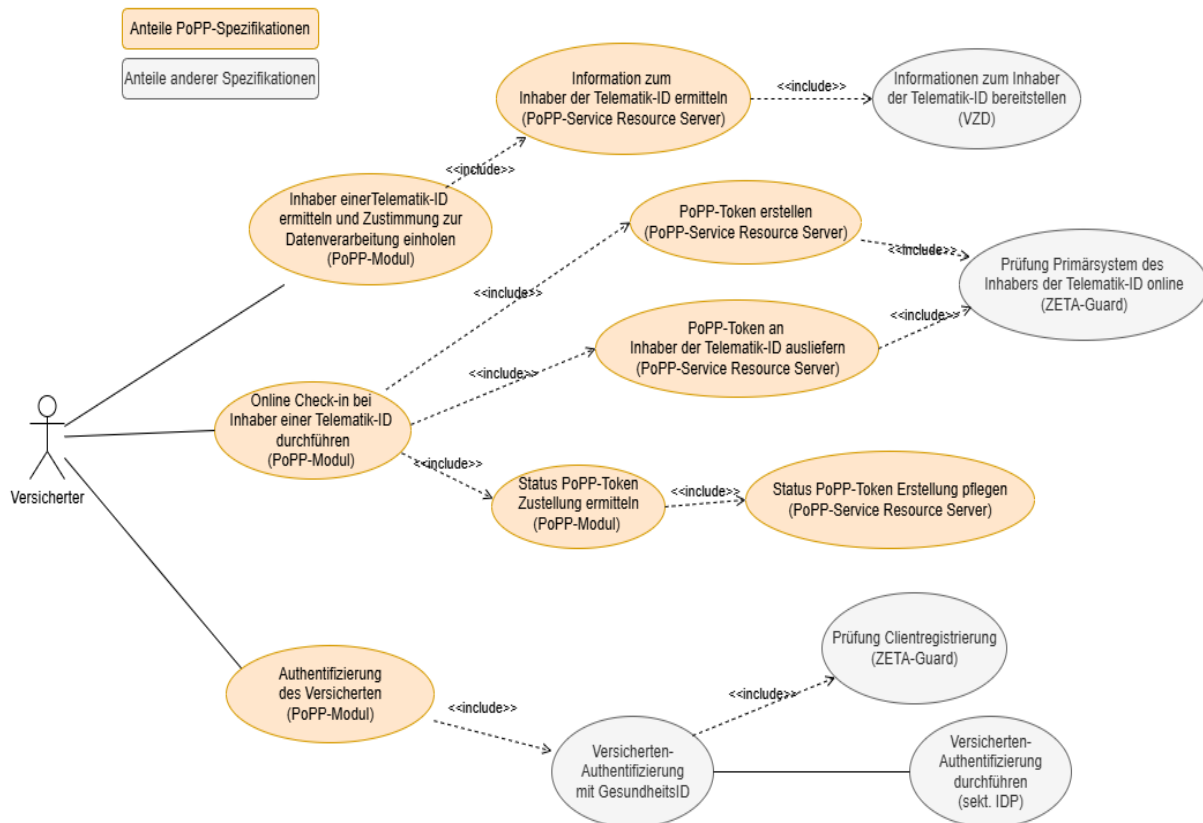


Abbildung 5: Use-Case-Übersicht Online Check-in aus einer App mit integriertem PoPP-Modul

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
	Die VER startet mit der Kassen-App über einen Eintrag in der GUI den "Online Check-in" Prozess
Inhaber der Telematik-ID ermitteln und Zustimmung zur Datenverarbeitung	Der Online Check-in startet mit der Auswahl des Inhabers der Telematik-ID. Die Auswahl des Inhabers der Telematik-ID kann z.B. erfolgen durch: 1. Scannen eines QR-Code durch die Versicherten über eine Funktion in der App 2. Darstellen einer Auswahlliste in der App und Auswahl des Inhabers der Telematik-ID durch den Versicherten 3. Visualisierung eines fest zugeordneten Inhabers einer Telematik-ID durch die App Die VER stimmt zu, dass seine KVNR an dem Inhaber der

	Telematik-ID übermittelt wird.
Information zum Inhaber der Telematik-ID ermitteln	Die Prüfung einer Telematik-ID und die Ermittlung der Informationen zum Inhaber der Telematik-ID (Name, Adresse, ..) wird durch den PoPP-Service Resource Server über eine Abfrage am VZD durchgeführt.
Check-in 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 der Inhaber der Telematik-ID online ist, 4. die Übertragung des PoPP-Token an den Inhaber der Telematik-ID, wenn dieser online ist.
Authentifizierung	Die Authentifizierung mit GesundheitsID wird durch den GesundheitsID-Flow über die sektoralen IDPs abgebildet.

