Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature:
Proof of Patient Presence (PoPP)

Version:	0.7.0 CC
Revision:	538553
Stand:	12.12.2022
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemF_PoPP

Dokumentinformationen

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
0.6.0	25.11.2022		Arbeitsversion zur Verteilung an die Konnektorhersteller	gematik
0.7.0 CC	12.12.2022		Arbeitsversion zur Kommentierung	gematik

Inhaltsverzeichnis

13 Anhang C – Offene Punkte, Fragen ..... Fehler! Textmarke nicht definiert.

13.1 <offener Punkt oder Frage> ..... Fehler! Textmarke nicht definiert.

1 Einordnung des Dokuments

1.1 Zielsetzung

Das Feature Proof of Patient Presence dient dazu, die Anwesenheit eines Versicherten - repräsentiert durch seine eGK - in einer Leistungserbringerinstitution zu einem bestimmten Zeitpunkt zu attestieren. Das Testat (PoPP-Nachweis) in Form eines signierten Token kann dann in der TI von verschiedenen Anwendungen verwendet werden, um Zugriff auf dafür vorgesehene Ressourcen zu geben. So kann zum Beispiel einer Apotheke Zugriff auf die Rezepte eines Versicherten gegeben werden.

1.2 Zielgruppe

<Thema 1 erläutern>

1.3 Abgrenzungen

<Thema 1 erläutern>

1.4 Methodik

1.4.1 Epic und User Story

<Methodik von Epic und User Story erläutern>

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

Epic und UserStory werden im Dokument wie folgt dargestellt:
<Jira-ID> - <Zusammenfassung des Jira-Issue>
Text / Beschreibung
[<=]

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

1.4.2 Anforderungen

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen

deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

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

Anforderungen werden im Dokument wie folgt dargestellt:
<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

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

Anforderungen mit "**PoPP-Modul:**" im Titel richten sich an den Konnektor.

Anforderungen mit "**PoPP-Dienst:**" im Titel richten sich an den PoPP-Dienst.

Anforderungen, die "**PoPP:**" im Titel haben, richten sich an den PoPP-Dienst und den Konnektor.

2 Epic und User Story

2.1 Proof of Patient Presence / Anwesenheitsnachweis

2.1.1 Erstellen eines Anwesenheitsnachweises

Als Leistungserbringer möchte ich einen Nachweis erstellen, dass ein Versicherter zum aktuellen Zeitpunkt in meiner Institution anwesend ist.

2.1.2 Verwenden des Anwesenheitsnachweises

Als Leistungserbringer möchte ich den Anwesenheitsnachweis an Dienste der TI senden, um Zugriff auf Daten zu bekommen, auf die ich bei Anwesenheit des Versicherten zugreifen darf.

2.1.3 Prüfen des Anwesenheitsnachweises

Als Dienst der TI möchte ich aus einem Anwesenheitsnachweis ablesen können

- welcher Versicherte
- zu welchem Zeitpunkt
- in welcher Institution

anwesend war. Der Nachweis muss integritätsgeschützt und vertrauenswürdig sein.

2.1.4 Fachliche Darstellung

Nutzung des Kontextes der Telematikinfrastruktur 1.0

- eGK mit KVNR als Identität des Versicherten
- SMC-B mit Telematik-ID als Identität der Institution
- eHKT und Konnektor mit online-Anbindung in der Institution

3 Einordnung in die Telematikinfrastruktur

4 Technisches Konzept

PoPP-Token

Der Anwesenheitsnachweis wird umgesetzt durch ein Token mit den Inhalten (1)-(5).

(1) Versichertenpseudonym (randomisiert verschlüsselte eGK-Daten)

- eGK-AUT-Zertifikat mit KVNR als Identität des Versicherten
- Information über OCSP-Prüfung des eGK-AUT-Zertifikats
- eGK-CV-Zertifikat
- CVC-Sub-CA-Zertifikat
- Signatur der eGK-CV-Identität über eine Challenge als Nachweis der Verwendung eines privaten Schlüssels der eGK

(2) Telematik-ID als Identität der Institution

(3) Zeitstempel der Anwesenheit

(4) Signatur über die Daten (1)-(3)

(5) Signaturzertifikat, welches den Signierenden als zugelassenen PoPP-Dienst ausweist

(De-)Pseudonymisierungsschlüssel

(6) Ein vom Konnektor erzeugter (De-)Pseudonymisierungsschlüssel (symmetrischer Schlüssel zur Ver-/Entschlüsselung der eGK-Daten) wird dem Primärsystem (und später dem nutzenden Fachdienst) neben dem Token übergeben. Diesen Schlüssel erhält der PoPP-Dienst nicht. Dieser Schlüssel ist notwendig, um das Token (PoPP-Nachweis) im nutzenden FD entpacken und verwenden zu können.

Der **Konnektor** wird um ein Modul im Basis-Konnektor erweitert (**Modul PoPP**), welches

- die Operation PerformPoPP für das Primärsystem anbietet
- die Echtheit der eGK prüft
- die Gültigkeit der eGK über eine Zertifikatsprüfung mit OCSP prüft
- eGK-Daten symmetrisch randomisiert verschlüsselt (d. h. jede Verschlüsselung gleicher Daten ergibt ein anderes Chiffrat) (Pseudonymisierungsschlüssel)
- eine TLS-Verbindung zum PoPP-Dienst aufbaut
- sich über ein Challenge-Response-Verfahren gegenüber dem PoPP-Dienst authentisiert
- mit den AUT-Identitäten der gSMC-K und der SMC-B parallel signierte Request-Daten an den PoPP-Dienst sendet
- das signierte Token zusammen mit dem Signaturzertifikat und dem Pseudonymisierungsschlüssel an das Primärsystem zurück liefert.

Der **PoPP-Dienst**

- erzeugt eine Challenge

- berechnet die Challenge basierend auf seiner Systemzeit und einem geheimen Schlüssel im PoPP-Dienst
- erstellt ein PoPP-Token
  - prüft AK.AUT-Zertifikat, inklusive OCSP
  - prüft AK.AUT-Signatur der Request-Daten
  - prüft HCI.AUT-Zertifikat, inklusive OCSP
  - prüft HCI.AUT-Signatur der Request-Daten
  - extrahiert die Telematik-ID aus dem AUT-Zertifikat der SMC-B
  - signiert die Daten (1)-(3) unter Verwendung eines Signaturzertifikats, welches nur an zugelassene PoPP-Dienste ausgegeben wird
  - erzeugt PoPP-Token aus den Daten (1)-(5)

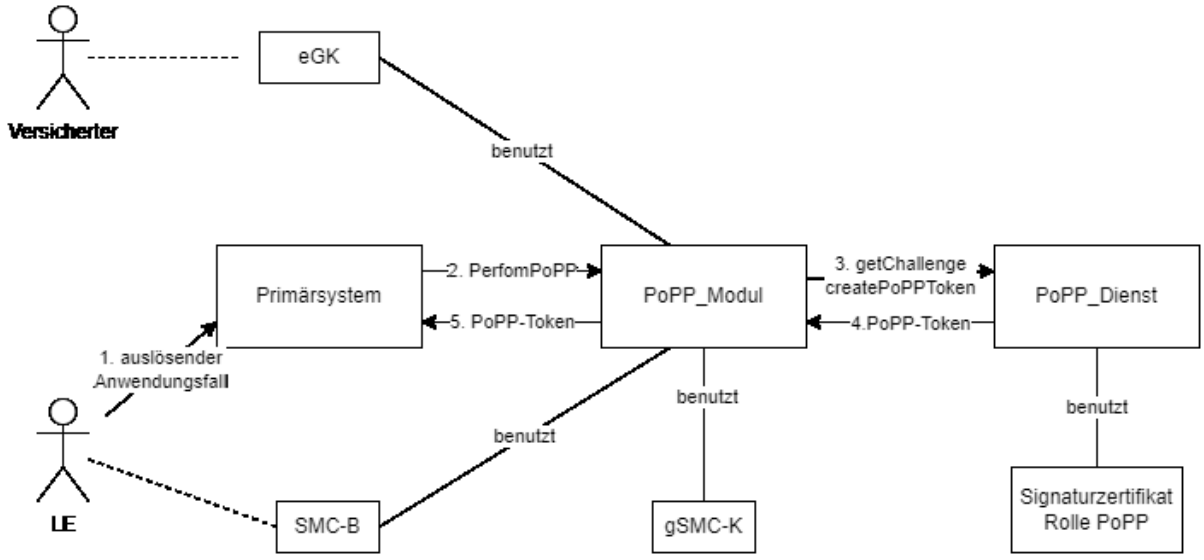

Abbildung 1 Übersicht Anwendungsfall PoPP

4.1 Systemzerlegung

Modul PoPP im Konnektor

- das Modul PoPP bietet dem Primärsystem die Operation PerformPoPP mit den Eingangsparametern CardHandle-eGK, CardHandle-SMC-B und Aufrufkontext
- das Modul PoPP nutzt die eGK, SMC-B und gSMC-K
- das Modul PoPP ruft getChallenge und createPoPPToken des PoPP-Dienstes auf

PoPP-Dienst

- der PoPP-Dienst bietet dem Konnektor (Modul PoPP) die Operationen getChallenge und createPoPPToken an

- der PoPP-Dienst prüft, dass der Request für ein PoPP-Token von einem Konnektor mit einer gültigen gSMC-K unter Nutzung einer gültigen SMC-B stammt
- der PoPP-Dienst nutzt ein Signaturzertifikat mit der Rolle PoPP-Dienst zum Signieren des PoPP-Token

4.2 Ablauf

Standardablauf in einer Leistungserbringerumgebung

1. Eine eGK wird in der Leistungserbringerumgebung gesteckt. Der Konnektor informiert das Primärsystem.
2. Der Leistungserbringer löst am Primärsystem einen Anwendungsfall aus, der einen PoPP benötigt, oder das Primärsystem löst diesen Anwendungsfall nach Steck-Information aus.
3. Das Primärsystem fordert einen PoPP-Nachweis am Konnektor für eine eGK und eine SMC-B an (PerformPoPP).
4. Der Konnektor fordert eine Challenge vom PoPP-Dienst an (getChallenge).
5. Der PoPP-Dienst sendet die Challenge zurück an den Konnektor.
6. Der Konnektor prüft die Echtheit der eGK. (Hier ist keine PIN-Eingabe erforderlich)
   a. Der Konnektor verwendet dabei die vom PoPP-Dienst empfangene Challenge in abgewandelter Form (gekürzter Hashwert) auch als Challenge bei der CV-Authentisierung der eGK.
   b. Der Konnektor führt eine einseitige Authentisierung der eGK mittels INTERNAL AUTHENTICATE durch.
   c. Die Antwort (ECDSA-Signatur der Challenge von der eGK) speichert der Konnektor für später.
   d. Der Konnektor prüft die Signatur (Response) der eGK auch selbst.
7. Der Konnektor liest das Zertifikat C.CH.AUT mit KVNR (gemSpec_PKI#Tab_PKI_232) von der eGK.
8. Der Konnektor prüft die Gültigkeit inkl. Sperrstatus (OCSP) des eGK-Zertifikats C.CH.AUT.
9. Der Konnektor erstellt einen Request mit der vom PoPP-Dienst empfangenen Challenge und den symmetrisch verschlüsselten eGK-Daten (C.CH.AUT, Status der OCSP-Prüfung des C.CH.AUT, C.eGK.AUT_CVC, CVC-Sub-CA-Zertifikat, an die eGK gesendete Challenge, von der eGK mit PrK.eGK.AUT_CVC erzeugte Signatur der Challenge (ECDSA-Signatur von oben)).
10. Der Konnektor signiert den Request mit PrK.AK.AUT der gSMC-K und PrK.HCI.AUT der SMC-B, fügt die Signaturzertifikate hinzu und fordert ein signiertes Token vom PoPP-Dienst an (createPoPPToken).
11. Der PoPP-Dienst prüft die Signaturen und Gültigkeit und Zertifikatsstatus (OCSP) des gSMC-K-Zertifikats C.AK.AUT und des SMC-B-Zertifikats C.HCI.AUT. Caching von Zertifikatsprüfungsergebnissen und OCSP-Antworten ist vorgesehen (12h).
12. Der PoPP-Dienst erstellt das Token mit den verschlüsselten eGK-Daten, der Telematik ID aus dem C.HCI.AUT-Zertifikat und seiner vertrauenswürdigen Zeit,

signiert das Token und sendet es zusammen mit der Signatur und dem Signaturzertifikat C.ZD.SIG zurück an den Konnektor.

13. Der Konnektor sendet das Token und den symmetrischen Schlüssel für die Entschlüsselung der eGK-Daten zurück an das Primärsystem.

