

Telematikinfrastruktur 2.0

Spezifikation PoPP (Proof of Patient Presence) -Modul

Version:	0.5.0
Revision:	1105684
Stand:	20.01.2025
Status:	in Bearbeitung
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_PoPP_Modul

Dokumenteninformationen

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
0.5.0	20.01.2025		initiale Erstellung	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes.....	4
1.1 Zielsetzung.....	4
1.2 Zielgruppe.....	4
1.3 Geltungsbereich.....	4
1.4 Abgrenzungen.....	5
1.5 Methodik.....	5
2 Systemüberblick/Systemkontext.....	6
3 Übergreifende Festlegungen.....	7
4 Funktionsmerkmale.....	8
4.1 Anforderungen PoPP-Modul als OAuth-Client.....	8
4.2 Anforderungen PoPP-Modul an TAN und QR-Code.....	9
4.3 Anforderungen PoPP-Modul für GesundheitsID.....	9
4.4 Anforderungen PoPP-Modul für eGK (mobil).....	11
5 Informationsmodell.....	13
6 Verteilungssicht.....	14
7 Implementierungsleitfaden für PoPP-Modul.....	15
7.1 QR-Code.....	15
8 Anhang A - Verzeichnisse.....	16
8.1 Abkürzungen.....	16
8.2 Glossar.....	16
8.3 Abbildungsverzeichnis.....	18
8.4 Tabellenverzeichnis.....	18
8.5 Referenzierte Dokumente.....	18
8.5.1 Dokumente der gematik.....	18
8.5.2 Weitere Dokumente.....	19

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps Proof of Patient Presence Frontend des Versicherten (PoPP-Modul).

Diese basieren auf dem Technischen Konzept [gemKPT_PoPP] und weitergeführten Abstimmungen mit den Gesellschaftern der gematik als Konsumenten der gesamten PoPP-Lösung, insbesondere zu Themen bei Nutzung der GesundheitsID.

Das PoPP-Modul bietet Nutzern mit GesundheitsID den Zugang zur PoPP-Lösung. Der PoPP-Service erzeugt die Bestätigung eines Versorgungskontextes in Form des kryptographisch gesicherten PoPP-Token. Dieses bestätigt, dass ein bestimmter Versicherter mit einer bestimmten Leistungserbringerinstitution (LEI) zusammengekommen ist.

Neben dem PoPP-Modul, tragen weitere Komponenten zur PoPP-Lösung bei:

- Der PoPP-Service ist der Server Anteil der PoPP-Lösung.
- Die PoPP-Clients, die als Teil der Primärsysteme implementiert werden.
- Apps, die bei der mobilen Nutzung der eGK in die Kommunikation zur Erstellung der PoPP-Token eingebunden sind.

Die Spezifikationen oder Beschreibungen dieser Komponenten erfolgt in anderen Dokumenten.

1.2 Zielgruppe

Das Dokument richtet sich an den Hersteller und Betreiber von Frontends der Versicherten für PoPP, insbesondere die Kassen und ihre Auftragnehmer.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. gemPTV_ATV_Festlegungen, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekanntgegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder

Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch [Anhang 8]).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps PoPP-Modul verzeichnet.

1.5 Methodik

Anwendungsfälle und Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID, Anforderungen zusätzlich durch die dem [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.

Anwendungsfälle und Anforderungen werden im Dokument wie folgt dargestellt:

<AF-ID> - <Titel des Anwendungsfalles>

Text / Beschreibung

[<=]

bzw.

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

Dabei umfasst der Anwendungsfall bzw. die Anforderung sämtliche zwischen ID und Textmarke [<=] angeführten Inhalte.

Hinweis auf offene Punkte <<optional; Kasten mit "Offener Punkt" in das entsprechende Kapitel einfügen>>

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

2 Systemüberblick/Systemkontext

Ein ausführlicher Systemüberblick und eine Darstellung der Use-Cases und Anwendungsfälle ist in [gemSpec_PoPP_Service] dargestellt.