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

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

Die Abläufe zur Auswahl der Telematik-ID, einer Suche im FHIR-VZD, der Aufbereitung der 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 ist anschließend in der Lage unter Angabe der Client-Credentials Zugangstoken für den Zugang zum FHIR-VZD abrufen.
[<=]

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

Der PoPP-Service DARF Zugangstoken für den Zugang zum FHIR-VZD NICHT verwenden, wenn diese älter als 24 Stunden sind.[<=]

4.1.11.2 Neues Kapitel 4.5.1.2: Ermittlung von Informationen zum Inhaber der Telematik-ID

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

Der PoPP-Service MUSS eine Schnittstelle gemäß [I_PoPP_Service_mobile_CheckIn.yaml] zur Ermittlung von Informationen zum Inhaber einer 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. [≤]

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*. [≤]

4.1.12 Neues Kapitel 4.5.2: Online Check-in mit GesundheitsID

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

Wurde die Telematik-ID ermittelt, bei welcher VER einen Online Check-in durchführen möchte und nachdem VER der Datennutzung durch den Inhaber der Telematik-ID zustimmte, authentifiziert sich VER mit ihrer GesundheitsID, um sich 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 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 "[Detaillierter Ablauf der PoPP-Token Generierung durch Authentifizierung Versicherter über ihre GesundheitsID](#)" von [gemSpec_PoPP_Modul] dargestellt.

AF_10386-01 -Online Check-in mit GesundheitsID

Attribute	Bemerkung
Beschreibung	Zunächst wird die Telematik-ID ermittelt, bei welcher der Online Check-in geplant ist. Dann stimmt VER der Datennutzung durch den Inhaber der Telematik-ID zu. Anschließend bietet das PoPP-Modul VER diverse Möglichkeiten zur Authentisierung an. Im hier betrachteten Fall wählt VER "GesundheitsID" aus. Dabei wird VER durch den sektoralen IDP seiner Krankenversicherung authentifiziert. 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 unter anderem die KVNR der authentifizierten VER und die IK-Nummer der Krankenkasse enthält. Außerdem liefert das ID-Token Informationen über die

	Vertrauenswürdigkeit der Authentifizierung (Vertrauensniveau) und über das eingesetzte Authentisierungsmittel. Der ZETA Guard Authorization-Server des PoPP-Service erstellt daraufhin ein Access-Token für das PoPP-Modul und speichert folgende Informationen zur späteren Verwendung: 1. KVNR 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 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 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.
Vorbedingungen	1. VER hat einer Datennutzung (KVNR) durch den 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 (mandatory) b. WorkplaceID (optional) 3. Die Authentifizierung der VER mit GesundheitsID wurde von den ZETA-Komponenten und den Komponenten des sektoralen IDP seiner Krankenversicherung erfolgreich durchgeführt. a. Zum Zeitpunkt der Authentisierung der VER muss dieser

	einen Internetzugang haben. b. VER 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 die VER im sektoralen IDP seiner Krankenversicherung eingerichtet und VER 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-Request b. den im vom ZETA-Guard ausgestellten 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 der 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 (mandatory) - aus dem HTTP-Request e. WorkplaceID (optional) - aus dem HTTP-Request f. client_id (mandatory) - aus dem Header des HTTP-Request 3. Der PoPP-Service Resource Server prüft, ob für die KVNR und Telematik-ID bereits ein PoPP-Datensatz existiert und der zugehörige Nachrichten-Datensatz den Status "pending" hat. Ist dies der Fall antwortet der PoPP-Service Resource Server dem eingegangenen Request mit der Statusnachricht "pending". Der Ablauf ist beendet, es wird kein weiterer Datensatz angelegt. 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. <i>id</i>- eindeutiger Identifier zur Identifikation der Nachricht bei asynchronem Abruf b. <i>status</i> - repräsentiert den Status der PoPP-Token-Erstellung (<i>success</i>, <i>pending</i>, <i>canceled</i>). Bei Erstellung ist der status immer "pending". c. <i>client_id</i>- 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. 6. Der PoPP-Service Resource Server speichert den Identifier (<i>id</i>) des Nachrichten-Datensatz zum Status der PoPP-Token-Erstellung zusätzlich im PoPP-Datensatz. 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. c. Der PoPP-Service Resource Server hat dem ZETA Guard HTTP-Proxy mit HTTP-201 und der Statusnachricht zur PoPP-Token-Erstellung geantwortet. 2. Fehlerfall 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-ServiceResource Server hat geantwortet mit einem i. HTTP-201 (CREATED), wenn die Bearbeitung des Requests fehlerfrei abgearbeitet werden konnte ii. HTTP-400 (Bad Request), wenn nicht alle mandatory Attribute extrahiert werden konnten iii. HTTP-500 in allen anderen Fehlerfällen 2.  ML-198839 - AF_10386 - Prüfung auf bereits bestehenden PoPP-Datensatz 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. KVN-Nummer der VER ii. IK-Nummer der Krankenversicherung iii. Telematik-ID iv. WorkplaceID v. proofMethod=" vi. Zeitstempel vii. Identifier der Nachricht zur PoPP-Token-Generierung 4.  ML-184339 - AF_10386 - 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 iii. client_id des anfragenden Clients 5.  ML-185491 - AF_10386 - Response an ZETA Guard HTTP-Proxy zum eingegangenen Request 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 Telematik-ID zugestellt wurde. ii. "pending", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token noch nicht erstellt und dem Inhaber der Telematik-ID zugestellt wurde iii. "canceled", wenn der Inhaber der Telematik-ID den PoPP-Token nicht innerhalb von 72h abgeholt hat oder wenn ein Fehler aufgetreten ist. Initial ist der Status immer "pending".
Fehlerfälle	1. Die Geräte- und/oder App-Prüfung durch ZETA ist fehlgeschlagen. 2. Die Prüfung der übergebenen Parameter zum Anlegen des PoPP-Datensatzes ist fehlgeschlagen. 3. Die Authentifizierung des Nutzers über ZETA und sektorale IDP ist fehlgeschlagen. 4. Das Anlegen des Datensatzes im PoPP-Service Resource Server ist fehlgeschlagen.

