Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste

ENTWURF

Version:	1.1.0~~.0~~ CC
Revision:	~~241924~~269880
Stand:	~~30.06~~17.08.2020
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_IDP_FD

Dokumentinformationen

Änderungen zur Vorversion

~~Es handelt sich um die Erstversion~~Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	30.06.20		initiale Erstellung des Dokuments	gematik
1.1.0 CC	17.08.20		Einarbeitung Scope-Themen zu R4.0.1 zur Abstimmung freigegeben	gematik

ENTWURF

Inhaltsverzeichnis

ENTWURF

ENTWURF

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb ~~des Produkttyps gemSpec_IDP_FD~~der Schnittstellen von Fachdiensten, die den Identity Provider-Dienst (IdP-Dienst) nutzen wollen.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von Fachdiensten und Fachanwendungen, welche die Funktion des ~~Identitäts-Prüfungs-Dienst (~~IdP-Dienst~~)~~ nutzen wollen.

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. Dokumentenlandkarte, 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 diesem Dokument die von dem Produkttyp IdP-Dienst bereitgestellten ~~(angebotenen)~~ Schnittstellen sowie die Bedingungen, unter denen diese zu nutzen sind. Weitere Details zu den benutzten Schnittstellen werden in der Spezifikation des IdP-Dienstes beschrieben. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang ~~9~~8).

ENTWURF

Die vollständige Anforderungslage für den Produkttyp IdP-Dienst ergibt sich aus den weiteren Konzept- und Spezifikationsdokumenten; diese sind in dem Produkttypsteckbrief des Produkttyps IdP-Dienst verzeichnet.

~~Die vollständige Anforderungslage für den Produkttyp, welcher den Identitäts-Prüfungs-Dienst nutzt, ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten; diese sind in dem Produkttypsteckbrief des jeweiligen Produkttyps (IdP-Dienst bzw. IdP-Frontend) verzeichnet.~~

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen und Anforderungen, welche sich an den IdP-Dienst selbst richten.

1.5 Methodik

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

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

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

Hinweis auf offene Punkte

Offene Punkten werden im Dokument in dieser Darstellung ausgewiesen.

ENTWURF

2 Systemüberblick

~~*Im aktuellen Stand des Dokumentes fehlen noch in Diskussion befindliche, Festlegungen zur Erweiterung des Integritätsschutzes des Discovery Documents sowie weiterer verwendeter Schlüssel. Die Standards sehen Verschlüsselungen vor, aber lassen die Methoden des Schlüsselaustausch offen und die gematik ist noch in Abstimmung zu praktikablen Methoden.*~~

~~*Im aktuellen Stand des Dokumentes fehlen an einigen Punkten noch Verweise auf die zugrundeliegenden Operationen der Standards OpenID Connect und OAuth2.*~~

In der Telematikinfrastruktur (TI) werden zahlreiche Fachdienste angeboten. ~~Um es den Anbietern von~~ Anwendungsfrontends können über die Authentifizierung des Nutzers am IdP-Dienst Zugriff zu den von den Fachdiensten ~~(Service Provider) zu ermöglichen, den Aufwand für die Kontrolle der Zugriffsberechtigung auf ein Minimum zu beschränken, bietet die TI einen Identitäts-Prüfungs-Dienst (IdP-Dienst) an.~~ angebotenen Daten erhalten. Der IdP-Dienst stellt durch gesicherte JSON Web Token (JWT) attestierte Identitäten aus ~~und ist Garant dafür, dass deren aktuelle Gültigkeit gegeben ist.~~ Gegen Vorlage eines "ACCESS_TOKEN" erhalten Anwendungsfrontends, entsprechend der im Token attestierten professionOID, Zugriff auf die Inhalte der Fachdienste.

~~Aufgabe des IdP-Dienstes ist es, die von verschiedenen Entitäten vorgetragenen Attribute auf Zugehörigkeit zur TI ebenso wie auf aktuelle Gültigkeit und Integrität zu prüfen.~~

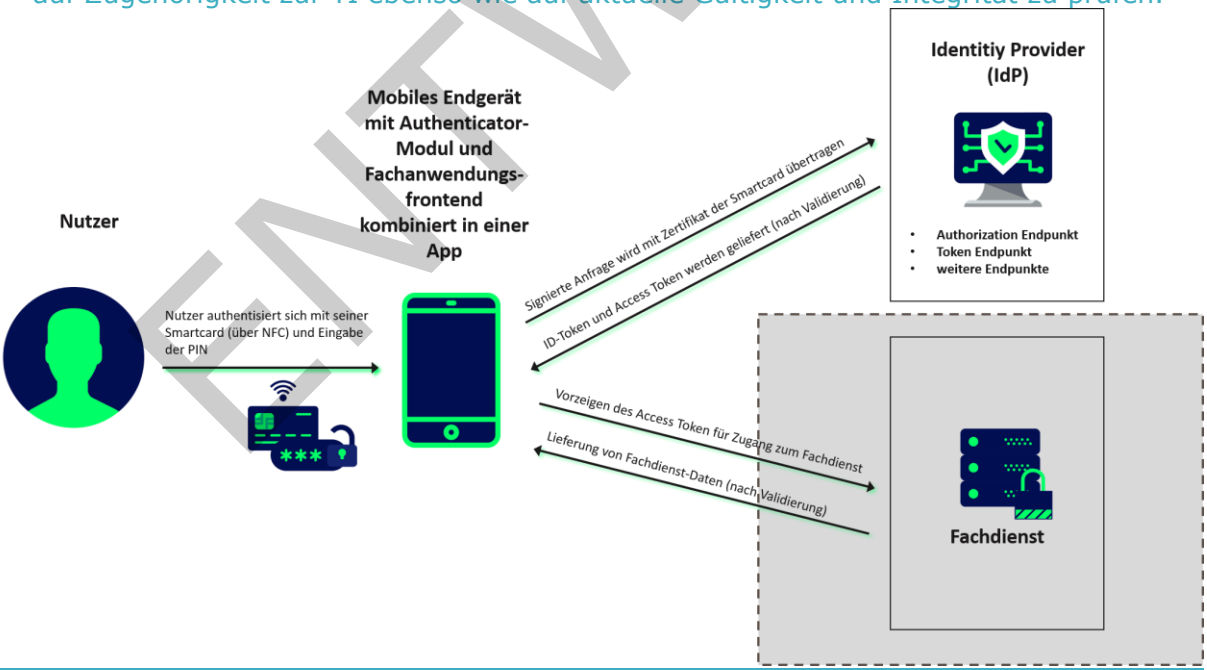


Abbildung 1: Systemüberblick (vereinfacht)

ENTWURF

Die Abbildung stellt den Systemüberblick dar. Der Authentifizierungsprozess, welcher mit der Ausstellung und Übergabe der Token an das Anwendungsfrontend endet, wird dabei zur besseren Übersicht vereinfacht dargestellt.