3 Übergreifende Festlegungen

A_27220 - PoPP-Modul - TLS-Verbindungsaufbau

Das PoPP-Modul MUSS beim TLS-Verbindungsaufbau das TLS-Server-Zertifikat des PoPP-Service wie folgt prüfen:

- Prüfung, dass das Zertifikat von einer CA aus dem [CAB Forum] ausgestellt wurde,
- Hostnamevalidierung,
- OCSP Status "good",
- Signatur OCSP-Response auf CA aus [CAB Forum] rückführbar

und nur im Falle einer erfolgreichen, positiven Prüfung die TLS-Verbindung aufbauen.

[<=]

Hinweis: Eine OCSP-Response wird im Handshake vom PoPP-Service mitgeliefert (Unterstützung von OCSP-Stapling [RFC 6066]).

A_27221 - PoPP-Modul - Sichere Speicherung Token und TANs

Das PoPP-Modul MUSS Access Token und TANs so speichern, dass auf diese nicht durch andere Prozesse auf dem Gerät, auf dem das PoPP-Modul läuft, zugegriffen werden kann und dafür Funktionen der Plattform (Android, iOS) und wann immer möglich HW-basierte Schlüsselspeicher verwenden. **[<=]**

Offener Punkt: wird QR-Code Eingabevalidierung (Scannen des LEI QR-Code läuft auch über PoPP-Modul) benötigt?

4 Funktionsmerkmale

4.1 Anforderungen PoPP-Modul als OAuth-Client

A_26550 - PoPP-Modul - Regelmäßiges Einlesen des Entity Statements

Das PoPP-Modul MUSS sicherstellen, dass das Entity Statement des PoPP-Service, über welches die benötigten öffentlichen Schlüsseln bezogen werden, nicht älter als 24 Stunden ist. Ist das Entity Statement des PoPP-Service älter als 24h, so muss das PoPP-Modul das aktuelle Entity Statement einlesen und auswerten. [\leq]

A_26551 - PoPP-Modul - Prüfung der Signatur des Entity Statements

Das PoPP-Modul MUSS die Signatur des heruntergeladenen Entity Statements prüfen und auf einen zeitlich gültigen Signaturschlüssel des PoPP-Service Authorization Server zurückführen, bei dem die Anwendung registriert ist, welche das PoPP-Modul integriert. Vor der weiteren Verwendung MUSS die Prüfung des Entity Statements erfolgreich abgeschlossen sein. [\leq]

A_26552 - PoPP-Modul - Organisatorische Registrierung des Anwendungsfrontends

Das PoPP-Modul MUSS sicherstellen, dass die Anwendungen, welche das PoPP-Modul integrieren, sich über einen organisatorischen Prozess am PoPP-Service Authorization Server registrieren und die dabei vom PoPP-Service Authorization Server vergebene `client_ids` und `ApiKeys` sicher im Anwendungsfrontend speichern. Die `client_ids` und der `ApiKey` müssen vom Anwendungsfrontend bei jedem Request an den PoPP-Service Authorization Server übertragen werden. [\leq]

A_26553 - PoPP-Modul - Bildung von "code_verifier" und "code_challenge"

Das PoPP-Modul MUSS zur Laufzeit einen `code_verifier` (Zufallswert) gemäß [[RFC7636 # section-4.1](#)] bilden. Der `code_verifier` MUSS eine Entropie von mindestens 43 und maximal 128 Zeichen enthalten.