Abbildung 2 stellt den systemübergreifenden fachlichen Ablauf der Erstellung eines PoPP-Token dar.

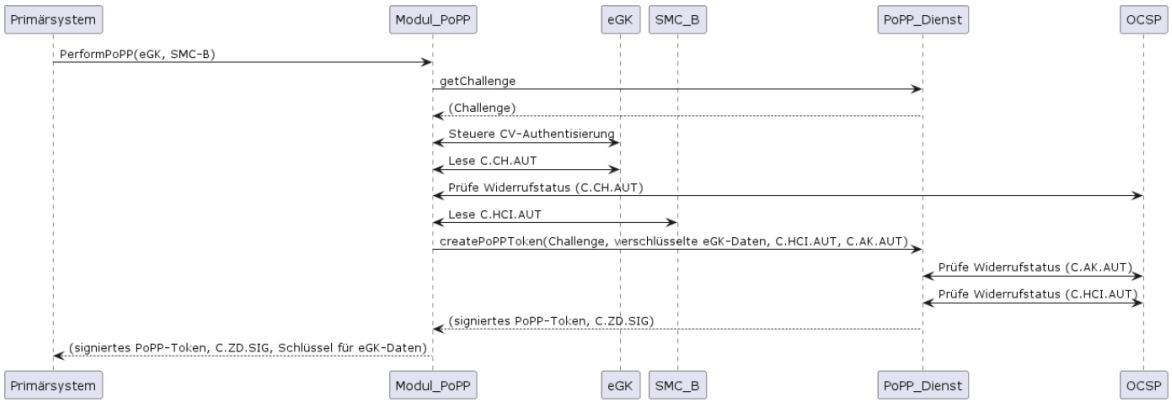

Abbildung 2 Fachlicher Ablauf PoPP

4.3 Sicherheit

Die Funktion "Proof of Patient Presence" liefert ein Token, das einen Rückschluss auf die Anwesenheit von Versicherten in einer Leistungserbringerumgebung zulässt. Es ist jedoch für nutzende Anwendungen, die auf Basis eines solchen Tokens Autorisierungsentscheidungen treffen, wichtig zu bewerten, welche Aussagen gerade nicht technisch aus dem Token entnommen werden können. Konkret beweist das Token die Anwesenheit der eGK von Versicherten, nicht jedoch die Anwesenheit dieser Versicherten selbst. Zudem ist dem Token nicht zu entnehmen, ob Versicherte dem Abruf des Tokens explizit zugestimmt haben, da dafür bis auf die Übergabe der eGK gerade keine Interaktion der Karteninhaber notwendig ist.

Bei der Prüfung der eGK durch den Konnektor im Zuge der Token-Erstellung werden Fehler bei der OCSP-Prüfung, die dazu führen, dass keine Antwort erhalten wird, toleriert, um an dieser Stelle nicht von etwaigen Verfügbarkeitsproblemen beim OCSP-Responder der TSP-eGK abhängig zu sein. Sollten tatsächlich keine OCSP-Informationen eingeholt werden können, wird dies durch den Konnektor im Token hinterlegt. Fachanwendungen können also erkennen, ob der Konnektor die OCSP-Prüfung erfolgreich durchführen konnte oder nicht und können dies für sich entsprechend auswerten und ggf. selber eine OCSP-Prüfung durchführen.

Anwendungen müssen bewerten, ob dieses Nachweisniveau für sie ausreichend ist, um den Zugriff auf die Daten der Anwendung zu gewähren.

5 Modul PoPP im Konnektor

5.1 Schnittstelle zum Clientsystem

A_23324 - PoPP-Modul: Schnittstelle PoPPService
Der Konnektor MUSS den Clientsystemen den Basisdienst PoPPService anbieten.

Tabelle 1 Tab_Kon_Basisdienst_PoPP

Name	**PoPPService**	
Version (KDV)	1.0.0 (WSDL-Version), 1.0.0 (XSD-Version)	
Operationen	**Name**	**Kurzbeschreibung**
	PerformPoPP	Anwesenheitsnachweis liefern
WSDL	PoPPService.wsdl (WSDL-Version 1.0.0)	
Schema	PoPPService.xsd (XSD-Version 1.0.0)	

[<=]

A_23323 - PoPP-Modul: Operation PoPPService:PerformPoPP
Der Konnektor MUSS an der Clientsystemschnittstelle die Operation PerformPoPP anbieten.

Tabelle 2 Tab_Kon_Operation_PerformPoPP

Name	**PerformPoPP**	
Beschreibung	Mit dieser Operation können Primärsysteme einen Nachweis ausstellen lassen, dass die eGK eines Versicherten zum aktuellen Zeitpunkt in der Leistungserbringerumgebung gesteckt ist.	
Aufrufparameter	**Name**	**Beschreibung**
	POPP:EhcHandle	CardHandle für die eGK
	POPP:HpcHandle	CardHandle für die SMC-B
	CCTX:Context	Aufrufkontext

Rückgabeparameter	Name	Beschreibung
	CONN:Status	Ausführungsstatus der Operation
	POPP:PoPPToken	PoPP-Token
	POPP:PKey	Pseudonymisierungsschlüssel für eGK-Daten (AES-128-Bit Schlüssel)
Fehlermeldungen		

[<=]

<ToDo: Spezifizieren von Fehlerfällen und Fehlercodes>

5.2 Umsetzung PoPPService:PerformPoPP

5.2.1 Prüfung der Karten (eGK, SMC-B)

A_23277 - PoPP-Modul: Echtheit der eGK prüfen
Der Konnektor MUSS die Echtheit der eGK über eine einseitige Authentisierung mittels INTERNAL AUTHENTICATE prüfen. Der Konnektor MUSS mittels SHA-256 einen Hashwert über die vom PoPP-Dienst in der getChallenge-Response erhaltene Challenge ("challenge") bilden. Der Konnektor MUSS die ersten 192 Bit (= 24 Byte) des Hashwerts bei INTERNAL AUTHENTICATE an die eGK übergeben (als"Data" gemäß [gemSpec_COS#A_16592], bzw. in [gemSpec_COS#14.7.4] meist als "token" bezeichnet). Der Konnektor MUSS die in der Response von der eGK erhaltene Signatur prüfen und dabei das verwendete CV-Zertifikat der eGK bis zu einem CV-Root-CA-Zertifikat aus der TSL verifizieren.**[<=]**

--> Fehler: Echtheitsprüfung der eGK fehlgeschlagen

A_23280 - PoPP-Modul: Challenge-Wert und Signatur der eGK speichern
Der Konnektor MUSS den vom PoPP-Dienst in der getChallenge-Response erhaltenen und lokal verwendeten Challenge-Wert unverändert im Payload des createPoPPToken-Request unter "challenge" ablegen.
Der Konnektor MUSS die Antwort der eGK auf INTERNAL AUTHENTICATE (von der eGK mit PrK.eGK.AUT_CVC erzeugte ECDSA-Signatur) als "egk_signature" base64-kodiert im Payload des createPoPPToken-Request ablegen.**[<=]**

A_23278 - PoPP-Modul: Zertifikat C.CH.AUT der eGK prüfen
Der Konnektor MUSS das AUT-Zertifikat der eGK auslesen und die Gültigkeit prüfen mittels
TUC_KON_037 „Zertifikat prüfen“ {
    certificate = C.CH.AUT;

qualifiedCheck = not_required;
offlineAllowNoCheck = true;
policyList = oid_egk_aut;
intendedKeyUsage= digitalSignature;
intendedExtendedKeyUsage = id-kp-clientAuth;
validationMode = OCSP}.**[<=]**

--> Fehler: Zertifikat der eGK nicht gültig (Fehler bei offline-Zertifikatsprüfung)

A_23279 - PoPP-Modul: Austausch gesteckter Karten erkennen
Der Konnektor MUSS im Verlauf der Operation PerformPoPP die Verarbeitung mit einem Fehler abbrechen, wenn die gesteckte eGK oder die gesteckte SMC-B ausgetauscht wurden (vom KT werden Informationen über einen Wechsel der gesteckten Karten gesendet).**[<=]**

--> Fehler: eGK/SMC-B gezogen / neu gesteckt

5.2.2 Schnittstelle zum PoPP-Dienst

A_23388 - PoPP-Modul: DNS-SD
Der Konnektor MUSS den FQDN und Port des PoPP-Dienstes durch eine DNS-SD Namensauflösung gemäß [RFC-6763] mit dem Bezeichner "_popp._tcp.<DNS_TOP_LEVEL_DOMAIN_TI>." ermitteln.
[<=]

A_23284 - PoPP-Modul: TLS-Verbindungen zum PoPP-Dienst
Der Konnektor MUSS eine TLS-Verbindung zum PoPP-Dienst aufbauen. Dabei MUSS er das durch den Server präsentierte Zertifikat mittels
TUC_KON_037 „Zertifikat prüfen" {
certificate = C.ZD.TSL-S;
qualifiedCheck = not_required;
offlineAllowNoCheck = false;
policyList = oid_zd_tls_s;
intendedKeyUsage= digitalSignature;
intendedExtendedKeyUsage = id-kp-serverAuth;
validationMode = OCSP}
auf Gültigkeit prüfen.
Das Server-Zertifikat C.ZD.TLS-S MUSS für den Produkttyp PoPP-Dienst ausgestellt sein.
[<=]

A_23306 - PoPP-Modul: Schnittstelle I_PoPP_Service umsetzen
Der Konnektor MUSS die Schnittstelle I_PoPP_Service des PoPP-Dienstes umsetzen.**[<=]**

5.2.2.1 Umsetzung I_PoPP_Service:getChallenge

Der Konnektor muss zur Authentisierung vom PoPP-Dienst eine Challenge beziehen. Der Konnektor fordert eine Challenge vom PoPP-Dienst an (GET-Request via HTTPS-Schnittstelle). Die vom PoPP-Dienst empfangene Challenge ist für den Konnektor ein intransparentes (opakes) Objekt. Der Konnektor verwendet die Challenge unverändert bei der Kommunikation mit dem PoPP-Dienst. Für die Kommunikation mit der eGK bildet

der Konnektor einen Hashwert über die Challenge und verwendet die ersten 192 Bit des Hashwerts beim INTERNAL AUTHENTICATE mit der eGK.

A_23262 - PoPP-Modul: Challenge anfordern
Der Konnektor MUSS über die Operation I_PoPP_Service:getChallenge vom PoPP-Dienst eine Challenge anfordern. **[<=]**

5.2.2.2 Umsetzung I_PoPP_Service:createPoPPToken

A_23314 - PoPP-Modul: Pseudonymisierungsschlüssel erzeugen pro PoPP-Nachweis-Bezug
Der Konnektor MUSS einen Pseudonymisierungsschlüssel (AES-Schlüssel der Länge 128 Bit) für jeden PoPP-Nachweis-Bezug (also pro Aufruf der Operation PerformPoPP durch das Primärsystem) zufällig erzeugen.
[<=]

A_23398 - PoPP-Modul: Datenstruktur egk_aut_status erzeugen
Der Konnektor MUSS den Zertifikatsstatus des CH.AUT-Zertifikats im createPoPPToken-Request unter "egk_aut_status" gemäß Tab_eGK_AUT_Status ablegen.

Tabelle 3 Tab_eGK_AUT_Status

Zertifikatsstatus C.CH.AUT	Wert für "egk_aut_status"
Die OSCP-Prüfung erfolgte mit dem Ergebnis "good".	CERT_GOOD
Die OCSP-Prüfung konnte nicht durchgeführt werden.	OCSP_CHECK_REVOCATION_FAILED

[<=]

A_23313 - PoPP-Modul: Datenstruktur enc_egk_data erzeugen
Der Konnektor MUSS für den createPoPPToken-Request die Datenstruktur "enc_egk_data" gemäß Tab_enc_egk_data_Datenstruktur erzeugen.
Der Konnektor MUSS die Datenstruktur "enc_egk_data" gemäß Tab_JSON_Key_Values_enc_egk_data befüllen und die JSON-Values base64-kodiert ablegen.
Der Konnektor MUSS die JSON-Struktur "enc_egk_data" als Byte-Folge serialisieren (kodieren). Diese Byte-Folge MUSS der Konnektor gemäß [gemSpec_Krypt#A_20163-* Punkt 9] mittels AES/GCM und dem Schlüssel aus A_23314-* verschlüsseln.
Sei c = IV (96-Bit) || eigentliches AES/GCM-Chiffrat || 128-Bit Authentication Tag.
Die Base64-Kodierung von c ist die enc_egk_data-Datenstruktur.