905
906

【<=】

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.yaml] für die Entgegennahme eines HTTP-Requests zur Erzeugung eines PoPP-Token, nachdem VER über seine GesundheitsID authentifiziert wurde.
[<=]

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

Der PoPP-Service hat geprüft, ob zur KVN- 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
	KVN- 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, ermittelt aus dem Query-Parameter aus dem HTTP-Request	Gültige Telematik-ID
workplaceId	WorkplaceID, ermittelt aus dem Query-Parameter aus dem HTTP-Request	string Wertebereich: ^[^\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	Identifiziert des Nachrichten- Datensatzes zur PoPP- Token-Generierung	UUID

[<=]

ML-184339 -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 1. "success" - PoPP-Token wurde erstellt, dem Primärsystem zugestellt 2. "pending" - PoPP-Datensatz ist angelegt, PoPP-Token wurde noch nicht erstellt 3. "canceled" - Erstellung des PoPP-Token wurde abgebrochen	string Wertebereich: ["success", "pending", "canceled"]
client_id	ZETA-Identifier des anfragenden Clients, wie er im HTTP Header vom ZETA Guard PEP http Proxy mitgegeben wird.	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.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 und das PoPP-Token erstellt.
2. "pending", wenn der PoPP-Datensatz angelegt aber das PoPP-Token noch nicht erstellt
und dem Primärsystem zugestellt wurde.
3. "canceled", wenn die Erstellung des PoPP-Token abgebrochen wurde.

947 [**<=**]

948 *Hinweis: Nach der initialen Erstellung des Nachrichten-Datensatzes ist der Status immer*
949 *"pending".*

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

952 Der PoPP-Service MUSS

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

959 Für die Speicherung gilt A_26603*.

960 Für die Übernahme von Daten von Clients gilt A_26470*.

961 [**<=**]

964 **4.1.13 Neues Kapitel 4.5.3: PoPP-Token bei Online Check-in**

Offener Punkt: 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.