Das PoPP-Modul MUSS über den `code_verifier` einen HASH-Wert, die sogenannte `code_challenge`, gemäß [[RFC7636 # section-4.2](#)] bilden. [\leq]

A_27024 - PoPP-Modul - Bildung einer "Nonce"

Das PoPP-Modul MUSS zur Laufzeit eine Nonce (Zufallswert) gemäß [[RFC7636 # section-4.1](#)] bilden. Die Nonce MUSS eine Entropie von mindestens 43 und maximal 128 Zeichen enthalten. [\leq]

A_26555 - PoPP-Modul - Einreichen des Authorization Codes

Das PoPP-Modul MUSS zur Abfrage des Access Tokens eine Anfrage beim Token-Endpunkt des PoPP-Service Authorization Server in Form eines HTTP/1.1 GET-Request stellen und dabei die folgenden Attribute anführen:

Attribut	Beschreibung
<code>code_verifier</code>	Code verifier, mit dem die vom PoPP-Modul im Authorization Request übergebene <code>code_challenge</code>

	validiert werden kann.
authorization_code	Vom PoPP-Service Authorization Server ausgestellter Authorization Code, den das PoPP-Modul als Ergebnis des Authorization Requests erhalten hat.

[<=]

4.2 Anforderungen PoPP-Modul an TAN und QR-Code

A_27029 - PoPP-Modul - Übertragung einer TAN an PoPP-Clients

Das PoPP-Modul MUSS technische Möglichkeiten unterstützen, um TANs an PoPP-Clients zu übertragen. **[<=]**

Hinweis: Mit technischen Möglichkeiten ist neben der Darstellung als QR-Code z.B. das Anbieten eines Eingabefeldes für 6-stellige TAN im PoPP-Modul einer App und die Übertragung zum PoPP-Client durch dessen backend gemeint. Da es je nach Anwendungsfall und Anwendungen unterschiedliche Möglichkeiten einer technischen Realisierung gibt, ist die Anforderung allgemein gehalten.

A_26558 - PoPP-Modul - Darstellung der TAN als QR-Code

Das PoPP-Modul MUSS die Übertragung einer TAN über die eine Darstellung als QR-Code im PoPP-Modul unterstützen. **[<=]**

Hinweis: Die Anforderung A_26558 erweitert A_27029* hinsichtlich auf jeden Fall zu unterstützenden Möglichkeiten zur TAN Übertragung.*

A_27263 - PoPP-Modul - Generierung QR-Code

Das PoPP-Modul MUSS die TANs in eine QR-Code-Darstellung gemäß ISO/IEC 18004:2024 überführen können. **[<=]**

A_26559 - PoPP-Modul - Löschen der TAN

Das PoPP-Modul MUSS sicherstellen, dass TAN nach einmaliger Verwendung oder bei nicht Verwendung nach Ablauf der Gültigkeit unwiderruflich gelöscht werden. **[<=]**

4.3 Anforderungen PoPP-Modul für GesundheitsID

Die Abläufe des Check-in über die Authentifizierung des Nutzers mit GesundheitsID sind in [gemSpec_PoPP_Service] Kapitel "Mobiler Check-in mit GesundheitsID" dargestellt.

Aus dem PoPP-Modul einer Anwendung wird ein Authorization Request an den PoPP-Service Authorization Server gesendet. Dieser löst durch einen Pushed Authorization Request (PAR) die Durchführung der Nutzerauthentifizierung über den sektoralen IDP aus.

Nach erfolgreicher Nutzerauthentifizierung wird vom PoPP-Service Authorization Server ein "ehealth-check" Access Token für das PoPP-Modul ausgestellt, der dieses zum Aufruf des PoPP-Services Resource Server autorisiert.

Der PoPP-Services Resource Server stellt dem anfragenden PoPP-Modul je nach Anwendungsfall eine "kurze" TAN oder ein TAN-Set mit "langen" TANs zum Einlösen in einer LEI aus.