Tabelle 4 Tab_enc_egk_data_Datenstruktur

Datenstruktur von "enc_egk_data" (unverschlüsselt):

```
{
  "egk_aut": "...",
  "egk_aut_status": "...",
  "egk_signature": "...",
  "egk_cvc": "...",
  "egk_cvc_ca": "..."
}
```

Tabelle 5 Tab_JSON_Key_Values_enc_egk_data

JSON-Key	JSON-Value
egk_aut	Zertifikat C.CH.AUT der eGK
egk_aut_status	Zertifikatsstatus des C.CH.AUT der eGK
egk_cvc	Zertifikat C.eGK.AUT_CVC der eGK
egk_cvc_ca	Zertifikat C.CA_eGK.CS von der eGK
egk_signature	Von der eGK mit PrK.eGK.AUT_CVC erzeugte ECDSA-Signatur

[<=]

Tabelle 6 Tab_enc_egk_data_Beispiel

Beispiel-Datenelement "enc_egk_data" (unverschlüsselt):

```
{
  "egk_aut": "...",
  "egk_aut_status": "CERT_GOOD",
  "egk_signature": "...",
  "egk_cvc": "...",
  "egk_cvc_ca": "..."
}
```

A_23265 - PoPP-Modul: PoPP-Token anfordern

Der Konnektor MUSS über die Operation I_PoPP_Service:createPoPPToken beim PoPP-Dienst ein PoPP-Token anfordern. Der Konnektor MUSS den Payload mit den privaten Schlüsseln der Identitäten ID.AK.AUT der gSMC-K und ID.HCI.AUT der SMC-B parallel signieren und die Signaturen unter "signatures/signature" base64-kodiert in der JSON-Struktur übertragen. Für jede der beiden Signaturen MUSS im Header der Signaturalgorithmus unter "alg" und das Signaturzertifikat base64-kodiert unter "x5c" abgelegt werden.

[<=]

A_23319 - PoPP-Modul: Signaturalgorithmen für Payload des createPoPPToken-Request

Der Konnektor MUSS für die Signaturen des Payload des createPoPPToken-Request mit der gSMC-K und der SMC-B die Signaturalgorithmen und Bezeichner gemäß Tabelle verwenden, wobei entsprechend der Reihenfolge in der Tabelle der erste verfügbare Algorithmus auf der Karte zu wählen ist.

Tabelle 7 Tab_createPoPPToken_Request_Signaturalgorithmen

Schlüssel	Signaturalgorithmus	Bezeichner für "alg"
ECC auf der Kurve P-256	ECDSA P-256 SHA-256	ES256
ECC auf der Kurve brainpoolP256r1	ECDSA brainpoolP256r1 SHA-256	ES256
RSA Schlüssellänge 2048 (Verständnishinweis: für SMC-B G2.0 Karten ohne ECC-X.509-Identitäten)	RSASSA-PSS SHA-256	PS256

[<=]

Tabelle 8 Tab_createPoPPToken_Request_Beispiel

Request:


```
{
  "payload": "ewogICAgImNoYWxsZW5nZSI6ICIxNjY2NTUyMjc...",
 "signatures":  [
    {
      "header":  {
          "alg": "PS256",
         "x5c": [
              "MIIDcDCCAlgCFGLhrD3t7FkGOlQzHCJgfzGAdZpQMA0GCSq..."
          ]
      },
      "signature":
"C0IA5D9HF9TuebaHd92j6jsKPCR0pxPQ7Iw8qTm0FekQrz0WRgglJgZytm..."
    },
    {
       "header":  {
           "alg": "ES256",
           "x5c":  [
                "MIIB4jCCAYgCFGf+ShVJZKpcC7k+p2IYQkJXCe2NMA..."
           ]
       },
       "signature":
"njsqcQszHt_uYlRppWXeIsFrCp1bltMBTtxU4elgraBgVOkbEGMW-6KMa3h..."
    }
 ]
}
```


Payload:


```
{
 "challenge": "1666552275:Wm1GR8T7wWRhc2jma54itA==",
 "enc_egk_data": "qzFByol8Ueg1HM6tZSF1V5E7eLV8...",
}
```


Hinweise:

Besitzt die signierende Chipkarte (gSMC-K bzw. SMC-B) ECC-X.509-AUT-Identitäten, so werden diese für die Signatur verwendet (Bezeichner ES256), andernfalls wird RSASSA-PSS (Bezeichner PS256) verwendet.

Die in Tab_createPoPPToken_Request_Beispiel aufgeführte Datenstruktur ist konform zu [RFC-7515] (https://www.rfc-editor.org/rfc/rfc7515 JSON Web Signature). Es wird die in [RFC-7515] definierte "JWS JSON Serialization" gewählt, weil diese im Gegensatz zur "JWS Compact Serialization" parallele Signaturen (SMC-K und SMC-B) erlaubt.

Die Angriffe aus RFC-7515#A.6.4 sind im hier vorliegenden Kontext nicht anwendbar. Deshalb werden die "header"-Elemente [RFC-7515] und nicht die "protected"-Elemente verwendet. Dies ermöglicht eine deutlich einfachere Implementierung der Signaturerzeugung und -prüfung.

5.2.2.3 Weitere Vorgaben zu Nachrichten

A_23266 - PoPP-Modul: Content-Type der Nachrichten an PoPP-Dienst
Der Konnektor MUSS die Client-Nachrichten per HTTPS mit dem Content-Type 'application/jose+json' (vgl. [RFC-7515#9.2.1]) an den PoPP-Dienst senden.**[<=]**

5.2.3 Rückgabe an Clientsystem

A_23263 - PoPP-Modul: PoPP-Token und Pseudonymisierungsschlüssel zurückgeben
Der Konnektor MUSS das PoPP-Token unverändert (so wie vom PoPP-Dienst emfangen) an das aufrufende Clientsystem zurückgeben. Der Konnektor DARF das PoPP-Token (JWS Compact Serialization [RFC-7515]) NICHT interpretieren.
Der Konnektor MUSS den vom Konnektor erzeugten (und verwendeten) Pseudonymisierungsschlüssel für die eGK-Daten unverschlüsselt an das aufrufende Clientsystem zurückgeben.

Tabelle 9 Tab_PerformPoPP_Response_Struktur

Struktur des Rückgabeparameters PoPPToken: gemäß A_23308 **(De-)Pseudonymisierungsschlüssel:** gemäß A_23314, base64-kodiert

[<=]

Hinweis: vgl. Abschnitt 5.1.

A_23332 - PoPP-Modul: Rückgabeparameter Pseudonymisierungsschlüssel base64-kodieren
Der Konnektor MUSS den Rückgabeparameter PKey base64-kodiert in der SOAP-Response an das aufrufende Clientsystem übertragen.**[<=]**

5.3 Test

6 PoPP-Dienst

6.1 Schnittstelle I_PoPP_Service

A_23267 - PoPP-Dienst: TLS mit serverseitiger Authentisierung
Der PoPP-Dienst MUSS die Schnittstelle I_PoPP_Service durch verpflichtende Verwendung von TLS mit serverseitiger Authentisierung sichern. Der PoPP-Dienst MUSS sich mit der Identität ID.ZD.TLS-S authentisieren. **[<=]**

A_23268 - PoPP: Webservice über HTTPS
Der PoPP-Dienst und Nutzer der Schnittstelle MÜSSEN die Schnittstelle I_PoPP_Service als Webservice über HTTPS implementieren. Dabei MUSS der PoPP-Dienst mindestens HTTP Version 1.1 unterstützen.**[<=]**

<ToDo: Festlegen der Error-Struktur, Spezifizieren von Fehlerfällen und Fehlercodes, Fehlerhandling beschreiben>

A_23372 - PoPP: JSON-Key/Value-Pairs
Der PoPP-Dienst und Nutzer der Schnittstelle MÜSSEN in Request- und Responsenachrichten JSON-Key-Value-Paare und Kodierungen gemäß Tab_JSON_Key_Values verwenden. Der PoPP-Dienst MUSS vom Nutzer der Schnittstelle zusätzlich eingebrachte Key-Value-Paare beim createPoPPToken-Request tolerieren.

Tabelle 10 Tab_JSON_Key_Values

JSON-Key	JSON-Value
alg	Signaturalgorithmus
challenge	Vom PoPP-Dienst erzeugte Challenge
enc_egk_data	Symmetrisch verschlüsselte Daten der eGK (Zertifikat C.CH.AUT etc.)
header	Struktur für Headerinformationen der Nachricht
iat (Issued At)	Zeitstempel des PoPP-Dienstes
iss (Issuer)	URL des PoPP-Dienstes
payload	Struktur für Payload der Nachricht
signature	Signatur
signatures	Struktur für eine oder mehrere Signaturen
key_egk_data	(De-)Pseudonymisierungsschlüssel für enc_egk_data

tid	Telematik-ID
typ	Media type ("JWT")
used_challenge	Vom PoPP-Dienst erzeugte Challenge
x5c	Signaturzertifikat

[<=]

6.1.1 Operation getChallenge

A_23315 - PoPP: getChallenge URL, HTTP-Methode
Der PoPP-Dienst MUSS die Operation I_PoPP_Service:getChallenge als HTTP GET über die URL https://*<ToDo: FQDN>*/v1/poppService/challenge anbieten. Nutzer der Schnittstelle MÜSSEN die Operation unter dieser URL lokalisieren.
[<=]

A_23331 - PoPP: Struktur getChallenge-Response
Der PoPP-Dienst MUSS die Responses der Operation getChallenge gemäß Tab_getChallenge_Response_Struktur aufbauen. Nutzer der Operation MÜSSEN Responses dieser Struktur verarbeiten.

Tabelle 11 Tab_getChallenge_Response_Struktur

```
{
   "challenge": "..."
}
```

[<=]

6.1.1.1 Umsetzung getChallenge

Ziel der "Challenge" ist es, einen für jeden Beteiligten außer dem PoPP-Dienst unvorhersagbaren Frischeparameter bereitzustellen. Später im Protokoll-Ablauf

1. signiert die eGK mittels des privaten Schlüssels PrK.eGK.AUT_CVC.E256 den auf 192-Bit gekürzten Hashwert der Challenge, und
2. im PoPP-Request des Konnektors wird die Challenge in der vom Konnektor (AK.AUT) und der SMC-B (HCI.AUT) signierten JSON-Datenstruktur aufgeführt (RFC-7515#A.6.4).

Damit ist sichergestellt, dass Zero-Knowledge-Beweise von eGK, gSMC-K und SMC-B (Signaturen, bei denen die DTBS von der Challenge abhängen) nicht vor einer bestimmten Zeit erfolgt sein können (untere Schranke). Beim Ausstellen der PoPP-Nachweises prüft der PoPP-Dienst, dass die im signierten PoPP-Request aufgeführte Challenge tatsächlich vom PoPP-Dienst erzeugt wurde und nicht zu alt ist. Damit ist der Signaturzeitpunkt relativ genau bestimmbar, d. h. der Zeitpunkt, zu dem die Chipkarten dem Primärsystem zur Verfügung standen (Proof of Presence).

A_23264 - PoPP-Dienst: Challenge erzeugen
Der PoPP-Dienst MUSS eine Challenge in Abhängigkeit von seiner aktuellen Systemzeit erzeugen.

Er MUSS dafür die aktuelle Systemzeit als Unix-Zeit mit Sekundengenauigkeit kodieren (Nachkommastellen sind abzuschneiden). Beispiel: 1669237455. Von der Unix-Zeit und dem PoPP-Dienst-internen CMAC-Geheimnis MUSS er per AES-CMAC [RFC-4493] den CMAC berechnen und base64-kodieren. Beide Teile (Zeit und kodierter CMAC) MUSS er per Doppelpunkt zusammenführen.
Beispiel: 1666552275:Wm1GR8T7wWRhc2jma54itA==. Dies ist dann die Challenge, die ein Nutzer der Schnittstelle bei Anfrage (getChallenge) als Antwort erhält. (vgl. A_23331-*)
[<=]

A_23396 - PoPP-Dienst: sichere Speicherung und Verwendung des CMAC-Schlüssel für die Challenge-Erzeugung
Der PoPP-Dienst MUSS den CMAC-Schlüssel (vgl. A_23264) vertraulich im Dienst verwahren. Er MUSS das CMAC-Geheimnis halbjährlich zufällig neu erzeugen. Die Anforderungen zur Schlüsselerzeugung gemäß [gemSpec_Krypt#GS-A_4368] MUSS der PoPP-Dienst umsetzen. [SR1]**[<=]**

A_23316 - PoPP-Dienst: Challenge liefern
Der PoPP-Dienst MUSS im Erfolgsfall eine getChallenge-Response erzeugen und an den Aufrufer zurückgeben.
[<=]

6.1.2 Operation createPoPPToken

A_23318 - PoPP: createPoPPToken URL, HTTP-Methode
Der PoPP-Dienst MUSS die Operation I_PoPP_Service:createPoPPToken als HTTP POST über die URL https://*<ToDo: FQDN>*/v1/poppService/poPPToken anbieten. Nutzer der Schnittstelle MÜSSEN die Operation über diese URL lokalisieren.
[<=]

A_23321 - PoPP: Struktur createPoPPToken-Request
Nutzer der Operation createPoPPToken MÜSSEN die Requests gemäß Tab_createPoPPToken_Request_Struktur aufbauen. Der PoPP-Dienst MUSS Requests dieser Struktur verarbeiten.