Der IdP-Dienst übernimmt für den Fachdienst die Aufgabe der Identifikation des Nutzers. ~~Zudem bestätigt~~ Der IdP-Dienst fasst die ~~Rolle des Nutzers anhand dessen~~ professionOID sowie ~~weiteren~~weitere für den Fachdienst ~~notwendigen Attributen und fasst diese in einem~~notwendige Attribute in signierten JSON Web Token ("`ID_TOKEN`", "`ACCESS_-`" und "`SSO_TOKEN`") zusammen. Fachdienste müssen ~~somit~~ keine ~~aufwendige~~ Überprüfung des Nutzers selbst implementieren, sondern können sich darauf verlassen, dass der Besitzer des bei ihnen ~~eingereichten "ID~~vorgetragenen "`ACCESS_TOKEN`" bereits ~~sicher~~ identifiziert wurde~~, und dass dessen~~. Des Weiteren stellt der IdP-Dienst sicher, dass die vom Nutzer vorgetragenen Attribute ~~aktuell~~(aus dem Signaturzertifikat) gültig sind.

Der IdP-Dienst prüft ~~hierbei~~, ob das vorgetragene X.509-nonQES-Signatur-Zertifikat der verwendeten Prozessor-Chipkarte (eGK, HBA oder ~~eHBA sowie ggf.~~ SMC-B) für die vorgesehene Laufzeit des Tokens zeitlich gültig ~~ist,~~und ob dessen Integrität sichergestellt ~~ist und ob andere Gründe (z.B. Widerruf, Sperrung) vorliegen, welche eine Token-Herausgabe verhindern~~ ist.

Der IdP-Dienst ~~wird~~stellt nur solche "`~~ID~~ACCESS_TOKEN`" ~~ausstellen~~aus, welche auf gültigen AUT-Zertifikaten (d.h. C.CH.AUT, C.HP.AUT oder C.HCI.AUT) basieren~~, und wird nur Attribute bestätigen, welche im vorgetragenen Zertifikat enthalten sind~~.

Fachdienste, welche den IdP-Dienst nutzen, müssen die folgenden Prozesse und Schnittstellen bedienen:

- Registrierung des Fachdienstes beim IdP-Dienst (organisatorischer Prozess gemäß Abschnitt 4)
- Abstimmen ~~des~~der Claims (Key/Value-Paare im Payload eines JSON Web Token) mit dem IdP-Dienst (organisatorischer Prozess gemäß Abschnitt 4.1)
- ~~Token Introspection (siehe Abschnitt 6. Token Introspection)~~
- Abstimmen der Rahmenbedingungen für die Gültigkeit von "`~~ID~~ACCESS_TOKEN`" (siehe Abschnitt ~~8~~7)

Alle Fachdienste müssen zur Absicherung der JSON Web Token gegen Einsichtnahme durch Dritte den Transportweg ~~zusätzlich~~ mit Transport Layer Security (TLS) gemäß [gemSpec_Krypt] absichern. ~~Dies ist erforderlich, da es sich um im höchsten Maße schützenswerte Daten handelt und der Datenverkehr auf Proxy-Servern ansonsten unverschlüsselt vorliegen würde. Die Absicherung mit TLS Transportweg-Sicherung erfolgt auf Seiten des Dienstanbieters.~~ Der Fachdienst muss ~~daher~~ sowohl im Internet, als auch innerhalb der TI über ~~ein entsprechend innerhalb der Domäne, in der sich der jeweilige Nutzer bewegt, ohne weitere Umstände~~ ein überprüfbares TLS-Serverzertifikat verfügen. Innerhalb der TI werden Fachdienste mit TLS-~~Serverzertifikaten~~Zertifikaten durch die Komponenten-Public Key Infrastructure (PKI) ausgestattet~~, welche in der gesamten Zertifikatskette bis zur Root-CA geprüft werden können.~~. Im Internet müssen die Fachdienste durch ein öffentlich prüfbares Serverzertifikat gesichert werden.

Fachdienste sind ebenfalls Nutzer des IdP-Dienstes ~~und~~als Resource Server und sind bei diesem organisatorisch als Open Authorization 2.0 (OAuth 2.0) Client registriert. Sie verwenden die vom IdP-Dienst ausgegebenen "`~~ID~~ACCESS_TOKEN`", um Nutzern Zugriff auf die von ihnen bereitgestellten geschützten Ressourcen, die Fachdaten, zu gewähren.

ENTWURF

3 Systemkontext

Der Systemkontext besteht für den Fachdienst aus dem Identity Provider und dem Anwendungsfrontend.

Der Fachdienst muss beim Identity Provider eine organisatorische Registrierung durchführen, bei der die vom Fachdienst erwarteten Werte, welche ein "ACCESS_TOKEN" für einen Zugriff auf die Fachdaten des Fachdienstes enthalten muss, hinterlegt werden.

Das Anwendungsfrontend erlangt nach Vorlage des "ACCESS_TOKEN" und positiver Validierung der Inhalte des Tokens durch den Fachdienst Zugang zu den angeforderten Fachdaten.

Die folgende Abbildung stellt den Systemkontext aus Sicht eines Fachdienstes dar. Eine Kommunikationsbeziehung besteht nur mit dem Identity Provider und dem Anwendungsfrontend.

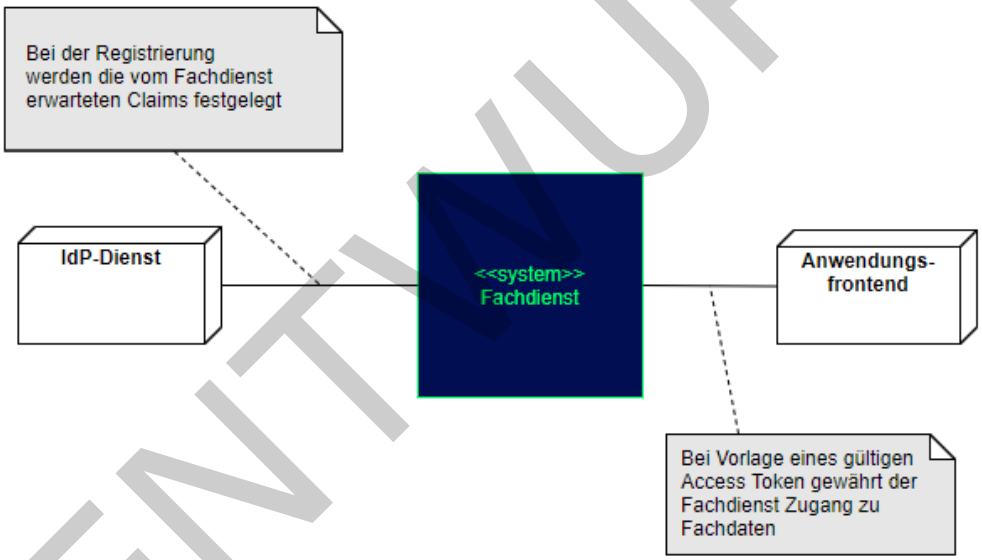


Abbildung 2: Systemkontext aus Sicht des Fachdienstes

3.1 Akteure und Rollen

~~Die Beschreibung der einzelnen Akteure und Rollen ist im Dokument [gemSpec_IDP_Dienst] enthalten.~~

Im Systemkontext des Fachdienstes interagieren verschiedene Akteure (Nutzer und aktive Komponenten) in unterschiedlichen OAuth2-Rollen gemäß [RFC6749 # section-1.1].