A_26554 - PoPP-Modul - Formulierung und Inhalte des Authorization Request zum Erhalt eines "ehealth-check" Access Token

Das PoPP-Modul MUSS, für eine Nutzerauthentifizierung mit GesundheitsID, den Authorization Request zur Erlangung eines "ehealth-check" Access Token beim Authorization-Endpunkt des PoPP-Service Authorization Server in Form eines HTTP-Request stellen. Die Schnittstellendefinitionen gemäß [I_PoPP_CheckIn_AuthorizationServer.yaml] und [I_PoPP_CheckIn_ResourceServer.yaml] sind zu verwenden. [≤]

Tabelle 1: Claims des Authorization Request zur Erlangung eines "ehealth-check" Access Token (informativ)

Name	Wert
issidp	Issuer Identifier (URL) des sektoralen IDP, über den die Nutzerauthentifizierung durchgeführt wird.
client_id	Vom PoPP Authorization Server bei der PoPP-Modul Registrierung vergebene ID
state	Der state-Parameter ist ein Zufallswert und wird genutzt, um CSRF (Cross-Site-Request-Forgery) zu verhindern [OAuth 2.0 for Native Apps (section-8.9)].
redirect_uri	Optional - an diese URL wird der vom sektoralen IDP ausgestellte Authorization Code propagiert und muss dann von dort an den PoPP Authorization Server weiter geschickt werden, damit dieser den Authorization Code beim sektoralen IDP gegen ein ID-Token eintauschen kann. Ist die redirect_uri nicht gesetzt, so wird der PoPP Authorization Server direkt adressiert.
code_challenge	Der über das eigene code_verifier [RFC7636 # section-4.1] gebildete HASH code_challenge [RFC7636 # section-4.2] mit Angabe des Algorithmus code_challenge_method [RFC7636#section-4.3] entsprechend dem gewählten Authorization Code Flow (response_type=code).
code_challenge_method	
response_type	response_type muss auf "code" gesetzt sein.
authorization_details	Optional - Übertragung der Telematik-ID der LEI als authorization_details <pre>{ "authorization_details": [{ "actorId": "<Telematik-ID Leistungserbringer>" }]}</pre>

A_26556 - PoPP-Modul - Abfrage und Speicherung von TAN oder TAN-Set

Das PoPP-Modul MUSS sicherstellen, dass, nach einer Nutzerauthentifizierung mit GesundheitsID, mit dem vom PoPP Authorization Server erhaltenen "ehealth-check" Access Token der PoPP-Service Resource Server aufgerufen und die vom PoPP-

Service Resource Server ausgestellte TAN bzw. das TAN-Set als Ergebnis entgegen genommen und sicher gespeichert wird.【<=】

4.4 Anforderungen PoPP-Modul für eGK (mobil)

Die Abläufe des Check-in über durch die Authentisierung einer eGK sind in [gemSpec_PoPP_Service] Kapitel "Mobiler Check-in mit eGK" dargestellt.

Die Funktion eGK (mobil) ist nur für PoPP-Module zulässig, die in Drittanbieter-Apps integriert sind. Für PoPP-Module, die in Kassen-Apps integriert sind, soll diese Funktion nicht verfügbar sein.

Aus dem PoPP-Modul einer Anwendung wird ein Authorization Request an den PoPP-Service Authorization Server gesendet. Dieser stellt dem PoPP-Modul ein "card-check" Access Token aus, mit dem das PoPP-Modul seine Requests an den PoPP-Service Resource Server autorisiert.

Der PoPP-Service Resource Server führt über das PoPP-Modul die Prüfung der eGK durch. Der PoPP-Services Resource Server stellt dem anfragenden PoPP-Modul je nach Anwendungsfall eine "kurze" TAN oder ein TAN-Set mit "langen" TANs zum Einlösen in einer LEI aus.