Tabelle 12 Tab_createPoPPToken_Request_Struktur

Struktur des Request:
```
{
 "payload": "...",
 "signatures": [
    {
     "header": {
         "alg": "...",
         "x5c":[
              "..."
          ]
      },
     "signature": "..."
    },
    {
      "header": {
          "alg": "...",
          "x5c": [
```

```
                "..."
            ]
        },
        "signature": "..."
    }
  ]
}
```

Struktur des Payload:

```
{
 "challenge": "...",
 "enc_egk_data": "..."
}
```

[<=]

A_23308 - PoPP: Struktur createPoPPToken-Response
Der PoPP-Dienst MUSS die Responses der Operation createPoPPToken gemäß Tab_createPoPPToken_Response_Struktur aufbauen. Nutzer der Operation MÜSSEN Responses dieser Struktur verarbeiten.

Tabelle 13 Tab_createPoPPToken_Response_Struktur

Struktur der Response:
Die Struktur der Response folgt JWS Compact Serialization gemäß [RFC-7515].
Die Signaturerstellung erfolgt nach [RFC-7515].
Für die Kodierung wird Base64URL [RFC-7515#7.1] verwendet.

Die Response enthält drei durch "." getrennte Abschnitte:
<base64URL-kodierter Header>.<base64URL-kodierter Payload>.<base64URL-kodierte Signatur>

Struktur des Header:

```
{
 "typ": "JWT",
 "alg": "...",
 "x5c": [ "..." ]
}
```

Struktur des Payload:

```
{
 "iat": ...,
 "tid": "...",
 "used_challenge": "...",
 "enc_egk_data": "...",
 "iss": "..."
}
```

[<=]

Hinweis: Im folgenden Beispiel-Protokoll-Durchlauf (erzeugt mit der PoC-Implementierung der gematik) stimmen Details wie bspw. die OIDs in den Beispiel-Zertifikaten noch nicht 100%-ig. Dies wird in einer Folge-Version der Spezifikation aktualisiert. Ziel ist es, um das Verständnis zu verbessern, ein Beispiel in seiner Gesamtheit einmal "vorzurechnen".

Tabelle 14 Beispiel Protokolldurchlauf

Response vom PoPP-Dienst auf GET /v1/poppService/challenge


```
{
   "challenge": "1670535981:YRJrjwAy2jKf4Z4xd/ZC/w=="
}
```


Request des Konnektor, POST auf /v1/poppService/poPPToken


```
{
    "payload":
"ewogICAgImNoYWxsZW5nZSI6ICIxNjcwNTM1OTgxOllSSnJqd0F5MmpLZjRaNHhkL1pDL3c9P
SIsCiAgICAiZW5jX2Vna19kYXRhIjogIkZUZ0w0aElwM0orVGRQLzBhL0Vtb01yOGh3c09nUDh
vTFJUOGtFVGN1UmtuTCtuK1NIb0M5VUQ2SkpyVTh6dngrbjBObHN0eHZiOWVuc1VMT0tTQjQrN
0hjOCttQWhpdW5PRHZ0c0hma0FlRHIvc3ZDWW1vMEVqRnlMREJFaW5LOXo5ZUdMQ2RKYXBvK2t
mU3dIUGVQeWc3VWpqRGRDdGJENTJBRTFOdXdpc0YzbjM2ODlXMVNtRWtrSG01QXlaMlo4akJFV
2JJc0l1VWp3YTRHUFBiZHZKaXg3MGkxTTZiK28ybm9JZWY4eEpFajFKYjB1bVhYT1dhUTlBRWN
0ekJwM0U0QzIyYkpZRmMrSkVoU0t5S2NBUU9TMXhRVDJaV3RrRWdqYXh2YkxGZUgwUTcwVGh1N
WRxQ2U3enR5YUJBUkFrZzFNRGF5WFk0MFdMRE9VcEw2RWxTS05rUjZRYjUxV3ByTVlFeG5RV0J
XMTRBQ2ZXZFZvZjArM0NhRWd4UTg4SlNrSWdyR0U0dFU5SjRzcTRjZVhyTE1ydlpJNDlWQ2RFW
Wt5NURMemk5TllWOVJaMDVNSW9xcTJHNWgwQmVpdlAxb0I4Zlh1UURVSTA2UnZiSjNpN3dvcjl
lRzZKeXNSTjE0V2F1ejlQS1hmcEw3R001eWRwbmZQSVcwU2NoTzYyeGVHU29YMjRUYjRHcW1ka
DNtVlFOMTFWdENkVTBTT1hmU2FucElmaklkL2xac0EvTWdLMm1QZng0N2JNM0pqb2Q1KzVPbWp
zVW1KSHFmcHpCajZSQTFmZWRkeE9TSEtNMkVtZER4aU1NNVBJRHU3U2pGQjI4Y0Z2WEN6eHBCV
GxiWno3dG55aXptVW8wT2FYLzMrMGJQZkZhZTBLaWhyZ2JQMDBIWGMyQm5COGExR1FCY0Q4OVU
2UDBJV0pDVEJjM3FmRXAxd1I4elVBSTJvaEpVWWNjdHZQdzhRemtMTytwQWxNMW5XOW11U0xMV
EI0eVJrQzhJczB0TXdzeVVkOHMvbVA4WFViajJjemMvTnY0MitRalAyaDhLQU0vUGo1a2JzUm9
DOG16WDJrck5JbGs1QWtLd2NwdFZUY0l3QytqNTFXRU9RaGhpaFdoOWtraUk2UGZjNE5LdXFqd
jVmaW52cVNkdWREYUo0dGRrRjhmU3FlY3p2V0prc3REdFlSSWMzVWtuZjVHZFYzNnQyNlV6WWU
vUzRDSlFRM0YzSHNabk5VTWdMRlNUWDE3YnA4Q1RyODBnNCtSUHJFRHFWeFYyeVBzYUhvWmZzb
mdRczh1YTUvSzlmd09vSjVldEwvS2Izenl3UTNhQmFJSFBPaUwzdGNuMGYrTmk1MnpxdnM5dCt
3PSIKfQ==",
    "signatures": [
        {
            "header": {
                "alg": "RS256",
                "x5c":
[                     "MIIDcDCCAlgCFGLhrD3t7FkGOlQzHCJgfzGAdZpQMA0GCSqGSIb3
DQEBCwUAMGYxCzAJBgNVBAYTAkRFMQ8wDQYDVQQIDAZCZXJsaW4xDzANBgNVBAcMBkJlcmxpbj
EQMA4GA1UECgwHZ2VtYXRpazEQMA4GA1UECwwHZ2VtYXRpazERMA8GA1UEAwwIU01DLUItQ0Ew
HhcNMjIxMDIzMTMzMjQwWhcNMjMxMDIzMTMzMjQwWjCBgjELMAkGA1UEBhMCREUxDzANBgNVBA
gMBkJlcmxpbjEPMA0GA1UEBwwGQmVybGluMRAwDgYDVQQKDAdnZW1hdGlrMRAwDgYDVQQLDAdn
ZW1hdGlrMS0wKwYDVQQDDCRBcnR6cHJheGlzIFRJRD00OjE6MTIzMTMyMTQyMzU0MzI0MTEwgg
EiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDR6kjVj5NFBACYfP0Of06/mcFhEIUIH9Qk
lcPZvkc7k3LX1p8KzQ/qGF2ASHz9ZZcmHpghUIF/NcVtNcnPpYvLMDOn92Tvm7E6x3F8+NUw/2
42C62+DIDk+X0aPOTEQ+uS2AbG3gl0zSAHNGTqQjmsPeoxrmjkNGbKx3GXOiqnJFcpq6OG4CMa
QrqaPjWZJ9yoFEKHy1+HR6N7yzS0lUlKe6qRpkfW28aSpqa26mcAzNdkfdUUoPI9RideqOW2W5
msMdZYXCsIlG5pFYE881FhzfeeoEiapEOiYyKJERbYpIn98DRDDaPWuaUgvImYGW/Tk2LmRli5
XbWaidWxC8pXAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAL/zq/Vdou1ugRo5kMSnJYeXY3xLJM
3mEkf1FJN/CljntiS07z30fUNnUce4jfch7OY98dRrfB3D1D5WUG9Cito5Ztx9kMIYsTOJJfrF
4OWHZXpvOxACdTjsf6a2KIJZiNqeg3ux81ynxkg14TrsGC2q4iaHoqH0wdBa5V8wgSGA8gtim+
```

```
pbn6+ZC82xePrLpk4ResxczUf7mpiOfC+3NNStDr1WqzH6rtPIriRldDbZ3Md2ncKRBPh9QBbc
odLDqurOHG2M/H3eZ2QdckuLal/onJ8cd+uOdtZAE0MLhLAsZ+bb4iSqN/R40DP7y6R9wUN6tY
MiI+1buXErwWM08tA="
                ]
            },
            "signature":
"XQrQWx_e_8o905iE4Y6n5msOO_TMUGf8wDxgVy9C1UVxVDFq9a98bLsItj1I-apbPItp--
azYSumyfHjg5pCa53OC-sKe2bhXCRVrS7APEiTu8sJkypuX9kI9I2rcD3ilnVQXfoBb1R-
YRz0tDYE95A7lNJzc6kpGL_7FlRUbOky3lPgZBvth5NkixwJqv7MKRYnFRngUVQa8y7IEwLE01
98M9tqD0EH9PH4deB4ZNvjm5Sf3kCwsXeuqSKXmOTl4w1ZQi7xNPv0-iIj00C5PNg-
UJBU3__jx3RO9SRQBtn7tQZBklT_yl4hYu2rtnIKumjdfT6Vm4qmwVBbMJsLyw=="
        },
        {
            "header": {
                "alg": "PS256",
                "x5c":
[                    "MIIB4jCCAYgCFGf+ShVJZKpcC7k+p2IYQkJXCe2NMAoGCCqGSM49
BAMCMHAxCzAJBgNVBAYTAkRFMQ8wDQYDVQQIDAZCZXJsaW4xDzANBgNVBAcMBkJlcmxpbjEQMA
4GA1UECgwHZ2VtYXRpazEQMA4GA1UECwwHZ2VtYXRpazEbMBkGA1UEAwwSS29tcG9uZW50ZW4t
UEtJLUNBMB4XDTIyMDkyNDA3NTIzN1oXDTIzMDkyNDA3NTIzN1owdjELMAkGA1UEBhMCREUxDz
ANBgNVBAgMBkJlcmxpbjEPMA0GA1UEBwwGQmVybGluMRAwDgYDVQQKDAdnZW1hdGlrMRAwDgYD
VQQLDAdnZW1hdGlrMSEwHwYDVQQDDBhLb25uZWt0b3ItQUstWmVyaXRpZmlrYXQwWjAUBgcqhk
jOPQIBBgkrJAMDAggBAQcDQgAEEXKDSSXSBkJ2gyQYX0e8gxCQFch2hUlGqRrTRmsWx4UTwOX6
8uiyFCGv4E4fMZpzU7xKXSFDBtgpo2omJU4mbDAKBggqhkjOPQQDAgNIADBFAiEAkFSKpKfxvq
holKnaOv7M1q1v50WYcEOkdLfCfg7Cz2YCIAUwOF7zEBFOZGL81ebsLVH/PcXN1Qpun7GP5Ov1
Jzcs"
                ]
            },
            "signature": "auCaJrcfN1OaisE5HsZVB-
QCfpCt3BVkhtuu7b1QlXyjeA9UR3NG3dnLbmdWE2Ml3dLhHxHo5Ya-CEUFa96Rmg=="
        }
    ]
}
```


Im Beispiel hat die SMC-B nur ein RSA-AUT-Zertifikat und der Konnektor besitzt RSA- und ECC-X.509-Zertifikate. Deshalb verwendet der Konnektor gemäß A_23319 das ECC-Material für die SMC-K-AUT-Signatur.