ENTWURF

Tabelle 1: TAB_IDP_FD_0001 Akteure und OAuth2-Rollen

Akteur	OAuth2-Rolle
Nutzer	Resource Owner
Fachdienst	Resource Server
Anwendungsfrontend	Teil des Clients
Authenticator-Modul	Teil des Clients
IdP-Dienst	Authorization Server
Fachdaten	Protected Resource

Nutzer (Rolle: Resource Owner)

Der Resource Owner ist der Nutzer, welcher auf die beim Fachdienst (Resource Server) für ihn bereitgestellten Daten (Protected Resource) zugreift.

Der Resource Owner verfügt über die folgenden Komponenten:

- Endgerät des Nutzers
- Authenticator-Modul
- Anwendungsfrontend

Fachdienst (Rolle: Resource Server)

Der Resource Server ist der Fachdienst, der dem Nutzer (Resource Owner) Zugriff auf seine Fachdaten (Protected Resource) gewährt. Der Fachdienst, der die geschützten Fachdaten (Protected Resources) anbietet, ist in der Lage, auf Basis von `"ACCESS_TOKEN"` Zugriff für Clients zu gewähren. Ein solches Token repräsentiert die delegierte Identifikation des Resource Owners.

Anwendungsfrontend/Authenticator-Modul kombiniert in einer Applikation (Rolle: Client)

Der Client greift mit dem Authenticator-Modul und dem Anwendungsfrontend (OIDC Relying Party bzw. OAuth2 Client) auf Fachdienste (Resource Server) und ihre geschützten Fachdaten (Protected Resource) zu. Das Anwendungsfrontend kann auf einem Server als Webanwendung (Primärsystem als Terminalserver), auf einem Desktop-PC oder einem mobilen Gerät (z.B. Smartphone) ausgeführt werden.

IdP-Dienst (Rolle: Authorization Server)

Der Authorization Server authentifiziert den Resource Owner (Nutzer) und stellt `"ID_TOKEN"`, `"ACCESS_TOKEN"` und `"SSO_TOKEN"` für den vom Resource Owner erlaubten Anwendungsbereich (SCOPE) aus, welche dieser wiederum beim Fachdienst einreicht.

ENTWURF

Tabelle 2: TAB_IDP_FD_0002 Kurzbezeichnung der Schnisttstellen des IdP-Dienstes

Kurzzeichen	Schnittstelle
AUTH	Authorization-Endpunkt
TOKEN	Token-Endpunkt
REDIR	Redirection-Endpunkt
DD	Discovery Document-Endpunkt

Weitere Akteure im Kontext IdP-Dienst sind:

Fachdaten (Rolle: Protected Resource)

Die geschützten Fachdaten, welche vom Fachdienst (Resource Server) angeboten werden.

3.2 Nachbarsysteme

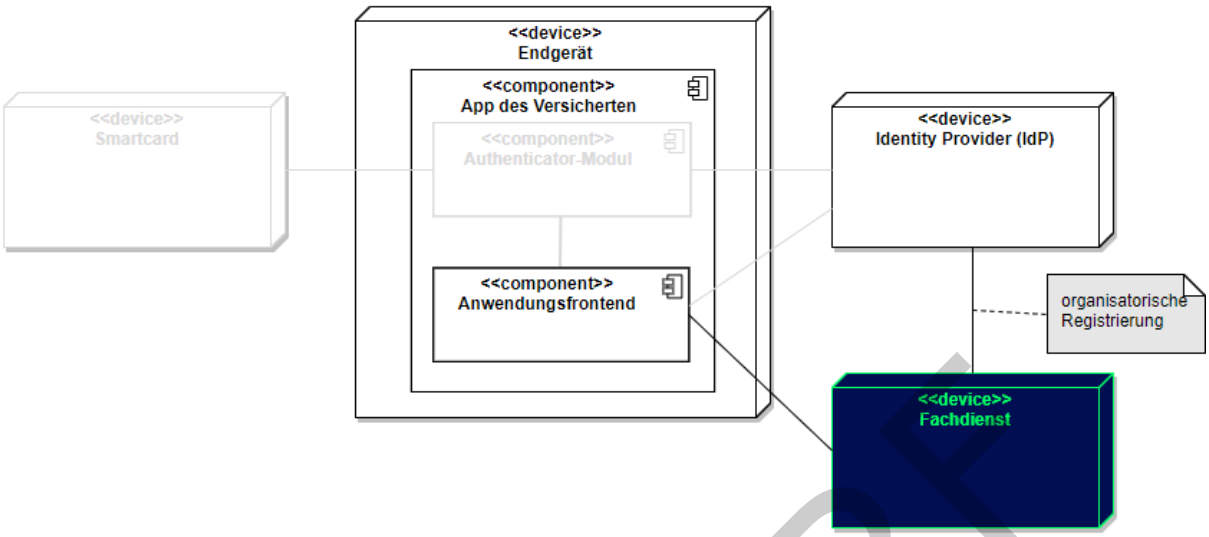
~~Aus Sicht des Fachdienstes sind die Nachbarsysteme primär das Endgerät des Nutzers, da dieser neben dem Anmeldeprozess auch die angebotenen Fachdienste nutzen möchte. Als weiteres Nachbarsystem ist der IdP-Dienst mit der Schnittstelle für Token Introspection zu sehen. Dieser bietet dem Fachdienstbetreiber zudem die Möglichkeit, die Subject Session eines Nutzers in Frage zu stellen, sodass diese beendet wird.~~

Die vom Fachdienst angebotene Schnittstelle, um Fachdaten zu erhalten, wird vom Anwendungsfrontend, welches auf dem Endgerät des Nutzers installiert ist, genutzt. Nutzer wollen über das Anwendungsfrontend Daten vom Fachdienst zur Anzeige, Änderung etc. erhalten. Die Identifikation des Nutzers wird anhand einer Smartcard und der Auswertung des vom Authenticator-Modul an den IdP-Dienst übergebenen Authentifizierungszertifikats (aus der Smartcard) sichergestellt.

Fachdienste registrieren sich über einen organisatorischen Prozess beim IdP-Dienst.