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

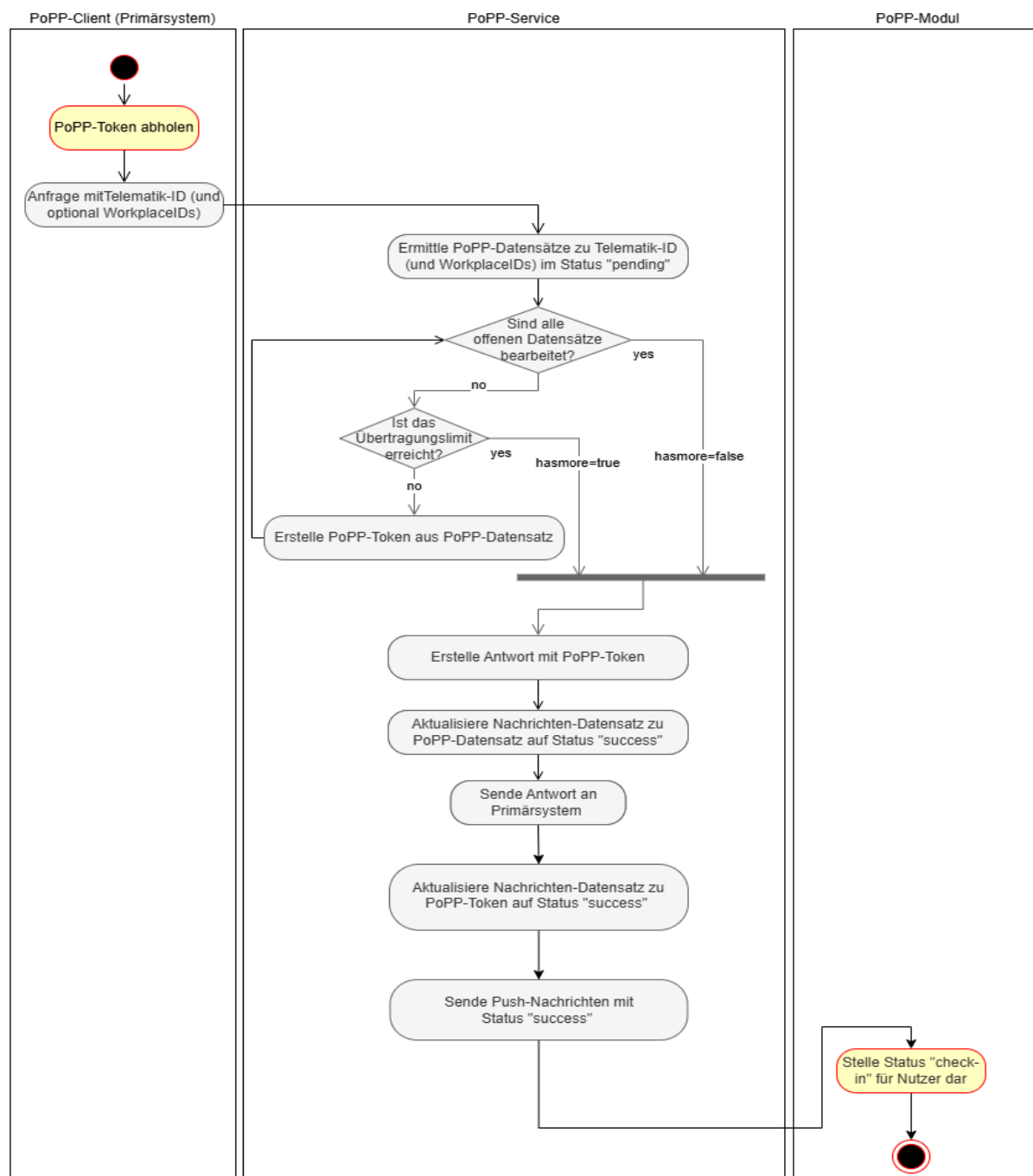


Abbildung 6 : Ablauf Abholen der PoPP-Token bei Online Check-in (auf die beteiligten ZETA-Komponenten wurde in der Abbildung verzichtet)

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.

978

979

AF_10390-01 -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 der Inhaber der Telematik-ID gegenüber dem ZETA-Guard (mit SM(C)-B) authentifiziert hat, wird aus diesem Datensatz ein PoPP-Token erzeugt (AF_10425*). Der PoPP-Service Resource Server übermittelt PoPP-Token an den PoPP-Client. Der PoPP-Service Resource Server übermittelt den Status der PoPP-Token-Generierung an das PoPP-Modul.
Vorbedingung	1. Der PoPP-Datensatz für die PoPP-Token-Generierung ist im PoPP-Service Resource Server erstellt und gespeichert. 2. Der Nachrichten-Datensatz zum Status der PoPP-Token-Generierung ist im PoPP-Service Resource Server erstellt und gespeichert. 3. Das Primärsystem desInhabers der Telematik-ID ist als PoPP-Client am ZETA-Guard registriert. 4. Der Inhaber der Telematik-ID hat sich gegenüber dem ZETA-Guard (mit SM(C)-B) authentifiziert.
Ablauf	Information an denInhaber der Telematik-ID 1. Der PoPP-Service Resource Server erstellt eine Push-Notification für das Primärsystem zum Abholen des PoPP-Token. 2. Der PoPP-Service Resource Server sendet die Push-Notification an ZETA-Guard zur Weiterleitung an das Primärsystem. <i>Hinweis: Wie die Push-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 Primärsystem: 1. Das Primärsystem sendet 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 (SM(C)-B). 2. Der PoPP-Service Resource Server sucht alle PoPP-Datensätze zur Telematik-ID

	a. mit der WorkplaceID, 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. 3. Der PoPP-Service Resource Server geniert PoPP-Token. 4. Der PoPP-Service Resource Server antwortet auf den HTTP-Request mit den ausgestellten PoPP-Token und, wenn vorhanden, der zugeteilten WorkplaceIDs und dem Identifier des zugehörigen Nachrichten-Datensatzes. 5. Der PoPP-Service Resource Server ändert den Status in den Nachrichten-Datensätzen zu den PoPP-Datensätzen auf <i>status = success</i>. 6. Der PoPP-Service Resource Server stellt PoPP-Modulen über die ZETA-Komponenten eine Nachricht zur Statusänderung zu. Die Zustellung der Nachricht erfolgt a. im synchronen Fall als Antwort auf den HTTP-Request (z.B. 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 c. asynchron als Push-Notification für alle neu verarbeiteten PoPP-Token.
Nachbedingung	1. Der PoPP-Service Resource Server löscht alle PoPP-Datensätze a. zu denen ein PoPP-Token erstellt und ausgeliefert und zu denen eine Nachricht an das PoPP-Modul erfolgreich zugestellt wurde. b. die älter als 72h sind. Der Status der Nachricht zu diesem Datensatz wird auf <i>status = canceled</i> gesetzt. 2. Der PoPP-Service Resource Server löscht alle Nachrichten-Datensätze mit <i>status = canceled</i> oder <i>status = success</i> sobald sie zugestellt wurden, spätestens jedoch nach 5 Tagen.
Akzeptanzkriterien	1.  ML-184426 - AF_10390 - PoPP-Token erstellt und übermittelt oder Abbruch des Check-in a. Der PoPP-Service Resource Server hat PoPP-Token erstellt und an das Primärsystem übermittelt oder den Zustellungsversuch nach 72h abgebrochen. 2.  ML-184425 - AF_10390 - Aktualisierung der Nachrichten-Datensätzen zu gesendeten PoPP-Token a. Der PoPP-Service Resource Server hat eine Nachricht zum Status der PoPP-Token-Erstellung aktualisiert. 3.  ML-184427 - AF_10390 - Löschung zugestellter oder abgelaufener Nachrichten

	a. Der PoPP-Service Resource Server hat zugestellte Nachrichten-Datensätze gelöscht. b. Der PoPP-Service Resource Server hat abgelaufene Nachrichten-Datensätze gelöscht.
--	---

[<=]

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

Der PoPP-Service hat gemäß [I_PoPP_Token_Generation.yaml] PoPP-Token erstellt. Die PoPP-Token wurde dem Primärsystem zugestellt. Wurde innerhalb von 72h nach Erstellung eines PoPP-Datensatz kein PoPP-Token dem Primärsystem zugestellt, hat der PoPP-Service den Check-in Prozess abgebrochen.