Der Wert in o. g. "payload" base64-dekodiert:


```
{
    "challenge": "1670535981:YRJrjwAy2jKf4Z4xd/ZC/w==",
    "enc_egk_data":
"FTgL4hIp3J+TdP/0a/EmoMr8hwsOgP8oLRT8kETcuRknL+n+SHoC9UD6JJrU8zvx+n0Nlstxv
b9ensULOKSB4+7Hc8+mAhiunODvtsHfkAeDr/svCYmo0EjFyLDBEinK9z9eGLCdJapo+kfSwHP
ePyg7UjjDdCtbD52AE1NuwisF3n3689W1SmEkkHm5AyZ2Z8jBEWbIsIuUjwa4GPPbdvJix70i1
M6b+o2noIef8xJEj1Jb0umXXOWaQ9AEctzBp3E4C22bJYFc+JEhSKyKcAQOS1xQT2ZWtkEgjax
vbLFeH0Q70Thu5dqCe7ztyaBARAkg1MDayXY40WLDOUpL6ElSKNkR6Qb51WprMYExnQWBW14AC
fWdVof0+3CaEgxQ88JSkIgrGE4tU9J4sq4ceXrLMrvZI49VCdEYky5DLzi9NYV9RZ05MIoqq2G
5h0BeivP1oB8fXuQDUI06RvbJ3i7wor9eG6JysRN14Wauz9PKXfpL7GM5ydpnfPIW0SchO62xe
GSoX24Tb4Gqmdh3mVQN11VtCdU0SOXfSanpIfjId/lZsA/MgK2mPfx47bM3Jjod5+5OmjsUmJH
qfpzBj6RA1feddxOSHKM2EmdDxiMM5PIDu7SjFB28cFvXCzxpBTlbZz7tnyizmUo0OaX/3+0bP
fFae0KihrgbP00HXc2BnB8a1GQBcD89U6P0IWJCTBc3qfEp1wR8zUAI2ohJUYcctvPw8QzkLO+
pAlM1nW9muSLLTB4yRkC8Is0tMwsyUd8s/mP8XUbj2czc/Nv42+QjP2h8KAM/Pj5kbsRoC8mzX
2krNIlk5AkKwcptVTcIwC+j51WEOQhhihWh9kkiI6Pfc4NKuqjv5finvqSdudDaJ4tdkF8fSqe
czvWJkstDtYRIc3Uknf5GdV36t26UzYe/S4CJQQ3F3HsZnNUMgLFSTX17bp8CTr80g4+RPrEDq
VxV2yPsaHoZfsngQs8ua5/K9fwOoJ5etL/Kb3zywQ3aBaIHPOiL3tcn0f+Ni52zqvs9t+w="
}
```

Der vom Konnektor erzeugte und verwendete Pseudonymisierungsschlüssel (base64-kodiert):

TvRIybprnMLZD9H8GnRcnw==

Antwort des PoPP-Dienstes auf diesen Request:

eyJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NiIsIng1YyI6WyJNSUlCMHpDQ0FYb0NGR2YrU2hWSl
pLcGNDN2srcDJJWVFrSlhDZTJNTUFvR0NDcUdTTTQ5QkFNQ01IQXhDekFKQmdOVkJBWVRBa1JG
TVE4d0RRWURWUVFJREFaQ1pYSnNhVzR4RHpBTkJnTlZCQWNNQmtKbGNteHBiakVRTUE0R0ExVU
VDZ3dIWjJWdFlYUnBhekVRTUE0R0ExVUVDd3dIWjJWdFlYUnBhekViTUJrR0ExVUVBd3dTUzI5
dGNHOXVaVzUwWlc0dFVFdEpMVU5CTUI0WERUSXlNRGt5TkRBM05USXpOMW9YRFRJek1Ea3lORE
EzTlRJek4xb3dhREVMTUFrR0ExVUVCaE1DUkVVeER6QU5CZ05WQkFnTUJrSmxjbXhwYmpFUE1B
MEdBMVVFQnd3R1FtVnliR2x1TVJBd0RnWURWUVFLREFkblpXMWhkR2xyTVJBd0RnWURWUVFMRE
FkblpXMWhkR2xyTVJNd0VRWURWUVFEREFwR1lXTm9aR2xsYm5OME1Gb3dGQVlIS29aSXpqMENB
UVlKS3lRREF3SUlBUUVIQTBJQUJLSkpwdG11amJjTFIwRUk2TS9IVjQ5NTBLdklFeVhtcXFtWF
Q3cmFGZ1U3ZmpwTWc0QzhZNXRzK0h4TDM4YjVzR2JhanJWRGZlSGw2bWo3dzBJNGsyZ3dDZ1lJ
S29aSXpqMEVBd0lEUndBd1JBSWdYSkxBNTVLL25mOWdBamZJbzhXUXBiSWZzQzJma0llRmFBS1
M4M0xLSWJvQ0lISGxKTFp0RUVmYjh5T2EwZXNOSDhIZUdYc3VZeHRXWVhHQ01MVHhMZWR2Il19
.eyJpYXQiOjE2NzA1MzIzODEuNTk1NTc3LCJ0aWQiOiI0OjE6MjIzNDMxNDM0MyIsInVzZWRfY
2hhbGxlbmdlIjoiMTY3MDUzNTk4MTpZUkpyandBeTJqS2Y0WjR4ZC9aQy93PT0iLCJlbmNfZWd
rX2RhdGEiOiJGVGdMNGhJcDNKK1RkUC8wYS9FbW9Ncjhod3NPZ1A4b0xSVDhrRVRjdVJrbkwrb
itTSG9DOVVENkpKclU4enZ4K24wTmxzdHh2YjllbnNVTE9LU0I0KzdIYzgrbUFoaXVuT0R2dHN
IZmtBZURyL3N2Q1ltbzBFakZ5TERCRWluSzl6OWVHTENkSmFwbytrZlN3SFBlUHlnN1VqakRkQ
3RiRDUyQUUxTnV3aXNGM24zNjg5VzFTbUVra0htNUF5WjJaOGpCRVdiSXNJdVVqd2E0R1BQYmR
2Sml4NzBpMU02YitvMm5vSWVmOHhKRWoxSmIwdW1YWE9XYVE5QUVjdHpCcDNFNEMyMmJKWUZjK
0pFaFNLeUtjQVFPUzF4UVQyWld0a0VnamF4dmJMRmVIMFE3MFRodTVkcUNlN3p0eWFCQVJBa2c
xTURheVhZNDBXTERPVXBMNkVsU0tOa1I2UWI1MVdwck1ZRXhuUVdCVzE0QUNmV2RWb2YwKzNDY
UVneFE4OEpTa0lnckdFNHRVOUo0c3E0Y2VYckxNcnZaSTQ5VkNkRVlreTVETHppOU5ZVjlSWjA
1TUlvcXEyRzVoMEJlaXZQMW9COGZYdVFEVUkwNlJ2YkozaTd3b3I5ZUc2SnlzUk4xNFdhdXo5U
EtYZnBMN0dNNXlkcG5mUElXMFNjaE82MnhlR1NvWDI0VGI0R3FtZGgzbVZRTjExVnRDZFUwU09
YZlNhbnBJZmpJZC9sWnNBL01nSzJtUGZ4NDdiTTNKam9kNSs1T21qc1VtSkhxZnB6Qmo2UkExZ
mVkZHhPU0hLTTJFbWREeGlNTTVQSUR1N1NqRkIyOGNGdlhDenhwQlRsYlp6N3RueWl6bVVvME9
hWC8zKzBiUGZGYWUwS2locmdiUDAwSFhjMkJuQjhhMUdRQmNEODlVNlAwSVdKQ1RCYzNxZkVwM
XdSOHpVQUkyb2hKVVljY3R2UHc4UXprTE8rcEFsTTFuVzltdVNMTFRCNHlSa0M4SXMwdE13c3l
VZDhzL21QOFhVYmoyY3pjL052NDIrUWpQMmg4S0FNL1BqNWtic1JvQzhtelgya3JOSWxrNUFrS
3djcHRWVGNJd0MrajUxV0VPUWhoaWhXaDlra2lJNlBmYzROS3VxanY1ZmludnFTZHVkRGFKNHR
ka0Y4ZlNxZWN6dldKa3N0RHRZUkljM1VrbmY1R2RWMzZ0MjZVelllL1M0Q0pRUTNGM0hzWm5OV
U1nTEZTVFgxN2JwOENUcjgwZzQrUlByRURxVnhWMnlQc2FIb1pmc25nUXM4dWE1L0s5ZndPb0o
1ZXRML0tiM3p5d1EzYUJhSUhQT2lMM3RjbjBmK05pNTJ6cXZzOXQrdz0iLCJpc3MiOiJodHRwc
zovL3BvcHAudGVsZW1hdGlrLiJ9.psV23oKaw7nMJ8lI2aJTrM5_3jrn0gNd9lukpdLP1dse0w
JFoTQ9g0syjhoNuxra2BqhAspHcpDU51clPirkdA

In diesem Token ([RFC-7519], [RFC-7515]) gibt es drei durch "." getrennte Abschnitte. Im mittleren Abschnitt befindet sich der payload, welche base64url-dekodiert [RFC-7515#7.1] folgenden Wert besitzt. (Hinweis: https://jwt.io kann man gut zum Dekodieren verwenden.)


```
{
  "iat": 1670531708.043164,
  "tid": "4:1:2234314343",
  "used_challenge": "1670535307:0fEFISWL7SB9FvpRwqVHqg==",
  "enc_egk_data":
"nkZkt/mC2jKjk3JrutsMmGslChRA9oH4hAA5Saswa7XU7cJHPIOCobfXZINBJX2Sd5/lQMAcf
wgvEGQ2dtQ2bIfGpR8w4jVjNdZAbVuF+UVehWMRxWWGFzauW/Tbo5NyIB4PL7AajyPbNDM8m1A
4sXRE5lWZ7CVAAs2cyIKIZU81255/OdUNVwUCXSP8YrSdCFTTG64imikJR9q0ijONXhbt8QuQ+
k2qcwqmgiJYq00w1u3WevmtIbXguu7PCSBqUyi7CQspNuzDWyV0iNISp4tnhU7m20UGpxqPDa/
o3ZFSilKEqgJ5lv605sK3358AoHRNlEe/PBjUPk3X3NyYadqBa+snJzg7e4SqKoz/oimQMy5HE
```

```
W7m6zTRgg2isQZrVvdrJhIrbCmX+FDhMZK/Cfedn2IEwZLCGVCcZkbnmvpq5kUplupf5v0Q6PT
GgwklehJcqeYRrdOr7/xv2uMqlyud+t4wrh1J1Y9X21GXDngeZISL4FKjEMfTWgRfzV6wXgr8v
KhU8BTkbMaU8NBRMRpAAYCOxzIGqZVzPCazGzEFJu+m1/eeODu2JBUfNJ8854w+mE6Hn1JRCw2
74hvIddyTgoZKmufnKnGMEOIF3tihQiXm4hoWSbRdyBqaRv3Nu5c6Bf1KymqOhNWcVbuFoDFdd
nFU5O8FCZ7emPpbgHRbyvx1kt5W0dK4UH9Le/4pF5pBK1C497b/PjUcXnEg9ifVuhehDAavDg7
9B4OQhUvB6bdVme4wHGC/NKs8f2+iT+hyTmOQ1j2VRofhi/dQtBP8zoy+dJXRBCjfDjkZ7C/fc
f9guQgu4lmZxjcf5TlUQlRaFgVra5JF1XUp/Zxc1THRkLEd2oJF96GaVjWDoNwBZ16OYr6zk/0
qB2L0CrvgGGCVUVjFRUtRlugBWXavihNuuuiVaIfCd6lceKUjCRE1zdYZ9mT/SrqytnZOE/yEM
3pj8di9eyIqEs1LyAe0oUPcRHEOfOobRcyNCya8K4PQGzYGzFU4inP8L2JWMM+x5xOzlY0=",
  "iss": "https://popp.telematik."
}
```


Der Rückgabewert des PoPP-Dienstes ("eyJ0eXAiO...") ist das PoPP-Token (PoPP-Nachweis). Dieses wird neben dem (De-)Pseudonymisierungsschlüssel an das aufrufende Primärsystem als Antwort übergeben (vgl. Abschnitt5.1- Schnittstelle zum Clientsystem (A_23323)).