In der nächsten Abbildung werden die Systeme, welche keine direkten Kommunikationsbeziehungen mit Fachdiensten unterhalten, grau angedeutet:

ENTWURF



289

290 **Abbildung 3: Nachbarsysteme des Fachdienstes**

ENTWURF

4 Registrierung des Fachdienstes beim IdP-Dienst

~~Fachdienste MÜSSEN sich beim IdP-Dienst registrieren,~~Fachdienste müssen sich beim IdP-Dienst registrieren. Die Registrierung erfolgt als organisatorischer Prozess, bevor ein Fachdienst am vom IdP-Dienst angebotenen Authentifizierungsprozess teilnehmen kann. Erst nach erfolgter Registrierung, bei der die Adresse des Fachdienstes, sein öffentlicher Schlüssel und die von ihm erwarteten Attribute, in Form von Claims, angegeben wurden, kann der IdP-Dienst "ACCESS_TOKEN" für den Zugriff zum Fachdienst ausstellen.

A_20295~~A_19748~~ - Adressen des Dienstes werden registriert
Der ~~Fachdienst~~ Anbieter des Fachdienstes MUSS, um ~~seine~~die Erreichbarkeit des Fachdienstes zu gewährleisten, entsprechende Adressen ~~und die damit verbundenen URI bei der gematik~~im TI-Namensraum beantragen. In Fällen, in denen der Fachdienst ebenfalls aus dem Internet erreichbar sein soll, MUSS der ~~Fachdienst~~ Anbieter des Fachdienstes neben der TI-internen auch die notwendigen öffentlichen Adressen bei einem Internet Service Provider (ISP) seiner Wahl beantragen.**~~[<=]~~**

Hinweis:
Die Beantragung beinhaltet neben einer sprechenden Fachdienstbezeichnung eine statische IP-Adresse, auf deren Basis die URI adressiert wird. Die URI des Fachdienstes "URI_FD" muss ~~durch den~~ dem Authorization Server ~~im Discovery Document veröffentlicht~~, welcher Teil des IdP-Dienstes ist, bekanntgegeben werden.**~~[<=]~~**

A_20296~~A_19749~~ - Adressen des Schlüsselmaterials werden registriert
Fachdienste MÜSSEN die URI "URI_PUK_FD" des von ihnen verwendeten öffentlichen Schlüssels "PUK_FD" beim IdP-Dienst registrieren lassen, damit der IdP-Dienst die "~~ID~~ACCESS_TOKEN" zielgerichtet für den entsprechenden Fachdienst verschlüsseln kann.**[<=]**

~~Da ein Nutzer eine Session nur wenige Sekunden vor Ablauf der Gültigkeit des aktuell verwendeten Schlüssels einen längere Zeit andauernden Prozess initiieren kann, muss die Gültigkeit des serverseitig verwendeten Schlüssels die doppelte Lebensdauer aufweisen wie die des Nutzers. Nur so ist gewährleistet, dass der Nutzer in jedem Fall die ihm möglicherweise durch einen Fachdienst zugesicherte Verbindungsdauer~~
A_20739 - Registrierung der Claims des Fachdienstes
Anbieter von Fachdiensten ~~24 Stunden ohne Schlüsselwechsel erreichen kann.~~

~~A_20002 - Gültigkeitsdauer von Schlüsselmaterial und weicher Schlüsselwechsel~~
~~Der Fachdienst MUSS sein Schlüsselmaterial im Rhythmus von 24 Stunden roulierend erneuern. Der Fachdienst MUSS zwei Schlüsselgenerationen vorhalten. Das heißt, der Fachdienst MUSS den gerade ersetzten Schlüssel nach dessen Austausch weitere 24 Stunden bedienen. Es ergibt sich ein Lebenszyklus von 48 (2 x 24) Stunden. Diese Vorgabe entspricht den Anforderungen der gematik und ist nicht Bestandteil des Standards.~~**~~[<=]~~**

ENTWURF

~~Der IdP-Dienst bietet die URIs zu den registrierten Adressen des Fachdienstes sowie den öffentlichen Schlüsseln im Discovery Document gemäß [RFC8414] bzw. [OIDC Discovery] an (siehe auch gemSpec_IDP_Dienst#Übergreifende Festlegungen).~~

~~**A_20003 - Registrierung der Claims des Fachdienstes**~~
~~Fachdienste~~ MÜSSEN bei der Registrierung ihrer Fachdienste am IdP-Dienst die von ihnen erwarteten Attribute in einem Claim (siehe Anschnitt 4.1- Inhalte des Claims) beschreiben und dem IdP-Dienst zur Verfügung stellen. Die Registrierung MUSS ebenso die absoluten URI des Fachdienstes in der TI sowie im Internet – wenn der Fachdienst auch im Internet erreichbar sein muss – umfassen.**[<=]**

Hinweis: Als Claims werden Key/Value-Paare im Payload eines JWT bezeichnet. Ein vereinbarter Claim sagt aus, welche Key/Value-Paare im Payload erwartet werden. Die Vereinbarung wird zwischen dem Fachdienst und dem IdP-Dienst während der Registrierung des Fachdienstes getroffen. Anwendungsfrontends, welche Zugang zum Fachdienst erhalten wollen, müssen die geforderten Claims liefern.

4.1 Inhalte des Claims

Der Payload eines JSON Web Tokens beinhaltet Key/Value-Paare, welche als Claims bezeichnet werden. Inhalte eines Claims sind ~~diese~~die Attribute, welche der IdP-Dienst auf Basis der vorgetragenen Identität aus deren Signaturzertifikat extrahieren kann. Als Basis kommen eGK [gemSpec_PKI # Abschnitt 5.1.3.1 Authentisierung eGK] und HBA [gemSpec_PKI # Abschnitt 5.2.1 Authentisierung HBA] bzw. ~~für die~~ SMC-B [gemSpec_PKI # 5.3 Ausweis einer Organisation/Einrichtung des Gesundheitswesens] in Frage. Davon abgesehen könnten zukünftig auch Identitäten, welche in einem eigenen oder externen Identity Management gehalten werden, vom IdP-Dienst bestätigt werden.

~~Der IdP-Dienst benötigt im Claim die Informationen, welche Attribute vom Fachdienst im "ID_TOKEN" erwartet werden, damit dieser für die von Fachdiensten angebotenen Dienste ein im jeweiligen Claim des Fachdienstes beschriebenes "ID_TOKEN" ausstellen kann. Das Claim beschreibt~~Die Claims beinhalten die für diesen Fachdienst ~~(das Claim wird~~abgestimmten Attribute (die Claims werden pro Fachdienst in einem organisatorischen Prozess gesondert vom jeweiligen Fachdienst mit dem IdP-Dienst abgestimmt) ~~abgestimmten Attribute~~ und den Wertebereich, welchen diese annehmen können.

Neben den im Standard vorgesehenen Attributen (siehe openid-connect-core-1_0.html#IDToken) erwarten Fachdienste weitere Attribute, welche vom Standard nicht bereitgestellt werden.