[<=]

ML-184425 -AF_10390 - Aktualisierung der Nachrichten-Datensätzen zu gesendeten PoPP-Token

Der PoPP-Service hat status = success für die Nachrichten-Datensätze gesetzt, für die ein PoPP-Token an ein Primärsystem übertragen wurde.[<=]

ML-184427 -AF_10390 - Löschung zugestellter oder abgelaufener Nachrichten

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

1. den status "success" oder "canceled" 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.

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

AF_10425 -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 der 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 das 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". Wird zu einem späteren Zeitpunkt der Inhaber der Telematik-ID authentifiziert und ruft das 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. Solange der Inhaber der Telematik-ID nicht authentifiziert ist, 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 "canceled" geändert. Das PoPP-Modul kann nach dem Online Check-in beim PoPP-Service Resource Server den aktuellen Status der PoPP-Token-Generierung anfragen und VER informieren, ob sein Online Check-in beim Inhaber der Telematik-ID erfolgreich war oder abgebrochen wurde.
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. - Zum Zeitpunkt der Authentisierung der VER muss dieser einen Internetzugang haben. - VER verwendet eine Kassen-App. - Gerät und Kassen-App sind in der ZETA Guard Client-Registry registriert. ZETA Guard hat ein Client Access-Token erstellt. - Der ZETA Guard HTTP-Proxy hat den PoPP-Service Resource Server mit dem vom PoPP-Modul erstellten HTTP-Request aufgerufen.
Ablauf	- Der PoPP-Service Resource Server nimmt den HTTP-Request vom ZETA Guard HTTP-Proxy entgegen. - Der PoPP-Service Resource Server extrahiert den Identifier (id) des Nachrichten-Datensatzes aus dem HTTP-Request. - Der PoPP-Service Resource Server ermittelt die aktuellen Informationen zur PoPP-Token-Erzeugung aus dem Nachrichten-Datensatz. - Der PoPP-Service Resource Server hat den eingegangenen Request mit der Statusnachricht zur PoPP-Token-Erstellung beantwortet.
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 Resource Server hat geantwortet mit einem - HTTP-200 (OK), wenn die Bearbeitung des Requests fehlerfrei abgearbeitet werden konnte - HTTP-400 (Bad Request) , wenn nicht alle mandatory Attribute extrahiert werden konnten - HTTP-500 in allen anderen Fehlerfällen  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 1. "success", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token erstellt und demInhaber der Telematik-ID zugestellt wurde 2. "pending", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token noch nicht erstellt und demInhaber der Telematik-ID zugestellt wurde 3. "canceled", wenn ein Fehler aufgetreten ist.
--	---

[<=]

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

Der PoPP-Service implementiert eine Schnittstelle gemäß [I_PoPP_Service_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_Service_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 Telematik-ID zugestellt wurde.
2. "pending", wenn der PoPP-Datensatz angelegt werden konnte und das PoPP-Token noch nicht erstellt und demInhaber der Telematik-ID zugestellt wurde.
3. "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.[<=]

4.1.15 Änderungen [gemSpec_PoPP_Service#5.2]: 5.2 Datenschutz und 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".[<=]

4.1.16 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 VER kommen weitere Komponenten der Zero-Trust-Architektur (ZETA) zum Einsatz.

ZETA Client

Beim Online Check-in ist der ZETA Client die Zero Trust-Komponente für ein 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 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 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 Vertrauenswürdigem 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. [$\leq$]

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-Notification 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 1.1] unter <Identifizier-URL>/ .well-known/openid-federation verfügbar macht.

Das Entity Statement beaufkundet allgemeine Informationen wie:

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

und Metadaten Informationen zur Konfiguration als:

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

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

Anforderungen in Kapitel 5.6 werden hinzugefügt

- **Allgemeine Anforderungen an Teilnehmer der TI-Föderation - Zweigung 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.

[<=]

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. [≤]

- **A_27294, A_27295, A_27296 entfallen durch die Zuordnung von A_28911 zum PoPP-Service(neu mit Release IDP 26.1)**

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"

Tabelle 7 : Allgemeine Attribute im well-known-Dokument des TI-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	JSON Object, erforderlicher Wert: "oauth_resource"

Tabelle 8 : Attribute des Metadatenblocks oauth_resource im well-known-Dokument des TI-Fachdienstes als Protected Resource

Name	Werte
resource	string, URL nach RFC1738 zulässiger Wert: identisch mit dem Wert des Claims iss
signed_jwks_uri(*)	string, URL nach RFC1738
organization_name	string (gemäß [OpenID-Federation "Informational Metadata Extensions"] - organization_name) Wertebereich: ^[a-zA-Üß\w\ \-\.\+*V]{1,128}\$
keywords	[string] (gemäß [OpenID-Federation "Informational Metadata Extensions"] - keywords) erforderliche Werte: "product_type_version:<VERSION>" "product_type:<von der gematik zugelassener Produkttyp>"
contacts	[string] (gemäß [OpenID-Federation "Informational Metadata Extensions"] - contacts) 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.
[<=]

4.1.20 Änderungen in [\[gemSpec_PoPP_Service#6.1.2\]](#): Schnittstelle für Token-Abrufe

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-

Interfaces https://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

Für den Abruf von PoPP-Token, die im Zusammenhang mit einem Online Check-in erstellt wurden, stellt der PoPP-Service 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 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.

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. [**<=**]

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.