6.1.2.1 Umsetzung createPoPPToken

A_23320 - PoPP-Dienst: Signaturen und Zertifikate im createPoPPToken-Request prüfen

Der PoPP-Dienst MUSS die mit den Identitäten ID.AK.AUT und ID.HCI.AUT erstellten Signaturen des Payload des createPoPPToken-Request prüfen. Der PoPP-Dienst MUSS die Signaturzertifikate C.AK.AUT und C.HCI.AUT gemäß TUC_PKI_018 prüfen (Prüfmodus=OCSP, TOLERATE_OCSP_FAILURE=false). Zertifikatsprüfergebnisse und OCSP-Antworten dürfen bis zu 12 Stunden gecacht und wiederverwendet werden.**[<=]**

A_23307 - PoPP-Dienst: CMAC prüfen

Der PoPP-Dienst MUSS prüfen, ob die im createPoPPToken-Request enthaltene Challenge ("challenge") vom PoPP-Dienst stammt, indem er den in der Challenge enthaltenen CMAC prüft. Falls der CMAC ungültig ist ("INVALID" [RFC-4493]), so MUSS der PoPP-Dienst die Abarbeitung des Protokolls mit einem Fehler an den Konnektor abbrechen. **[<=]**

A_23312 - PoPP-Dienst: Alter der Challenge prüfen

Der PoPP-Dienst MUSS prüfen, dass die im createPoPPToken-Request enthaltene Challenge ("challenge") nicht älter als 10 Minuten ist.**[<=]**

A_23326 - PoPP-Dienst: PoPP-Token signieren

Der PoPP-Dienst MUSS den Payload der createPoPPToken-Response mit dem privaten Schlüssel der Identität ID.ZD.SIG mit der technischen Rolle oid_popp signieren. Der PoPP-Dienst MUSS den Signaturalgorithmus entsprechend des vom ZD.SIG-Zertifikats unterstützten Schlüssels wählen. Den Bezeichner MUSS der PoPP-Dienst gemäß Tab_createPoPPToken_Response_Signaturalgorithmen verwenden. Die Signatur der Response erfolgt nach [RFC-7515].

Tabelle 15 Tab_createPoPPToken_Response_Signaturalgorithmen

Schlüssel	Signaturalgorithmus	Bezeichner für "alg"
ECC auf der Kurve P-256	ECDSA P-256 SHA-256	ES256
ECC auf der Kurve brainpoolP256r1	ECDSA brainpoolP256r1 SHA-256	ES256

[<=]

A_23317 - PoPP-Dienst: PoPP-Token liefern
Der PoPP-Dienst MUSS die createPoPPToken-Response erzeugen und an den Aufrufer zurückgeben.**[<=]**

6.2 Schnittstellen zu zentralen Diensten

A_23309 - PoPP-Dienst: TSL laden
Der PoPP-Dienst MUSS die TSL einmal täglich vom TSL-Dienst beziehen und die vertrauenswürdigen Komponenten-CAs und CAs der TSPs-SMC-B extrahieren. **[<=]**

A_23310 - PoPP-Dienst: Resource Records für DNS-SD
Der Anbieter des PoPP-Dienstes MUSS in den Nameservern TI die Resource Records gemäß Tabelle Tab_PoPP_DNS_SD verwalten.

Tabelle 16 Tab_PoPP_DNS_SD

Resource Record Bezeichner	Beschreibung
_popp._tcp.telematik.	SRV Resource Record zur Ermittlung von FQDN und Port des PoPP-Dienstes
FQDN des PoPP-Dienstes	A Resource Record zur Namensauflösung von FQDN des PoPP-Dienstes in IP-Adresse

[<=]

6.3 Datenschutz

A_23367 - Keine Protokollierung und Persistierung personenbezogener Daten
Der PoPP-Dienst DARF personenbezogene Daten NICHT protokollieren und NICHT persistieren.**[<=]**

6.4 Sicherheit

A_23305 - PoPP-Dienst - Speicherung privater Schlüssel mit einem HSM
Der Anbieter des PoPP-Dienstes MUSS den privaten Signaturschlüssel mit einem HSM speichern und sicherstellen, dass die Eignung des HSM durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Federal Information Processing Standard (FIPS) oder Common Criteria mit mindestens folgender Prüftiefe in Frage:

1. FIPS 140-2 Level 3 oder
2. Common Criteria EAL 4.

[<=]

A_23424 - Sichere Nutzungsprozesse zum HSM
Der Anbieter des PoPP-Dienstes MUSS sichere Prozesse zur Personalisierung und des Betriebs des HSMs (A_23305*) definieren und etablieren, die gewährleisten, dass

1. das Schlüsselmaterial für die Identität FD.SIG im HSM erzeugt wird,
2. der private Schlüssel PrK.FD.SIG nur in einem HSM im Klartext vorliegt,
3. Erzeugen, Backup, Restore und Löschen des Schlüssel PrK.FD.SIG sowie die Erzeugung und der Export des Certificate Signing Request (CSR) nur im 4-Augen-Prinzip möglich ist,
4. der CSR unter Wahrung der Integrität und der Vorgaben des TSPs an den TSP übertragen wird, eine Verifikation des vom TSP erhaltenen Zertifikats im 4-Augen-Prinzip erfolgt, dass diese den korrekten öffentlichen Schlüssel PubK.FD.SIG enthält,
5. die Konfiguration des PoPP-Dienst zur Nutzung des privaten Schlüssels PrK.FD.SIG im HSM (Kopplung von PoPP-Dienst und HSM) nur im 4-Augen-Prinzip möglich ist und
6. eine Nutzung des privaten Schlüssels PrK.FD.SIG durch Personal des Anbieters abgesehen von der Erstellung des CSR ausgeschlossen ist.

[<=]

6.5 Betrieb

6.5.1 Servicekonzept

6.5.1.1 Servicemodell

6.5.1.1.1 Servicezerlegung

Eigener Service	E
Unterstützungsservice	U
Vermittelnder Unterstützungsservice	V
Unterstützung optional	O
Keine verpflichtende Verbindung	.

Servicekomponenten (SK)	ID's	A1 Anbietertyp KTR-AdV	A2 Anbietertyp VPN-Zugangsdienst	A3 Anbieter ZPD	A4 Fachdienst VSDM	A5 gematik Test	A6 gematik Betrieb	A7 Gesamtverantwortlicher TI (GTI)	A8 Anbietertyp Service Monitoring	A9 Anbietertyp HBA	A10 Anbietertyp SMC-B / HSM-B	A11 Anbietertyp X.509 TSP eGK	A12 Anbietertyp Signaturdienst	A13 Anbietertyp X.509 Root-CA	A14 Anbietertyp TSP CVC eGK	A15 Anbietertyp CVC-Root-CA	A16 Anbietertyp Fachdienst KOM-LE	A17 Anbietertyp Anschlusspunkt SGW / SZZP	A18 WANDA Basic	A19 WANDA Smart	A20 WANDA Smart Hosting	A21 Anbietertyp ePA-Aktensystem	A22 Anbietertyp Basis-Consumer	A23 Anbietertyp KTR-Consumer	A24 Anbietertyp SGD_ePA zentral	A25 Anbietertyp IdP-Dienst	A26 Anbietertyp E-Rezept-Fachdienst	A27 Anbietertyp E-Rezept FdV	A28 Anbietertyp TI Messenger	A29 Anbietertyp Apothekenverzeichnis	A30 Anbietertyp Highspeed Konnektor	A31 Serviceprovider NCPeH-Fachdienst	A32 Anbietertyp PoPP Dienst
SK FD VSDM	1	V	V	V	E	.	.	.	.	.	.	V	.	.	V	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
SK Signatur und Verschlüsselung	2	.	.	V	.	.	.	.	.	V	V	V	.	.	V	.	U	.	.	.	.	.	.	.	V	.	.	.	.	.	.	.	.
SK Zugang zur TI	3	.	E	E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
SK Sicherer Internetzugang	4	.	E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
SK Konnektor Konfigurationsservice des LE	5	.	U	V	.	.	.	.	.	.	V	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
SK initiale Integration SMC-B des LE	6	.	U	.	.	.	.	.	.	U	U	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
SK Anbindung Bestandsnetze [1]	7	.	U	U	.	.	.	.	.	.	.	.	.	.	.	.	.	U	U	.	.	.	.	.	.	.	.	.	.	.	.	.	.
SK Konfigurationsdienst	8	.	V	E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
SK Verzeichnisdienst	9	.	V	E	.	.	.	.	.	.	.	.	.	.	.	.	U	.	.	.	.	.	U	U	U	U	U	U	.	U	.	.	U
SK Zentrales Netz	10	.	V	E	U	.	.	.	.	U	U	U	.	.	.	.	U	.	.	U	U	.	U	U	U	.	.	.	.	.	.	U	U
SK Zeitdienst	11	.	V	E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	U	U	U	.	.	.	.	.	.	.	U
SK Namensdienst	12	.	V	E	U	.	.	.	.	.	.	.	.	.	.	.	U	.	.	U	U	U	U	U	U	U	U	.	.	.	.	U	U
SK TSL Dienst	13	.	V	E	.	.	.	.	.	U	U	U	.	.	.	U	.	.	.	.	.	.	U	U	U	.	.	.	.	.	.	.	U
SK Intermediär VSDM	14	.	V	E	V	.	.	.	.	.	.	U	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
SK CVC Root CA	15	.	.	.	.	.	.	.	.	.	.	.	.	.	.	E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
SK TSP CVC	16	.	V	E	.	.	.	.	.	E	E	.	.	.	E	U	.	.	.	.	.	.	U	U	U	.	.	.	.	.	.	.	.
SK X.509 Root CA	17	.	V	E	.	.	.	.	.	.	.	.	.	E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
SK TSP X.509	18	.	V	E	.	.	.	.	.	E	E	E	.	.	.	.	.	.	.	.	.	.	U	U	U	U	U	U	.	.	.	.	U
SK OCSP Responder Proxy	19	.	V	E	.	.	.	.	.	E	E	E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	U
SK Weitere Anwendungen	20	.	U	U	.	.	.	.	.	.	.	.	.	.	.	.	.	U	E	E	E	.	.	.	.	.	.	.	.	.	.	.	.
SK Anschlusspunkt	21	.	U	U	.	.	.	.	.	.	.	.	.	.	.	.	.	E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
SK E-Rezept-Fachdienst	22	.	V	U	.	.	.	.	.	U	U	U	U	.	.	.	.	.	.	.	.	.	.	.	.	U	E	U	.	.	.	.	.
SK IdP-Dienst	23	.	V	U	.	.	.	.	.	U	U	U	.	U	.	.	.	.	.	.	.	.	.	.	.	E	U	U	U	.	.	.	.
SK E-Rezept FdV [5]	24	.	.	U	.	.	.	.	.	.	.	U	.	.	.	.	.	.	.	.	.	.	.	.	U	U	U	E	.	.	.	.	.
SK Apothekenverzeichnis	25	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	U	U	.	E	.	.	.
SK KOM-LE	26	.	U	U	.	.	.	.	.	.	.	.	.	.	.	.	E	.	.	.	.	.	U	U	.	.	.	.	.	.	.	.	.
SK Service Monitoring	27	.	U	U	U	.	.	.	E	U	U	U	.	U	.	.	U	.	.	.	.	U	.	.	U	U	U	U	U	U	.	.	U
SK ePA-Aktensystem	28	.	U	U	.	.	.	.	.	U	U	U	U	.	.	.	.	.	.	.	.	E	.	U	U	.	.	.	.	.	.	U	.
SK KTR-Consumer	29	.	.	U	.	.	.	.	.	.	U	.	.	.	.	.	U	.	.	.	.	U	.	E	.	.	.	.	.	.	.	.	.
SK Basis-Consumer	30	.	.	U	.	.	.	.	.	.	U	.	.	.	.	.	U	.	.	.	.	.	E	.	.	.	.	.	.	.	.	.	.
SK Signaturdienst [2]	31	.	V	V	.	.	.	.	.	.	.	[2]	E [2]	U	.	.	.	.	.	.	.	U	.	.	U	.	U	.	.	.	.	.	.
SK SGD_ePA am FD	32	.	.	.	.	.	.	.	.	.	.	U	.	U	.	.	.	.	.	.	.	E	.	.	U	.	.	.	.	.	.	U	.
SK SGD_ePA zentral	33	.	.	.	.	.	.	.	.	.	.	U	.	U	.	.	.	.	.	.	.	U	.	.	E	.	.	.	.	.	.	U	.
SK KTR-AdV	34	.	.	.	.	.	.	.	.	.	.	U	.	U	.	.	.	.	.	.	.	U	.	.	E	.	.	.	.	.	.	.	.
SK Versicherten Help Desk E-Rezept	35	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
SK VZD FHIR Directory	36	.	.	E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	U	.	.	.	.
SK TI-Messenger Fachdienst	37	.	.	U	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	E	.	.	.	.
SK TI-Messenger Client	38	.	.	U	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	U	.	.	E	.	.	.	.
SK Highspeed Konnektor	39	.	.	U	.	.	.	.	.	.	U	.	.	.	.	.	U	.	U	U	U	U	.	.	U	U	U	.	.	.	E	.	U
SK NCPeH-Fachdienst	40	.	.	.	.	.	.	.	.	.	U	.	.	.	.	.	.	U	.	.	.	U	.	.	U	.	.	.	.	.	.	E	.
SK PoPP-Dienst	41	.	V	U	.	.	.	.	.	.	U	U	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	E
Anbieten eines User Help Desks (UHD) 09:00 bis 17:00 [3]	100	.	.	.	.	.	.	.	.	E	E	.	.	.	.	.	E	E	.	.	.	.	.	.	.	.	.	.	E	.	.	E	.
Anbieten eines User Help Desks (UHD) 24 / 7 [31]	101	.	E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
Anbieten eines Versicherten Help Desks (VHD) 09:00 bis 17:00 Mo-Fr [32]	102	.	.	.	.	.	.	.	.	.	.	.	E	.	.	.	.	.	.	.	.	E	.	.	.	.	.	.	.	.	.	E	.
Anbieten eines Versicherten Help Desks (VHD) 08:00 bis 20:00 Mo-Fr [33]	103	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
Anbieten eines Versicherten Help Desks (VHD) 07:00 bis 22:00 Mo-Fr [34]	104	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	E	.	.	.	.	.
ServiceLevel (SLA) Zuordnung in Haupt- und Nebenzeit (H/N)	120	H	H/N	H/N	H	.	.	.	.	H	H/N	H	H/N	H	H	.	H/N	H	.	.	.	H/N	H	H	H/N	H/N	H/N	H/N	H/N	H/N	.	H/N	H/N
Lieferung von Rohdaten (R)	121	.	R	.	R	.	.	.	.	R	R	R	R	.	.	.	R	.	.	.	.	R	.	.	R	R	R	.	R	R	.	R	R