Im Falle des E-Rezept-Dienstes sind dies z. B.:

Für Versicherte (eGK):

- Rolle des Nutzers (oid_Versicherter, siehe [gemSpec_OID # Tab_PKI_402])
- ID des Nutzers (KVNR)
- Vorname und Nachname der Person

Für Leistungserbringer (SMC-B LEI):

ENTWURF

- Rolle des Nutzers (OID-Festlegung Institutionen, siehe [gemSpec_OID #Tab_PKI_403])
- ID des Nutzers (Telematik-ID)
- Bezeichnung der Organisation

~~Das Attribut "iss" beschreibt, für welche Schnittstelle das später auf Basis des Claims ausgestellte "ID_TOKEN" verwendet werden kann. Gemeinhin ist das die für den Fachdienst registrierte URL, wobei in externe (URL's für die Erreichbarkeit aus dem Internet) und interne (URL's für die Erreichbarkeit innerhalb der TI) URL unterschieden werden muss.~~

Das Attribut "iss" beschreibt, wer den "ACCESS_TOKEN" ausgestellt hat.

Das Attribut "sub" beschreibt das Subjekt, mit welchem der Fachdienst kommuniziert. Anhand dieses Attributes lassen sich Vorgänge einer bestimmen Entität zuordnen. ~~Die Zuordnung erfolgt in Verbindung mit der professionOID der agierenden Entität.~~

Das Attribut "professionOID" beschreibt die Rolle der agierenden Entität und ist im Falle eines Versicherten immer mit der OID eines Versicherten "oid_Versicherter" befüllt. Im Falle eines Leistungserbringers oder einer Leistungserbringerinstitution wird hier die sektorspezifische professionOID gemäß [gemSpec_OID # Tab_PKI_402] bzw.[gemSpec_OID # Tab_PKI_403] eingesetzt.

A_20676 - Nutzer-Informationen im Claim
~~**A_19750 - Keine Verwendung des Attributes "aud"**~~
~~Das Attribut "aud" (Audience) gemäß[rfc7519 # section-4.1.3] DARF in Claims NICHT verwendet werden.~~**[<=]**

Fachdienste MÜSSEN die im Claim benötigten, anforderbaren Informationen über den Nutzer bei ihrer Registrierung beim IdP-Dienst angeben.**[<=]**

A_20297~~A_19751~~ - Inhalte des Claims für Versicherte (eGK)
~~Der~~Fachdienste MÜSSEN bei ihrer Registrierung am IdP-Dienst ~~MUSS~~ sicherstellen, dass ~~die~~ für Versicherte mit einer eGK als Nutzer die folgenden Attribute ~~im Claim immer gesetzt~~als Claims beantragt sind~~:~~ - Standardclaims sind mit "public", eigene Claims mit "private" gekennzeichnet:

Tabelle 3 TAB_IDP_FD_0003 Inhalte des Claims für Versicherte (eGK)

Attribut	Inhalt
"iss" (public)	~~Beinhaltet die URL des Fachdienstes als HTTPs Adresse mit Pfad und Angabe des Ports, wenn dieser vom Standard abweicht. In jedem Fall dürfen keine zusätzlichen Parameter enthalten sein.~~Beinhaltet die URL des IdP-Dienstes
"sub" (public)	~~Beinhaltet die KVNR des Versicherten, welche aus dem nonQES-Signaturzertifikat auszulesen ist.~~Beinhaltet einen verschlüsselten Identifikator, der sich aus der "client_id" und dem Host-Teil der "redirect_uri" des Anwendungsfrontends zusammensetzt. Dieser zusammengesetzte Wert wird mit dem privaten Schlüssel des Authorization Servers

ENTWURF

	"PrK_SUBJECT_ENC" nach der pairwise-Methode [openid-connect-core-1_0 # PairwiseAlg] vom IdP-Dienst verschlüsselt.
"nonce" (public)	Beinhaltet einen Zufallswert, welchen der IdP-Dienst nach den Vorgaben des ~~AnwendungsfrontendAnwendungsfrontends~~ befüllt und anhand dessen das Anwendungsfrontend seine Vorgänge unterscheiden kann.
"acr" (public)	Authentication Context Class Reference gemäß ~~[~~[openid-connect-core-1_0 # IDToken]
"aud" (public)	Hier sind gemäß [RFC7519 # section-4.1.3] entweder die URI des Fachdienstes oder ein entsprechender eindeutiger String eingetragen, die bzw. der den Fachdienst identifiziert.
"professionOID" (private)	Beinhaltet die professionOID des Versicherten gemäß [gemSpec_OID#Tab_PKI_402].
"given_name" (public)	Vorname ~~Nachname~~ des Versicherten – der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus.
"family_name" (public)	Nachname des Versicherten – der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus.
"organizationName" (private)	Herausgeber - der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus.
"idNummer" (private)	Beinhaltet die KVNR des Versicherten – der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus.
"jti"	ID des Token

[<=]

Hinweise:

- Die Befüllung des Claims erfolgt grundsätzlich gemäß [rfc7519 # section-4]
- Beispiel-Wert des Attributes `"iss": "https://erp.telematik/pfad/login"`
- Das Attribut `"iss"` wird durch den IdP-Dienst befüllt.
- Das Attribut "~~sub~~aud" enthält die eindeutige URI des Fachdienstes oder einen beim IdP-Dienst ausschließlich diesem Fachdienst zugesprochenen Wert z. B. "E-Rezept" oder "eRp".
- Das Attribut "professionOID" des Versicherten wird durch den IdP-Dienst befüllt.
- Das Attribut "idNummer" wird mit den Informationen aus dem Signaturzertifikat durch den IdP-Dienst befüllt.
- ~~Das Attribut "professionOID" des Leistungserbringers wird durch den IdP-Dienst befüllt. Andere als die in dieser Tabelle aufgeführten OID sind in diesem Attribut nicht zulässig.~~

ENTWURF

- Das Attribut "jti" ~~wird auch zur Sperrung des "ID_TOKEN" in Störfällen verwendet.~~ kann als eindeutiger Identifikator für einen Replay-Schutz genutzt werden. Anhand des Attributs "jti" lassen sich "ID~~"~~_TOKEN" und "~~REFRESH~~_SSO_TOKEN" einem bestimmten Vorgang zuordnen. ~~Die eindeutige Token-ID aus dem Parameter "jti" wird auch zur Sperrung des "ID_TOKEN" in Störfällen verwendet.~~

A_20505 - Inhalte der Claims für Leistungserbringer (HBA)
~~**A_19752 - Inhalte des Claims für Leistungserbringer (HBA)**~~Fachdienste MÜSSEN bei ihrer Registrierung am~~Der~~ IdP-Dienst ~~MUSS~~ sicherstellen, dass für Leistungserbringer mit einer HBA als Nutzer, die folgenden Attribute ~~im Claim immer gesetzt~~als Claims beantragt sind - Standardclaims sind~~:~~ mit "public", eigene Claims mit "private" gekennzeichnet:

Tabelle 4 TAB_IDP_FD_0004 Inhalte des Claims für Leistungserbringer (HBA)