[$\leq$]

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. [$\leq$]

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.

[$\leq$]

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.

[$\leq$]

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 den Inhaber der Telematik-ID erzeugen, in dem die Telematik-ID enthalten ist. Der QR-Code enthält optional die WorkplaceID des Arbeitsplatzes, für den der QR-Code verwendet wird. [≤]

A_28533 -PS - PoPP - Format QR-Code

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

A_28534 -PS - PoPP - QR-Code Inhalt Payload

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

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

Wird einer VER ein QR-Code für den Online Check-in 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. Andere Apps auf dem Smartphone des Versicherten dürfen nicht verwendet werden.
3. Während des Online Check-in-Vorgangs 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.
4. Während des Online Check-in werden am Smartphone des Versicherten Angaben zum Inhaber der Telematik-ID präsentiert. Diese Angaben sind von der VER auf Richtigkeit zu prüfen.

[≤]

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 des Inhabers der 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 eine regelmäßige Überprüfung 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 Räumlichkeiten des Telematik-ID Inhabers in einem gut durch das Personal frequentiert Bereich - idealerweise am Tresen - aufgestellt bzw. angebracht werden soll sowie regelmäßig auf Korrektheit geprüft werden soll, 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 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 zusätzlich zum PoPP-Token auch eine WorkplaceID übermittelt, dann dient dies beispielsweise der Zuordnung des PoPP-Token zu einem Arbeitsplatz im Primärsystem des Telematik-ID Inhabers, an dem ein Online Check-in von einem Versicherten durchgeführt wurde.

Die WorkplaceID kann durch 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. 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

Im Zuge des Online Check-in eines Versicherten wird ein PoPP-Datensatz im PoPP-Service angelegt und für maximal 72h vorgehalten. Fragt das Primärsystem des Inhabers einer Telematik-ID während dieser Zeit über die Schnittstelle [I_PoPP_Service_mobile_Token_Generation.yaml] oder [I_PoPP_Service_mobile_Token_Generation_async.yaml] PoPP-Token an, erstellt der PoPP-Service auf Basis des hinterlegten PoPP-Datensatz ein PoPP-Token und liefert dieses an das Primärsystem zurück.

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.

【<=】

4.3 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
[I_PoPP_Service_mobile_Token_Generation.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, WorkplacelD, ...)
[I_PoPP_Service_mobile_CheckIn.yaml]	neu	Schnittstellen für die Kommunikation mit dem PoPP-Modul. Die OpenAPI-Definition umfasst: - Die Schnittstelle zur Authentifizierung mit GesundheitsID 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.yaml]	neu	Schnittstelle am PoPP-Modul für den Aufruf aus anderen Apps.
I_PoPP_Service_mobile_Token_Generation_async.yaml]	neu	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, WorkplacelD, ...)

1514

1515 4.4 Änderungen in [gemSpec_ZETA]

1516 Bei der Authentifizierung von Versicherten mit GesundheitsID werden in PoPP Stufe 2 u,a,
1517 ZETA-Komponenten (ZETA-Client / ZETA Guard) verwendet.Die Festlegungen dazu stehen
1518 in [gemSpec_ZETA] Stufe 2.

1519

1520 4.5 Änderungen in [gemKPT_Test]

1521 4.5.1 Änderungen im Kapitel 7.4 Interoperabilität

1522 Die Tabelle Tab_Test_033 Mindestumfang der Interoperabilitätsprüfung wird
1523 durch die Folgende ersetzt:

zu testendes Objekt	eGK G2	eGK 2.1	SMC-B G2	SMC-B G2.1	HBA G2	HBA G2.1	gSMC-KT G2 1	gSMC-KT G2.1	Primärsystem	E-Mail Client (auch PWS)	Clientmodul KIM 11	eHealth-KT 12	Konnektor	Highspeedkonnektor 1	Basis-Consumer	VPNzugd	Zentrales Netz TI	ZETA Guard	Namensdienst	Zeitdienst	TSL-Dienst	KSR	Sitzungsaufw./Betriebsdatenerfassung	OCSP-Responder-Proxy	TSP X.509 nonQES	TSP X.509 QES	PoPP-Service	PoPP-Modul	Intermediär VSDM	VSDM Fachdienst	VSDM 2.0	SG Bestandsnetze	Fachdienst KIM	TI-Messenger Fachdienst	TI-Messenger Pro Fachdienst	TI-Messenger ePA Fachdienst	TI-Messenger Client	TI-Messenger Pro Client	Verzeichnisdienst	FHIR-VZD	ePA-Aktensystem	ePA-Frontend des Versicherten	Schlüsselgenerierungsdienst	Signaturdienst	E-Rezept Fachdienst	IDP-Dienst	Federation Master	Sektorale IDP	E-Rezept FdV																									
Konnektor	2	2	2	2	2	2	2	2 ¹⁰		2	3 ¹	2 ¹	4 ^{1,2}	3 ¹								1	1		1	1	1	1	3		2									2	2 ⁷	1																																
Konnektor (HSK)	2	2	2	2	2	2	2	2 ¹⁰		2	3 ¹	3 ^{1,2}	3 ^{1,2}	3 ¹							1				1	1	1	1	1	3		2								2	2 ⁷	1																																
eHealth-Kartenterminal	1	2	2	2	2	2	2	2	2 ¹⁰				3	4 ¹								1					1	1	1	1	3																																											
Mobiles Kartenterminal	2	2	2	2	2	2	2	2 ¹⁰																																																																		
VPN Zugangsdienst												2					1	1	1	1	1	1		1		1																																																
Zentrales Netz der TI (SZZP)																	1		1	1	1	1	1	1	1	1	1	1	1	1																																												
Namensdienst																		1	1	1	1	1	1																																																			
Zeitdienst																	1	1	1	1	1	1	1																																																			
ZETA Guard								2 ¹⁰																					1																																													
Konfigurationsdienst												2						1	1	1	1	1	1																																																			
Verzeichnisdienst											2	2									1	1	1	1	1																																																	
FHIR VZD																																																																										
PoPP-Service		2		2				2 ¹⁰			2	3	3 ¹													2				2																																												
Popp-Modul		2																										1																																														
SG Bestandsnetze																	1	1	1	1	1	1	1																																																			
Intermediär VSDM											a ^{1,13}	3 ³	1 ⁴				1	1	1	1	1	1	1		1		1	1																																														
VSDM 2.0								2 ¹⁰																																																											</							