[1] Die Anbindung der Bestandsnetze erfolgt außerhalb der Regelungshoheit der gematik
[2] Die SK Signaturdienst neu nicht mehr Option des Anbieters TSP X.509 eGK
[3] siehe AFO TIP1-A_7260-01
[31] siehe AFO A_19532-01
[32] siehe AFO A_16217-01
[33] siehe AFO A_20734-01
[34] siehe AFO A_20733-03
[5] Die SK E-Rezept FdV enthält auch die SK E-Rezept AdV.

6.5.1.1.2 Mitwirkungsverpflichtung im TI-ITSM gemäß [gemRL_Betr_TI]

Tab_KPT_Betr_TI_003 Mitwirkungsverpflichtung im TI-ITSM

Mitwirkung in den TI-ITSM-Prozessen:	INC	PRO	CHG	SKM	SLM	RF	Perf	CapM	KM	CSI	CM	NM
Anbieter Proof-of-Patient-Presence-Dienst	A/E	A/E	A/E	.	A/E	A	A	A	A/E	.	A/E	A/E

Legende:

INC: Incident Management

PRO: Problem Management

CHG: Change Management

SKM: Servicekatalog Management

SLM: Service Level Management

RF: Request Fulfillment

Perf: Perfomance Management

CapM: Capacity Management

KM: Knowledge Management

CSI: Continual Service Improvement

CM: Configuration Management

NF: Notfall Management

A: Auslöser in INC, PRO, CHG

Auslöser (A) ist, wer Incidents, Problems oder Changes eröffnet.

E: Empfänger von INC, PRO, CHG

Empfänger (E) ist wer Incidents, Problems oder Changes zugewiesen bekommt und dessen vollständige Mitarbeit gewährleistet ist.

Auslöser und Empfänger im SKM

Auslöser (A) ist, wer Änderungen im Service Katalog Management einbringt.

Empfänger (E) ist, wer Änderungen im Service Katalog Management aufnimmt.

Portalanbieter (P) ist, wer das TI-Service-Portal zur Verfügung stellt und selbst Nutzer ist.

A/E: Auslöser und Empfänger im SLM

Auslöser (A) ist, wer Änderungen im Servicelevel Management einbringt.

Empfänger (E) ist, wer im Servicelevel Management an Servicelevel-Reviews teilnimmt.

A/E: Auslöser und Empfänger im RF

Auslöser (A) ist, wer Services bei anderen Anbietern abruft.

Empfänger (E) ist, wer einen Servicekatalog führt und Services anbietet.

A/E: Auslöser und Empfänger im Perf

Auslöser (A) ist, wer Performancereports bzw. Rohdaten-Performance-Berichte sendet.

Empfänger (E) ist die gematik.

A/E: Auslöser und Empfänger im CapM

Auslöser (A) ist, wer Kapazitätspläne führt und reportet.
Empfänger (E) ist die gematik (GTI).

A/E: Auslöser und Empfänger im KM

Auslöser (A) ist, wer Artikel in der Wissensdatenbank einstellt.

Empfänger (E) ist, wer Artikel aus der Wissensdatenbank bezieht.

A/E: Auslöser und Empfänger im CSI

Auslöser (A) ist, wer ein CSI-Register führt und reportet.
Empfänger (E) ist die gematik (GTI).

A/E: Auslöser und Empfänger im CM

Auslöser (A) ist, wer Reports sendet, in denen die Konfigurationen der verwendeten Produkte dargestellt werden.

Empfänger (E) ist, wer Konfigurationsvorgaben und deren Umsetzung dar z.B. im Zuge eines CRs oder Changes empfängt und umsetzt.

A/E: Auslöser und Empfänger im NM

Aktiv (A) ist, wer im Notfall zuarbeiten und unterstützen muss.

Empfänger (E) stellen einen Notfall-Ansprechpartner bereit.

6.5.1.1.3 Spezifische Ausprägungen und Verpflichtungen einzelner Rollen

Tab_KPT_Betr_Betriebliche Rolle_Anbieterkonstellationen

Spezifische Ausprägung der Rolle	Zulässige Anbieterkonstellationen	Bemerkung
Anbieter Proof-of-Patient-Presence-Dienst	<I / II / III / IV>	

6.5.1.1.4 Anbieter Proof-of-Patient-Presence-Dienst

Für den Anbieter Proof-of-Patient-Presence-Dienst dienen die in [gemKPT_Betrieb#3.4.1.2.1] aufgeführten betrieblichen Konstellationen zur Orientierung – diese Optionen sind jedoch nicht abschließend. Der Anbieter kann entscheiden, in welcher Weise er den Betrieb organisiert. An dieser Stelle ist jedoch anzumerken, dass für die TI-ITSM-Prozesse nur ein einziger Dienstleister als TI-ITSM-Teilnehmer für den Anbieter im Zulassungsvertrag/Zulassungsbescheid eingetragen werden kann. Dieser erfüllt dann die in [gemKPT_Betrieb#3.4.1.2.1] aufgeführten Berechtigungen und Verpflichtungen für den Anbieter.

6.5.1.2 1.3 Supportkonzept

6.5.1.2.1 Spezifische Ausprägungen

Tab_KPT_Betr_TI_Anbieter_UHD/VHD

	UHD (Anwender)	VHD (Versicherte)
Anbieter Proof-of-Patient-Presence-Dienst	Mo - Fr 9:00 bis 20:00 *>	n.a.

* [außer an bundeseinheitlichen Feiertagen]

6.5.1.3 Organisatorische Service Level

Tabelle x: Tab_gemKPT_Betr_OrgSL_Serviceleistung_Zeiten

Serviceleistung	zu Haupt- und Nebenzeit (TIP1-A_7265)	zu Hauptzeit (A_13573)
Anbieter Proof-of-Patient-Presence-Dienst	x	

TIP1-A_7265-03 - Serviceleistung der TI-ITSM-Teilnehmer im TI-ITSM-Teilnehmersupport zur Haupt- und Nebenzeit

TI-ITSM-Teilnehmer mit Mitwirkungsverpflichtung zur Haupt- und Nebenzeit gemäß Tab_KPT_Betr_TI_002 Mitwirkungspflichten der TI-ITSM-Teilnehmer MÜSSEN die folgenden Service Level (Zeiten) einhalten:

Tabelle 17: Tab_KPT_Betr_TI_052 Service Level (Zeiten) im TI-ITSM

			PU			TU / RU			
			A	B	C	D	E	F	
	Prozess	Prio	Reaktionszeit in h	Lösungszeit/ Umsetzungszeit in h	Servicezeit (H,N)	Reaktionszeit in h	Lösungszeit/ Umsetzungszeit in h	Servicezeit	Erfüllungsgrad
1	INC	1	1	2	H+N	1	2	H	95%
2	INC	2	1	4	H+N	1	4	H	95%
3	INC	3	2	8	H	2	8	H	95%
4	INC	4	2	40	H	2	40	H	95%
5	PRO	1	4*	176	H	4*	176	H	95%
6	PRO	2		232	H		232	H	95%
7	PRO	3		400	H		400	H	95%
8	PRO	4		560	H		560	H	95%
9	CHG	Alle	40		H	40		H	100%
10	REP	Alle	-	40	H	-	40	H	100%
11	RF	Alle	8	**	H	8	**	H	90%
12	RCA	Alle	-	40	H	-	40	H	100%
	Verifikationsfrist:								
13	INC, PRO, CHG, RF**		168		H+N	168		H+N	100%

* Die Reaktionszeit gilt sowohl für die Rolle Incident/Problem - Verantwortlicher als auch Incident/Problem - Unterstützer.
H (Hauptzeit): Mo - Fr 09:00 - 17:00 im Rahmen eines Einschichtbetriebs [außer an bundeseinheitlichen Feiertagen].
N (Nebenzeit): Alle anderen Zeiten gelten als Nebenzeit.
** Abhängig vom im Business-Servicekatalog des TI-ITSM-Teilnehmers angebotenen konkreten Service**[<=]**

hinzufügen der Zuordnung zu Anbietertyp: Anbieter Proof-of-Patient-Presence-Dienst - org./betriebl. Eignung: Prozessprüfung

Sind SL nur der Hauptzeit (H) zugeordnet, so kann die Bearbeitung in der Nebenzeit unterbrochen werden und wieder in der Hauptzeit aufgenommen werden. Die Einhaltung dieses SL wird nur in der Hauptzeit gemessen.

6.5.1.4 Technische Service Level / Performance-Kenngrößen

6.5.1.4.1 Spezifische Ausprägungen

6.5.1.4.1.1 Proof-of-Patient-Presence-Dienst (PDT71)

Schnittstellen::Operation bzw. Anwendungsfall

<<PDT71-S01 ist reserviert für die Berechnung der rel. Verfügbarkeit und darf nicht für andere Performance-Kenngrößen verwendet werden.>>

Tab_gemKPT_Betr_Proof-of-Patient-Presence-Dienst_Operationen/Anwendungsfälle

Produkttyp / Anwen-dungstyp	S/A-ID	Schnittstellen::Operation / Anwendungsfall	Beschreibung	Berichtsformat-Alias (sofern von Schnittstellen::Operation bzw. Anwendungsfall abweichend)
PDT71	S01	I*		
PDT71	S02	I_PoPP_Service::createPoPPToken		

Performance-Kenngrößen / SL-Werte

Der Erfassungszeitraum für die aufgeführten Soll-Werte beträgt ein Kalendermonat.