A_27383 - PoPP-Modul - Ausschluss eGK (mobil) für Kassen-Apps

PoPP-Module, die in Kassen-Apps integriert sind DÜRFEN die Funktion eGK (mobil) NICHT anbieten.【<=】

A_27026 - PoPP-Modul - Formulierung und Inhalte des Authorization Request zum Erhalt eines "card-check" Access Token

Das PoPP-Modul MUSS für die Authentisierung einer eGK den Authorization Request zur Erlangung eines "card-check" Access Token beim Authorization-Endpunkt des PoPP-Service Authorization Server in Form eines HTTP-Request stellen. Die Schnittstellendefinitionen gemäß [I_PoPP_CheckIn_AuthorizationServer.yaml] und [I_PoPP_CheckIn_ResourceServer.yaml] sind zu verwenden.【<=】

Tabelle 2: Claims des Authorization Request zur Erlangung eines "card-check" Access Token (informativ)

Name	Wert
client_id	Vom PoPP Authorization Server bei der PoPP-Modul Registrierung vergebene ID
state	Der state-Parameter ist ein Zufallswert und wird genutzt, um CSRF (Cross-Site-Request-Forgery) zu verhindern [OAuth 2.0 for Native Apps (section-8.9)].
code_challenge	Der über das eigene code_verifier [RFC7636 # section-4.1] gebildete HASH code_challenge [RFC7636 # section-4.2] mit Angabe des Algorithmus code_challenge_method [RFC7636#section-4.3] entsprechend dem gewählten Authorization Code Flow (response_type=code).
code_challenge_method	

response_type	response_type muss auf <i>code</i> gesetzt sein.
authorization_details	Optional - Übertragung der Telematik-ID der LEI als authorization_details <pre>{ "authorization_details": [{ "actorId": "<Telematik-ID Leistungserbringer>" }]}</pre>

A_27027 - PoPP-Modul - Herstellung des Kommunikationskanals zur Authentisierung der eGK

Das PoPP-Modul MUSS für die Authentisierung einer eGK sicherstellen, dass mit dem vom PoPP-Service Authorization Server erhaltenen "card-Check" Access Token der PoPP-Service Resource Server aufgerufen wird. Die vom PoPP-Service Resource Server gesendeten Kommandos MUSS das PoPP-Modul an die eGK weiterleiten. Die Antworten der eGK auf die Kommandos MUSS das PoPP-Modul an den PoPP-Service Resource Server weiterleiten.【<=】

A_27028 - PoPP-Modul - Abschluss der Authentisierung der eGK

Das PoPP-Modul MUSS nach erfolgreichem Abschluss der Authentisierung einer eGK durch den PoPP-Service Resource Server die vom PoPP-Service Resource Server ausgestellte TAN bzw. das TAN-Set als Ergebnis entgegen nehmen und sicher speichern.【<=】

5 Informationsmodell

Eine gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten wird nicht benötigt.

6 Verteilungssicht

Die Apps mit integriertem PoPP-Modul werden über die bekannten App-Stores den Nutzern zur Verfügung gestellt.

7 Implementierungsleitfaden für PoPP-Modul

In diesem Kapitel finden sich Hinweise und Empfehlungen der gematik an PoPP-Modul Hersteller...

7.1 QR-Code

Für die Übertragung der TAN vom PoPP-Modul zum PS werden QR-Codes verwendet.

Offener Punkt: Für PS der LEI muss eine ähnliche Afo (A_27263) in den ILF für PS.

8 Anhang A - Verzeichnisse

8.1 Abkürzungen

Kürzel	Erläuterung
eGK	elektronische Gesundheitskarte
ePA	elektronischen Patientenakte
FdV	Frontend des Versicherten
HW	Hardware
IDP	Identity Provider
LE	Leistungserbringer
LEI	Leistungserbringerinstitution
OCSP	Online Certificate Status Protocol
PAR	Pushed Authorization Request
PoPP	Proof of Patient Presence
PS	Primärsystem
QR-Code	Quick Response Code
TAN	Transaktionsnummer
TLS	Trust Service Status List
URL	Uniform Resource Locator
VSDM	Versichertenstammdatenmanagement