4.6 Änderungen in [gemSpec_IDP_Sek]

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

Zum einen werden für die technische Abbildung eines PoPP-Modul Aufrufs aus einer Anbieter-App die Plattformmechanismen von Android und iOS (deeplink / universal link) verwendet. Hier kann allerdings bereits nachgenutzt werden, dass für eine Authentifizierung des Versicherten mit GesundheitsID die entsprechende Konfiguration schon eingerichtet ist. Allerdings ist es notwendig, die Mechanismen der eigentlichen Authentifizierung vom Mechanismus des Aufrufs des PoPP-Moduls zu trennen. Zu diesem Zweck ist ein eigener Endpunkt in A_29041* [gemSpec_PoPP-Modul] definiert. Der Endpunkt besteht aus der Client-ID des sektoralen 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 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 der TI-Föderation"

A_30017 -Information des Nutzers bei fehlender Installation der App mit integriertem Authenticator-Modul und PoPP-Modul

Der Hersteller eines sektoralen IDP MUSS ein technisches Verfahren für den Fall etablieren, dass ein Nutzer die App mit integriertem Authenticator-Modul und PoPP-Modul nicht installiert hat. In diesem Fall MUSS der sektorale IDP für den PoPP-Endpunkt (A_29041*) ein WebFrontend anbieten und dort darstellen, aus welcher Quelle die App mit integriertem Authenticator-Modul und PoPP-Modul zu beziehen ist, auf welchen Geräten/Plattformen es installiert werden kann und welche Voraussetzungen für die Verwendung der App zu erfüllen sind.【<=】

4.7 Änderungen in [gemSpec_Perf]

Änderungen am PoPP Service spezifischen Kapitel 3.X.

Die folgenden neuen Anwendungsfälle werden ebenfalls in gemSpec_Perf hinzugefügt:

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
PoPP.3	POST /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-RessourceServer und endet mit dem Absenden der Response StatusPoppTokenGeneration.
PoPP.4	(reserviert)	
PoPP.5	POST /httpReadStatusPoPPRequest	Anweisung für den Abruf des aktuellen Status zur PoPP-Token-Erstellung 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.6	POST /popp/practitioner/api/v1/token-deliveries	Anweisung zur Erstellung eines PoPP-Token nach Authentifizierung des Versicherten mit Mobilgerät (Smartphone) (REST)
POPP.7	POST (/popp/practitioner/api/v1/token-deliveries) (Hinweis: Link wird noch geändert)	Anweisung zur Erstellung eines PoPP-Token nach Authentifizierung des Versicherten mit Mobilgerät (Smartphone) (WebSocket)

Aktualisierung der Anforderung zu den Performance-Kenngrößen:

A_27030-04 -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

Operatio	Spitzenlas	Mittlere	Maximale	Erfüllungsquot
----------	------------	----------	----------	----------------

n	t [1/sec]	Bearbeitungszeit [msec]	Bearbeitungszeit [msec]	e [%]
PoPP.1	1400	600	1500	99,99
PoPP.2	1400	600	1500	99,99
PoPP.3	1400	1400	1800	99,99
PoPP.4	1400	800	1200	99,99
PoPP.5	2000	200	350	99,99
PoPP.6	1400	600	1500	99,99
PoPP.7	1400	600	1500	99,99

1574 [$\leq$]

1578 4.8 Änderungen in [gemKPT_Betr]

1579 Anpassung Tabelle:

1580 **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
...		