Attribut	Inhalt
"iss" (public)	Beinhaltet die URL des ~~Fachdienstes als HTTPs-Adresse mit Pfad und Angabe des Ports, wenn dieser vom Standard abweicht ohne zusätzliche Parameter.~~IdP-Dienstes
"sub" (public)	~~Beinhaltet die Telematik-ID des Leistungserbringers, welche aus dem nonQES-Signaturzertifikat auszulesen ist.~~Beinhaltet einen verschlüsselten Identifikator, der sich aus der "client_id" und dem Host-Teil der "redirect_uri" des Anwendungsfrontends zusammensetzt. Dieser zusammengesetzte Wert wird mit dem privaten Schlüssel des Authorization Servers "PrK_SUBJECT_ENC" nach der pairwise-Methode [openid-connect-core-1_0 # PairwiseAlg] vom IdP-Dienst verschlüsselt.
"nonce" (public)	Beinhaltet einen Zufallswert, welchen der IdP-Dienst nach den Vorgaben des ~~Anwendungsfrontend~~Anwendungsfrontends bzw. Primärsystems befüllt und anhand dessen das Primärsystem seine Vorgänge unterscheiden kann.
"acr" (public)	Authentication Context Class Reference gemäß ~~[~~[openid-connect-core-1_0 # IDToken]
"aud" (public)	Hier sind gemäß [RFC7519 # section-4.1.3] entweder die URI des Fachdienstes oder ein entsprechender eindeutiger String eingetragen, die bzw. der den Fachdienst identifizieren.
"professionOID" (private)	Beinhaltet die professionOID des Leistungserbringers gemäß [gemSpec_OID # Tab_PKI_402].
"given_name" (public)	Vorname ~~Nachname~~ des Leistungserbringers – der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus.
"family_name" (public)	Nachname des Leistungserbringers – der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus.

ENTWURF

"organizationName" (private)	leer
"idNummer" (private)	Beinhaltet die Telematik-ID des Leistungserbringers – der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus.
"jti"	ID des Tokens

[<=]

Hinweise:

- Die Befüllung des Claims erfolgt grundsätzlich gemäß [rfc7519 # section-4]
- Beispiel-Wert des Attributs "iss": "https://erp.telematik/pfad/login"
- Das Attribut "iss" wird durch den IdP-Dienst befüllt.
- Das Attribut "aud" beschreibt den Fachdienst durch dessen eindeutige URI oder einen beim IdP-Dienst ausschließlich diesem Fachdienst zugesprochenendiscovery Wert z.B. "E-Rezept" oder "eRP".
- Das Attribut "professionOID" des Leistungserbringers wird durch den IdP-Dienst befüllt. Andere als die in dieser Tabelle gemäß [gemSpec_OID # Tab_PKI_402] aufgeführten OID sind in diesem Attribut nicht zulässig.
- ~~sub~~Das Attribut "idNummer" wird mit den Informationen aus dem Signaturzertifikat durch den IdP-Dienst befüllt.
- ~~Das Attribut "professionOID" des Leistungserbringers wird durch den IdP-Dienst befüllt. Andere als die in dieser Tabelle gemäß [gemSpec_OID # Tab_PKI_402] aufgeführten OID sind in diesem Attribut nicht zulässig.~~
- Das Attribut "jti" ~~wird auch zur Sperrung des "ID_TOKEN" in Störfällen verwendet.~~kann als eindeutiger Identifikator für einen Replay-Schutz genutzt werden. Anhand des Attributs "jti" lassen sich Zugriffs- und ~~Refresh~~SSO-Token einem bestimmten Vorgang zuordnen. ~~Die eindeutige Token-ID aus dem Parameter "jti" wird auch zur Sperrung des "ID_TOKEN" in Störfällen verwendet.~~

Das Claim einer Leistungserbringerinstitution beschreibt nicht die Entität, welche im Namen der Institution agiert, sondern die Institution selbst.

A_20506 - Inhalte der Claims für Leistungserbringerinstitutionen (SMC-B)
~~**A_19753 - Inhalte des Claims für SMC-B**~~Fachdienste MÜSSEN bei ihrer Registrierung am~~Der~~ IdP-Dienst ~~MUSS~~ sicherstellen, dass für Leistungserbringerinstitutionen mit einer SMC-B für Nutzer, die folgenden Attribute ~~im Claim immer gesetzt~~als Claims beantragt sind~~:~~ - Standardclaims sind mit "public", eigene Claims mit "private" gekennzeichnet:

Tabelle 5 AB_IDP_FD_0005 Inhalte des Claims für Leistungserbringerinstitutionen (SMC-B)

Attribut	Inhalt
"iss" (public)	Beinhaltet die URL des ~~Fachdienstes als HTTPs Adresse mit Pfad ohne zusätzliche Parameter und Angabe des Ports, wenn dieser vom Standard abweicht.~~IdP-Dienstes

ENTWURF

"sub" (public)	~~Beinhaltet die "telematikID" der Leistungserbringerinstitution~~Beinhaltet einen verschlüsselten Identifikator, der sich aus der "client_id" und dem Host-Teil der "redirect_uri" des Anwendungsfrontends zusammensetzt. Dieser zusammengesetzte Wert wird mit dem privaten Schlüssel des Authorization Servers "PrK_SUBJECT_ENC" nach der pairwise-Methode [openid-connect-core-1_0 # PairwiseAlg] vom IdP-Dienst verschlüsselt.
"nonce" (public)	Beinhaltet einen Zufallswert, welchen der IdP-Dienst nach den Vorgaben des ~~Anwendungsfrontend~~Anwendungsfrontends befüllt und anhand dessen das Anwendungsfrontend seine Vorgänge unterscheiden kann.
"acr" (public)	Authentication Context Class Reference gemäß [openid-connect-core-1_0 # IDToken]
"aud" (public)	Hier sind gemäß [RFC7519 # section-4.1.3] entweder die URI des Fachdienstes oder ein entsprechender eindeutiger String eingetragen, die bzw. der den Fachdienst identifizieren.
"professionOID" (private)	Beinhaltet die professionOID ~~des Leistungserbringers~~der Leistungserbringerinstitution gemäß [gemSpec_OID#Tab_PKI_403]
"given_name" (public)	Vorname des Verantwortlichen/Inhabers – der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus.
"family_name" (public)	Nachname des Verantwortlichen/Inhabers – der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus
~~"name" (public)~~"organizationName" (private)	Beinhaltet die Bezeichnung der Institution~~/Organisation~~, so wie diese im nonQES-Signaturzertifikat im Attribut "subject/organisationName" eingetragen ist. Der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus.
"idNummer" (private)	Beinhaltet die Telematik-ID der Leistungserbringerinstitution – der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus.
"jti"	ID des Tokens

[<=]

Hinweise:

ENTWURF

- Die Befüllung des Claims erfolgt grundsätzlich gemäß [rfc7519 # section-4]
- Beispiel-Wert des Attributs "iss": "https://erp.telematik/pfad/login"
- Das Attribut "iss" wird durch den IdP-Dienst befüllt.
- Das Attribut "aud" beschreibt den Fachdienst durch dessen eindeutige URI oder einen beim IdP-Dienst ausschließlich diesem Fachdienst zugesprochenen Wert z.B. "e-Rezept" oder "eRp".
- Das Attribut "professionOID" der Leistungserbringerinstitution wird durch den IdP-Dienst befüllt. Andere als die in dieser Tabelle gemäß [gemSpec_OID # Tab_PKI_402] aufgeführten OID sind in diesem Attribut nicht zulässig.
- ~~sub~~Das Attribut "idNummer" wird mit den Informationen aus dem Signaturzertifikat durch den IdP-Dienst befüllt.
- ~~Das Attribut "professionOID" des Leistungserbringers wird durch den IdP-Dienst befüllt. Andere als die in dieser Tabelle gemäß [gemSpec_OID # Tab_PKI_402] aufgeführten OID sind in diesem Attribut nicht zulässig.~~
- Das Attribut "jti" ~~wird auch zur Sperrung des "ID_TOKEN" in Störfällen verwendet.~~kann als eindeutiger Identifikator für einen Replay-Schutz genutzt werden. Anhand des Attributes "jti" lassen sich ~~Zugriffs~~ "ACCESS_TOKEN" und ~~Refresh-Token~~ "SSO_TOKEN" einem bestimmten Vorgang zuordnen. ~~Die eindeutige Token ID aus dem Parameter "jti" wird auch zur Sperrung des "ID_TOKEN" in Störfällen verwendet.~~

~~Möglicher Inhalt eines durch den IdP-Dienst befüllten ID_TOKEN einer Institution/Organisation, angereichert mit den im Claim vereinbarten Attributen am Beispiel E-Rezept, wie es im Attribut "jti" erkennbar ist.~~Das folgende Beispiel eines vom IdP-Dienst ausgestellten "ACCESS_TOKEN beschreibt die möglichen Inhalte anhand des Beispiels E-Rezept. Grundsätzlich besteht der Aufbau aus einem Header, dem Payload und der Signatur. Die jeweiligen Teile sind durch das Trennzeichen Punkt "." voneinander separiert. Als Trennzeichen zwischen den einzelnen Attribut-Wert-Paaren ist ein Komma "," vorgesehen. Nicht nummerische Werte sind in doppelte Anführungszeichen "" zu setzen. Innerhalb eines Attribut-Wertes sind Aufzählungen durch Doppelpunkte ":" und Wertegruppen durch Komma "," zu trennen. Werte innerhalb eines Attributs können verschachtelte JSON Web Token enthalten. Diese sind durch Eingrenzung mit geschweiften Klammern "{}" einzugrenzen.

Das im folgenden Beispiel verwendete Schlüsselmaterial lautet:

Privater Schlüssel des IdP-Dienstes "PRK_TOKEN"

```
MIG2AgEAMBAGByqGSM49AgEGBSuBBAAiBIGeMIGbAgEBBDAamStb0Xep3y3sWw2u
SSAdUPkgQ9Rvhlnx8XEVOYy2teh69T0on77ja02m03n8t8WhZANiAARUNSar38Rz
lKPyZFsNSGUanzpNRth0C+MikVEH8FAlDHMMpAs34dyF4IK0uxgbiEe9bQ+ieLrl
6xwFR0yaTivuwoyXC+ScGUnwnpaXmid6UUgw4ypbneHsaKuZ9JLdMAo=
```

Öffentlicher Schlüssel des IdP-Dienstes "PUK_TOKEN"

```
MHYwEAYHKoZIzj0CAQYFK4EEACIDYgAEVDUmq9/Ec5Sj8mRbDUhlGp86TUbYdAvj
IpFRB/BQJQxzDKQLN+HcheCCtLsYG4hHvW0Poni65escBUdMmk4r7sKMlwvknBlJ
8J6Wl5onelFIMOMqW53h7GirmfSS3TAK
```

ENTWURF

Der Zeitstempel "exp" liegt 300 Sekunden nach dem Erstellungszeitpunkt des Tokens "iat". Das Attribut "jti" beinhaltet die Kennzeichnung des Providers, einen 20 Ziffern langen Zufallswert sowie die mit dem Token beantragten Rechte.

Die folgenden Attribute sind mit Beispielen befüllt.

```
{
      "iss": "https://idp1.telematik.de/jwt",
      "sub": "3-15.1.1.123456789",
      "RabcUSuuWKKZEEHmrcNm_kUDOW13uaGU5Zk8OoBwiNk",
      "professionOID": "1.2.276.0.76.4.50",
      "nbf": 1585336956,
      "exp": 1585337256,
      "iat": 1585336956,
      "given_name": "der Vorname",
      "family_name": "der Nachname",
      "organizationName": "Institutions- oder Organisations-Bezeichnung",
      "idNummer": "3-15.1.1.123456789",
      "jti": "<IDP>_01234567890123456789",
      "typaud": "https://erp.telematik.de/login"
}
```

Aus den im Beispiel aufgeführten Attributen ergibt sich unter Verwendung obigen Schlüsselmaterials das folgende Token:

Base64-Darstellung des Token Header bestehend-Header, bestehend aus den JWT-Standard-Headern (siehe [RFC7519 # section-3.1]) "alg" = "ES256" und "typ" = "JWT"

```
eyJhbGciOiJFUzM4NCIsInR5cCI6IkpXVCJ9
```

Trennzeichen (Punkt) gefolgt vom base64-codierten Payload des mit Parametern befüllten Claims

```
eyJpc3MiOiJodHRwczovL2lkcDEudGVsZW1hdGlrLmRlL2p3dCIsInN1YiI6InJmYzkyMjptZWl
uZVRlbGVtYXRp
lEQHRlbGVtYXRpay5kZSIsIm9pZCI6IjEuMi4yNzYuMC43Ni40LjQ5IiwibmJmIjoxNTg1MzM2O
TU2LCJleHAiOj
1ODUzMzcyNTYsImlhdCI6MTU4NTMzNjk1Niwidm4xIjoiSGFucyIsIm5uMSI6Ild1cnN0Iiwian
RpIjoiYXZhcnR
XzAxMjM0NTY3ODkwMTIzNDU2Nzg5IGVSUDpyZWFkLGRlbGV0ZSIsInR5cCI6Imh0dHBzOi8vZXJ
wLnRlbGVtYXRp
ay5kZS9sb2dpbiJ9
```

Trennzeichen (Punkt) gefolgt von der Signatur des Tokens

```
NwlB-Qd2eniyqCjJFzEohC227QJ4m2ar0_ar1xUn-Ld29XFxUyxY6L-orZR-
rtQhpEcR6QiZDqzhN9tauDRqQ-jpoGdcgjpVj0IwHxb9sc3ckOLKGaIFUbcEZNQ2R0ox
```