Tab_gemKPT_Betr_Proof-of-Patient-Presence-Dienst_Performance-Kenngroessen

Performance-Kenngröße (PKG-ID)	Beschreibung	berechnet aus (Rohdaten-BDE, Probing)	SL-Wert (Soll-Wert)	min / max	Normative Referenz
Proof-of-Patient-Presence-Dienst - PDT71 - I*					
PDT71-S01-D3-G12	Relative Verfügbarkeit im Erfassungszeitraum exkl. Wartung. [%*1000]	Probing			
PDT71-S01-D3-G14	Relative Verfügbarkeit im Erfassungszeitraum zur Hauptzeit exkl. Wartung. [%*1000]	Probing			
PDT71-S01-D3-G16	Relative Verfügbarkeit im Erfassungszeitraum zur	Probing			

	Nebenzeit exkl. Wartung. [%*1000]				
Proof-of-Patient-Presence-Dienst - PDT71 - I_PoPP_Service::createPoPPToken					
PDT71-S02-D1-G01	Anzahl der Aufrufe im Erfassungszeitraum. [Stück]	Rohdaten-BDE			
PDT71-S02-D2-G08	Mittlere Bearbeitungszeit im Erfassungszeitraum. [msec]	Rohdaten-BDE			
PDT71-S02-D2-G30	Maximale Bearbeitungszeit im Erfassungszeitraum. [msec]	Rohdaten-BDE			
PDT71-S02-D2-G31	Anteil Bearbeitungen innerhalb der Bearbeitungszeitvorgabe im Erfassungszeitraum. [%]	Rohdaten-BDE			

6.5.2 gemKPT_Betr: Anhang A

2.1.1.1 Produkttypen (PDT-IDs)

<< Produkttypen sind fortlaufend. Die Texte für Spalte 2 und 3 sind identisch mit den Texten im entsprechenden Zulassungstyp (PET)>>

Tab_gemKPT_Betr_Produkttypen

ID	Produkttyp / Anwendungstyp	Produkttyp-Name / Anwendungsname
PDT71	gemProdT_PoPP_Dienst	Proof-of-Patient-Presence-Dienst

6.5.3 gemSpec_Perf#Rohdaten-Performance-Reporting

in [gemSpecPerf::Kapitel 2.5.2] Rohdaten-Performance-Reporting (Rohdatenerfassung v.02)

Tabelle : Tab_gemSpec_Perf_Produkte_Rohdatenerfassung_Version_v02

PDT	Produkttyp
PDT71	Proof-of-Patient-Presence-Dienst

Die Zuweisungen der Anforderungen zu dem Produkttypen Proof-of-Patient-Presence-Dienst sowie zu dem entsprechenden Anbietertypen werden wie folgt vorgenommen:

A_22057 - Performance - Rohdaten - Verpflichtung des Anbieters (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Anbietertyp: Anbieter Proof-of-Patient-Presence-Dienst - org./betriebl. Eignung: Prozessprüfung

A_22482 - Performance - Rohdaten - Erfassung von Rohdaten (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Test Produkt/FA

6.5.3.1 Umfang

A_22002 - Performance - Rohdaten - Übermittlung (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Test Produkt/FA

A_22000 - Performance - Rohdaten - zu liefernde Dateien (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Test Produkt/FA

A_22429 - Performance - Rohdaten - Inhalt der Selbstauskunft (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Test Produkt/FA

A_22004 - Performance - Rohdaten - Korrektheit (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Test Produkt/FA

A_22005 - Performance - Rohdaten - Frist für Nachlieferung (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Herstellererklärung

A_22003-01 - Performance - Rohdaten - Nachlieferung auf Anforderung (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Anbietertyp: Anbieter Proof-of-Patient-Presence-Dienst - org.-betr.: Anbietererklärung

A_22996 - Performance - Rohdaten - Zeitpunkte der Übermittlungen (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Anbietertyp: Anbieter Proof-of-Patient-Presence-Dienst - org.-betr.: Anbietererklärung

6.5.3.2 Lieferintervalle

A_21976 - Performance - Rohdaten - Konfigurierbarkeit der Lieferintervalle (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Test Produkt/FA

A_22047 - Performance - Rohdaten - Änderung der Konfiguration der Lieferintervalle (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Test Produkt/FA

A_22620 - Rohdaten - Umsetzungszeit für Änderung der Lieferintervalle

hinzufügen der Zuordnung zu Anbietertyp: Anbieter Proof-of-Patient-Presence-Dienst - org.-betr.: Anbietererklärung

A_21978 - Performance - Rohdaten - Trennung der Lieferintervalle (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Herstellererklärung

A_21975 - Performance - Rohdaten - Default-Werte für Lieferintervalle (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Test Produkt/FA

A_21979 - Performance - Rohdaten - Bezug der Lieferverpflichtung (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Herstellererklärung

A_21980 - Performance - Rohdaten - Leerlieferung (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Test Produkt/FA

6.5.3.3 Format

A_22001-01 - Performance - Rohdaten - Name der Berichte (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Test Produkt/FA

A_21981-02 - Performance - Rohdaten - Format des Rohdaten-Performance-Berichtes (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Test Produkt/FA

A_22500-01 - Performance - Rohdaten - Status-Block (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Test Produkt/FA

A_21982-01 - Performance - Rohdaten - Message-Block (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst - funkt. Eignung: Test Produkt/FA

A_22513-01 - Performance - Rohdaten - Message-Block im Fehlerfall - JSON (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst- funkt. Eignung: Test Produkt/FA

6.5.4 gemSpecPerf#3.x Proof-of-Patient-Presence-Dienst

Im Folgenden werden die spezifischen Leistungsanforderungen und Anforderungen an das Rohdaten-Performance-Berichtsformat des Proof-of-Patient-Presence-Dienstaufgeführt.

6.5.4.1 3.x.1 Leistungsanforderungen Proof-of-Patient-Presence-Dienst

6.5.4.1.1 3.x.1.3 Performancevorgaben Proof-of-Patient-Presence-Dienst

A_23418 - Performance - Proof-of-Patient-Presence-Dienst - Skalierung
Der Anbieter des Proof-of-Patient-Presence-Dienst MUSS nachvollziehbar darstellen, wie die Skalierung im Produktivbetrieb erreicht wird.**[<=]**

Im Zuge des Zulassungsverfahrens hat der Anbieter des Proof-of-Patient-Presence-Dienstes der gematik gegenüber nachvollziehbar darzustellen, welche technischen Skalierungsmaßnahmen anhand welcher messbarer Parameter er für den Produktivbetrieb plant durchzuführen. Die Skalierungsmaßnahmen können dabei unterschiedliche Ausprägungen und Dimensionen umfassen. Beispielsweise eine automatisierte Ressourcenzuteilung oder eine Anpassung oder Änderung unterschiedlicher technischer Komponenten, die zu einer Produktänderung im Sinne der [gemSpec_OM] führt. Die Darstellung muss Verifikationsbeschreibungen enthalten, mit denen der Erfolg der Maßnahmen ermittelt werden kann.

A_23419 - Performance - Proof-of-Patient-Presence-Dienst - Verfügbarkeit
Der Anbieter des Proof-of-Patient-Presence-Dienst MUSS zur Hauptzeit eine Verfügbarkeit von 99,99% und zur Nebenzeit von 99,97% für alle Operationen der technischen Schnittstellen aufweisen.

Wartungsfenster MÜSSEN vollständig in der Nebenzeit liegen. Genehmigte Wartungsfenster werden nicht als Ausfallzeit gewertet.

Hauptzeit ist Montag bis Freitag von 6 bis 22 Uhr sowie Samstag und Sonntag von 6 bis 20 Uhr. Alle übrigen Stunden der Woche sind Nebenzeit. Bundeseinheitliche Feiertage werden wie Sonntage behandelt, alle übrigen Feiertage wie Werktage.

Die Anschlüsse aller Standorte an das zentrale Netz MÜSSEN über die Anschlussoption "Hohe Verfügbarkeit" erfolgen.
[<=]

Die Verfügbarkeit der funktionalen Eigenschaften des Proof-of-Patient-Presence-Dienstes wird mittels der Probes des Service Monitorings und die nicht funktionalen Eigenschaften durch Auswertung der Rohdaten ermittelt.

6.5.4.2 3.x.2 Rohdaten-Performance-Reporting Spezifika Proof-of-Patient-Presence-Dienst

In Ergänzung an die allgemeinen Anforderungen an das Performance-Rohdaten-Reporting befinden sich nachfolgend die produktspezifischen Anforderungen.

6.5.4.2.1 3.x.2.2 Format

A_23414 - Performance - Rohdaten - Proof-of-Patient-Presence-Dienst - Duration (Rohdatenerfassung v.02)

Der Produkttyp Proof-of-Patient-Presence-Dienst MUSS bei Rohdaten-Performance-Berichten bzgl. der "duration_in_ms"-Felder die Hinweise der Spalte "Duration" aus Tabelle Tab_gemSpec_Perf_Berichtsformat_Proof-of-Patient-Presence-Dienst berücksichtigen.**[<=]**

Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst- Prüfverfahren funkt. Eignung: Test Produkt/FA

A_23415 - Performance - Rohdaten - Proof-of-Patient-Presence-Dienst - Operation (Rohdatenerfassung v.02)
Der Produkttyp Proof-of-Patient-Presence-Dienst MUSS bei Rohdaten-Performance-Berichten bzgl. der "operation"-Felder die Angabe der Spalte "Operation/Usecase" aus Tabelle Tab_gemSpec_Perf_Berichtsformat_Proof-of-Patient-Presence-Dienst berücksichtigen.
[<=]

Zuordnung zu Produkttyp: Proof-of-Patient-Presence-Dienst- Prüfverfahren funkt. Eignung: Test Produkt/FA

Tabelle : Tab_gemSpec_Perf_Berichtsformat_Proof-of-Patient-Presence-Dienst

Operation / Usecase	Duration
I_PoPP_Service::createPoPPToken	Bei Aufruf der Operation beginnt die Messung mit Annahme der Aufrufnachricht an der Außenschnittstelle des Produkttyps und endet mit dem vollständigen Versenden der Antwortnachricht.

6.6 Test

7 Informationen für nutzenden Fachdienst

Ein nutzender Fachdienst nimmt vom Primärsystem den PoPP-Nachweis zusammen mit dem vom Konnektor erzeugten (De-)Pseudonymisierungsschlüssel entgegen (vgl. Rückgabewerte von PerformPoPP in Abschnitt "5.2.3- Rückgabe an Clientsystem ").

Der nutzende FD bewertet vor der Weiterverwertung die Integrität, Gültigkeit und hinreichende Aktualität des PoPP-Nachweises. Die Plausibilität ist gegeben, wenn die Telematik-ID im PoPP-Token mit dem Accesstoken der Anfrage übereinstimmt.

Für die Prüfungen entschlüsselt der nutzende Fachdienst die "enc_egk_data" und erhält damit folgende JSON-Datenstruktur:

```
{
      "egk_aut": "<eGK AUT>",
      "egk_aut_status": "CERT_GOOD",
      "egk_signature": "<Base64-kodierte Signatur>",
      "egk_cvc": "<Base64-kodiertes CVC EE>",
      "egk_cvc_ca": "<Base64-kodiertes CVC CA>"
 }
```

Ist der "egk_aut_status" auf einem anderen Zustand als "CERT_GOOD", so ist die dem Anwendungsfall entsprechenden Fachlogik anzustoßen. Diese kann eine Nachprüfung oder einen Negativfall des entsprechenden Anwendungsfalls implizieren.

Schlussendlich kann der nutzende FD aus dem eGK-AUT-Zertifikat die für den Anwendungsfall notwendigen personenbezogenen Daten entnehmen, um den Anwendungsfall im entsprechenden Kontext durchführen zu können.

8 Anpassungen an gemSpec_OID

8.1 Änderung in Kapitel 3.5.4 „OID-Vergabe für technische Rollen"

GS-A_4446-09 - OID-Festlegung für technische Rollen
Ein TSP-X.509 MUSS die technischen Rollen für die Nutzung in X.509-Zertifikaten der TI mit OIDs entsprechend der Tabelle Tab_PKI_406-05 referenzieren.

Tabelle 18 Tab_PKI_406-05 OID-Festlegung technische Rolle in X.509-Zertifikaten

OID-Referenz in anderen Dokumenten	ProfessionItem (Beschreibung der technischen Rolle)	ProfessionOID (OID der technischen Rolle)	Zertifikatsprofil(e) in denen die ProfessionOID im Element Admission vorkommen darf
(...)			
oid_popp	Proof of Patient Presence (PoPP) Dienst	1.2.276.0.76.4.293	C.ZD.TLS-S C.ZD.SIG

9 Dokumentenhaushalt

<optional: Auswirkungen auf den Dokumentenhaushalt>

9.1 Neue Dokumente

<Optional: Eine Übersicht betroffener Dokumente mit kurzer Charakterisierung, z.B. Inhalt, etc.>

9.2 Übersicht betroffener Dokumente

<Optional: Eine Übersicht betroffener Dokumente,z. B. Spezifikationen, Konzepte, SystemDesign etc.>

9.3 Übersicht Produkt- und Anbietertypen

<Optional: Eine Übersicht neuer / betroffener Produkt und Anbietertypen>

10 Beispiele und Referenzimplementierungen

<Optional: Beispiele für Aufrufsequenzen, ausgetauschte Daten, etc. zur Unterstützung der Implementierung>

11 Anhang A – Verzeichnisse

11.1 Abkürzungen

Kürzel	Erläuterung
PoPP	Proof of Patient Presence

11.2 Referenzierte Dokumente

11.2.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	**Herausgeber: Titel**
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur

11.2.2 Weitere Dokumente

[Quelle]	**Herausgeber (Erscheinungsdatum): Titel**

[RFC-4493]	RFC 4493 (June 2006): The AES-CMAC Algorithm https://www.rfc-editor.org/rfc/rfc4493.html
[RFC-6763]	IETF RFC6763 (Februar 2013) DNS-Based Service Discovery https://www.rfc-editor.org/rfc/rfc6763.html
[RFC-7515]	RFC 7515 (Mai 2015): JSON Web Signature (JWS) https://www.rfc-editor.org/rfc/rfc7515.html
[RFC-7519]	RFC 7519 (Mai 2015): JSON Web Token (JWT) https://www.rfc-editor.org/rfc/rfc7519.html