1581
1582
1583 **Tabelle der PerformanceKenngrößen ist nicht mehr im Betriebskonzept**
1584 **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
PS	Primärsystem
SM(C)-B	Secure Module (Card) - Typ B
VER	versicherte Person oder dessen Vertreter
VZD	Verzeichnisdienst
eGK	elektronische Gesundheitskarte
eH-KT	eHealth-Kartenterminal
glD	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.
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 Kassen-Apps (1-App-Strategie), andere halten Kassen-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.
Drittanbieter-Anwendung	Eine Drittanbieter-Anwendung ist eine Anwendung im Kontext des Gesundheitswesens, die Personen digitale Gesundheitsdienste bereitstellt und nicht von einer gesetzlichen oder privaten Krankenversicherung angeboten wird. Drittanbieter-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. Kassen-Apps sind keine Anbieter-Apps im Sinne dieser Spezifikation. Drittanbieter-Anwendungen können als native mobile Anwendungen oder browserbasierte Webanwendungen umgesetzt sein.
GesundheitsID	Die GesundheitsID ist die digitale Identität im Gesundheitswesen für VER, 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.
Kassen-App	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 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 desInhabers einer 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 Kassen-App, welche für Online-Anwendungsfälle die Kommunikation mit dem PoPP-ServiceResource Server übernimmt. Das PoPP-Modul initiiert die Authentifizierung einer 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 demInhaber einer Telematik-ID.
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.....	23
Abbildung 2: Produkttypzerlegung PoPP-Service.....	25
Abbildung 3: Systemkontext PoPP-Service.....	26
Abbildung 4: Anwendungsfälle zur Attestierung des Versorgungskontexts.....	31
Abbildung 5: Use-Case-Übersicht Online Check-in aus einer App mit integriertem PoPP-Modul.....	33
Abbildung 6 : Ablauf Abholen der PoPP-Token bei Online Check-in (auf die beteiligten ZETA-Komponenten wurde in der Abbildung verzichtet).....	44

6.4 Tabellenverzeichnis

Tabelle 1: Ablauf Online Check-in.....	14
--	----

1608	Tabelle 2: PoPP-Use Cases (Business Sicht).....	21
1609	Tabelle 3: Kurzbeschreibung der Komponenten in der PoPP-Lösung.....	27
1610	Tabelle 4: Zuordnung der Anwendungsfälle zu den Use Cases.....	31
1611	Tabelle 5: Kurzbeschreibung technische Use Cases Online Check-in aus einer App mit	
1612	integriertem PoPP-Modul.....	33
1613	Tabelle 6: Header des Entity Statement des TI-Fachdienstes als Protected Resource.....	54
1614	Tabelle 7 : Allgemeine Attribute im well-known-Dokument des TI-Fachdienstes als	
1615	Protected Resource.....	55
1616	Tabelle 8 : Attribute des Metadatenblocks oauth_resource im well-known-Dokument des	
1617	TI-Fachdienstes als Protected Resource.....	55
1618	Tabelle 9: Übersicht über die OpenAPI-Definitionen.....	63
1619	Tabelle:10 Tab_gemSpec_Perf_PoPP_Service: Performancerelevante UseCases.....	66
1620	Tabelle 11: Tab_gemSpec_Perf_PoPP_Service: Last- und Bearbeitungszeitvorgaben.....	68
1621	Tabelle 12: Tab_gemKPT_Betr_Produkttypen.....	68
1622	Tabelle 13: Glossar der explizit im Dokument verwendeten Begriffe.....	70
1623		

1624 6.5 Referenzierte Dokumente

1625 6.5.1 Dokumente der gematik

1626 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
1627 referenzierten Dokumente der gematik zur Telematikinfrastruktur.

1628

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_PoPP]	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" 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-ilm-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_CC2 (vom 22.01.2026)
[_PoPP_Service_mobile_CheckIn.yaml]	OpenAPI Schnittstellenspezifikation für - den Aufruf des VZD-Suche am PoPP-Service - den Aufruf zum Anlegen eines PoPP-Datensatzes am PoPP-Service - den Aufruf zur Statusabfrage am PoPP-Service I_PoPP_Service_mobile_CheckIn.yaml
[I_PoPP_Service_mobile_Token_Generation.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 I_PoPP_Service_mobile_Token_Generation.yaml
[I_PoPP_Token_Generation.yaml]	OpenAPI Schnittstellenspezifikation des PoPP-Service für PoPP-Clients: I_PoPP_Token_Generation.yaml

1629

1630

6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ISO/IEC 18004:2024]	ISO/IEC 18004:2024] "Information technology – Automatic Identification and Data Capture Techniques – QR Code 2005 Bar Code Specification," ISO/IEC 18004:2024, International Organization for Standardization, 2024. https://www.iso.org/standard/83389.html
[RFC3629]	D. B. Cohen, "UTF-8, a transformation format of ISO 10646," RFC

	3629, Nov. 2003. https://datatracker.ietf.org/doc/html/rfc3629
[RFC1738]	Uniform Resource Locators (URL) https://www.rfc-editor.org/rfc/rfc1738.html
[RFC7517]	https://datatracker.ietf.org/doc/html/rfc7517 JSON Web Key (JWK)
[RFC7519]	JSON Web Token (JWT) https://datatracker.ietf.org/doc/html/rfc7519
[RFC8259]	D. B. Crockford, "The JavaScript Object Notation (JSON)," RFC 8259, Dez. 2017. https://datatracker.ietf.org/doc/html/rfc8259
[OpenID Federation 1.0]	OpenID Federation Standard https://openid.net/specs/openid-federation-1_0.html

1631

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 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 das Primärsystem desInhabers 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 Kapitel4-Spezifikation von diesem Dokument enthalten.

8 Anhang C - Offene Punkte, Fragen

8.1 Offene Punkte

OP-PoPP-1	4.1.13 [gemSpec_PoPP-Service#4.5.3]: PoPP-Token bei Online Check-in	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.
OP-PoPP-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-PoPP-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-PoPP-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-PoPP-5	[gemSpec_Popp_Modul#5.6.4]	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-PoPP-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-PoPP-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-PoPP-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 WorkplacelD 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.

1659

1660