8.2 Glossar

Begriff	Erläuterung
---------	-------------

Drittanbieter-App	Eine App, die ein Versicherter zum mobilen Check-in nutzt, wird im Gegensatz zur Kassen-App von beliebigen Stellen herausgegeben. Drittanbieter-App können für beliebige Smartphone-Betriebssysteme wie Android oder iOS sowie für unterschiedliche Desktop Betriebssysteme wie Windows oder Linux verfügbar sein. Zudem ist es möglich, dass Drittanbieter-Apps innerhalb beliebiger Internetbrowser laufen.
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
GesundheitsID	Die GesundheitsID ist die digitale Identität im Gesundheitswesen für Versicherte, welche durch die eigene Krankenversicherung bereitgestellt wird. Sie dient zur Anmeldung an TI-Anwendungen und weiteren versorgungsrelevanten Fachanwendungen und kann perspektivisch auch als Versicherungsnachweis - analog zur elektronischen Gesundheitskarte - verwendet werden.
Kassen-App	Eine App, die ein Versicherter zum mobilen Check-in nutzt, wird im Gegensatz zur Drittanbieter-App von seiner Krankenkasse herausgegeben.
PoPP-Client	Eine Komponente im Primärsystem, die für die sichere Kommunikation zum PoPP-Service verantwortlich ist.
PoPP-Modul	Eine Komponente von Kassen-App oder Drittanbieter-App, welche beim mobilen Check-in die Kommunikation mit dem PoPP-Service übernimmt. Das PoPP-Modul verwaltet TANs und TAN-Sets, die es vom PoPP-Service Resource Server im Rahmen eines mobilen Check-in erhält und unterstützt die Übertagung von TANs an einen PoPP-Client.
PoPP-Service	Zentraler Dienst in der Telematikinfrastruktur 2.0 (TI 2.0), der PoPP-Tokens generiert und verwaltet.
PoPP-Service Authorization Server	Der Server, der für die Authentifizierung und Autorisierung im Rahmen des PoPP-Services zuständig ist.
PoPP-Service Resource Server	Der Server, der TAN oder TAN-Sets für Versicherte an PoPP-Module ausgibt und PoPP-Token für PoPP-Clients erzeugt.
PoPP-Token	Ein Token, das als Nachweis für einen Versorgungskontext dient.
Versorgungskontext (VK)	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.
--	--

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

8.3 Abbildungsverzeichnis

No table of figures entries found.

8.4 Tabellenverzeichnis

Tabelle 1: Claims des Authorization Request zur Erlangung eines "ehealth-check" Access Token (informativ).....	10
Tabelle 2: Claims des Authorization Request zur Erlangung eines "card-check" Access Token (informativ).....	11

8.5 Referenzierte Dokumente

8.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemSpec_PoPP_Service]	gematik: Spezifikation PoPP Authorization Server, PoPP-Service (Dokument noch in Erstellung)
[gemKPT_PoPP]	gematik: Technisches Konzept Proof of Patient Presence (PoPP) https://gemspec.gematik.de/docs/gemKPT/gemKPT_PoPP/
[I_PoPP_CheckIn_AuthorizationServer.yaml]	OpenAPI Schnittstellenspezifikation des PoPP-Service Authorization Server für PoPP-Module: https://github.com/gematik/api-popp/blob/main/src/openapi/I_PoPP_CheckIn_AuthorizationServer.yaml
[I_PoPP_CheckIn_ResourceServer.yaml]	OpenAPI Schnittstellenspezifikation des PoPP-Service Resource Server für PoPP-Module:

	https://github.com/gematik/api-popp/blob/main/src/openapi/I_PoPP_CheckIn_ResourceServer.yaml
--	---

8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC2119]	Key words for use in RFCs to Indicate Requirement Levels https://datatracker.ietf.org/doc/html/rfc2119
[RFC8414]	OAuth 2.0 Authorization Server Metadata https://datatracker.ietf.org/doc/html/rfc8414
[RFC7636]	Proof Key for Code Exchange by OAuth Public Clients https://datatracker.ietf.org/doc/html/rfc7636
[RFC8252]	OAuth 2.0 for Native Apps https://datatracker.ietf.org/doc/html/rfc8252
[CAB Forum]	https://cabforum.org/