ENTWURF

554

~~5 Administratives Logoff~~

ENTWURF

5 Blacklisting von Client-IP-Adressen

Bekommt ein Fachdienst Kenntnis davon, dass ein "~~ID~~ACCESS_TOKEN" zur Durchführung eines Angriffs~~(~~, z. B. einer Distributed Denial of Service DDOS-Attacke~~)~~ (DDOS), verwendet wird, ~~DARF~~muss der Fachdienst die ~~Token ID verwenden, um damit eine sofortige Löschung~~IP-Adresse des ~~"ID_TOKEN" und damit verbundener "REFRESH_TOKEN" durchzusetzen.~~

~~Hierbei wird die zwischen IdP-Dienst und Authenticator sowie Anwendungsfrontend als Basis genutzte Subject Session eliminiert, woraufhin alle darauf basierenden Token ungültig werden. Der Fachdienst kann hiervon nur durch eine Token Introspection Kenntnis erhalten. Es ist daher dringend angeraten, jedoch nicht zwingend erforderlich, vor der Annahme und Verwendung der "ID_TOKEN" eine Token Introspection durchzuführen.~~

~~Diese Maßnahme soll nur genutzt werden, wenn es unbedingt erforderlich ist und der Missbrauch des "ID_TOKEN" offensichtlich ist. Dies ist z.B. der Fall, wenn das "ID_TOKEN" von unterschiedlichen URI oder mehrfach nacheinander~~Absenders in ~~hoher Frequenz eingereicht wird.~~

~~Die folgenden Anforderungen sind nicht durch die verwendeten Standards (siehe [gemSpec_IDP_Dienst] und [gemSpec_IDP_Frontend]) abgedeckt. Es ist Aufgabe des IdP-Dienstes und der Fachdienste, Angriffe durch ein befallenes oder korruptes Endgerät zu vereiteln. Da der Standard hierzu keine valide Maßnahme bietet, stehen zwei alternative Umsetzungsmaßnahmen zur Auswahl, wovon beide umgesetzt werden sollen, um das höchstmögliche Maß an Kontrolle zu gewährleisten.~~

~~**A_19754 - Backchannel Revocation durch Fachdienste**~~
~~Fachdienste MÜSSEN das "ID_TOKEN" beim Revocation Endpunkt TLS-gesichert einreichen, um eine Backchannel Revocation auszulösen. Um den Request von einem Widerruf eines "ID_TOKEN" (Token Revocation) zu unterscheiden, MUSS der HTTP-Header zusätzlich den Parameter "events" mit dem Wertepaar des vorgefallenen Ereignisses und dem Identifier der mit dem Ereignis verbundenen "SUBJECT_SESSION" enthalten. Die Anfrage MUSS vom Fachdienst mit dessen privatem Schlüssel "PRK_FD" signiert sein.**[<=]**~~

~~Hinweis: Das Löschen der gesamten Subject Session erfordert am Endgerät des Nutzers das erneute Registrieren des Authenticators und des Anwendungsfrontend beim Authorization-Endpunkt.~~

~~**A_19755 - Blacklisting von ID_TOKEN**~~
~~Der Fachdienst MUSS~~ eine Blacklist ~~führen, in welche er "ID_TOKEN" einträgt, denen er zur Laufzeit nicht mehr vertrauen will. Die TTL (Time to live) des Eintrags MUSS länger gesetzt sein als die Gültigkeitsdauer des "ID_TOKEN". **[<=]**~~

eintragen, um sich vor weiteren Angriffen von dieser Adresse ausgehend zu schützen. Der Fachdienst muss diese IP-Adresse nach einer Stunde wieder**~~A_20056 - Keine Reaktion auf Anfragen~~** aus **~~dem Blacklisting~~**
~~Der Fachdienst MUSS das vorgetragene "ID_TOKEN" in~~ der Blacklist ~~suchen.~~
~~Der Fachdienst MUSS Reaktionen auf Anfragen von "ID_TOKEN" aus der Blacklist unterlassen.**[<=]**~~

ENTWURF

entfernen, wenn von der gefilterten IP-Adresse keine weiteren Angriffe mehr verzeichnet werden, damit im Falle dynamisch vergebener IP-Adressen diese wieder genutzt werden kann.

A_20019 - Blacklisting von IP-Adressen
Der Fachdienst MUSS eine Blacklist führen, in welcher er IP-Adressen oder ganze Subnetze einträgt, wenn Angriffsszenarien von diesen Adressen oder Netzen erfolgen.
[<=]

~~**A_19756 - Bereinigen der "ID_TOKEN"-Blacklist**~~
~~Fachdienste MÜSSEN in die Blacklist eingetragene "ID_TOKEN" in regelmäßigen Abständen (spätestens alle 60 Minuten) bereinigen und aus der Blacklist diejenigen "ID_TOKEN" löschen, deren natürliche Lebensdauer beendet ist. **[<=]**~~

A_20020 - Bereinigung der "IP-Adress"-Blacklist Host-Adressen
Fachdienste MÜSSEN Host-Adressen mit einer Verzögerung von einer Stunde aus der Blacklist streichen, wenn von der gefilterten IP-Adresse keine weiteren Angriffe mehr verzeichnet werden.**[<=]**

A_20631 - Einschränkung zur Bereinigung der "IP-Adress"-Blacklist Subnetze
~~**A_20021 - Bereinigung der "IP-Adress"-Blacklist Subnetze**~~Fachdienste ~~MÜSSEN~~DÜRFEN Netzadressen NICHT aus der Blackliste streichen, wenn es sich hierbei um Blacklisting auf Basis von Geo-IP-Adressbereichen handelt.**[<=]**

ENTWURF

6 Token Introspection

Der Fachdienst muss die Möglichkeit haben und ist ebenso dazu verpflichtet, die Gültigkeit eines vorgetragenen "ID_TOKEN" zu prüfen. Diese Prüfung hat mindestens einmal im Zeitrahmen der Gültigkeit des "ID_TOKEN" zu erfolgen. Die Prüfung kann häufiger erfolgen, soll aber zusätzlich nur dann durchgeführt werden, wenn ein begründeter Verdacht (z.B. Token-Missbrauch) vorliegt.

Für die Token Introspection bietet der IdP-Dienst gemäß [RFC7662] eine entsprechende Schnittstelle an, bei welcher Fachdienste, gegen Vorlage der ID des zu untersuchenden "ID_TOKEN", dessen aktuellen Gültigkeitsstatus überprüfen können. Die URI des Token Introspection-Endpunktes "URI_INT" erfährt der Fachdienst aus dem Discovery Document, welches beim Systemstart eingelesen und ausgewertet werden muss.

Die Anfrage (Token Introspection Request) erfolgt gemäß [RFC7662 # section-2.1], wobei dem IdP-Dienst die folgenden Informationen bereitgestellt werden müssen:

6.1 Token Introspection Request

A_19757 – Inhalt des Token Introspection Request
Fachdienste MÜSSEN in der Token Introspection-Anfrage mindestens die folgenden Attribute angeben:
"token" (zwingend erforderlich)
Beinhaltet die ID des "ID_TOKEN", welches auf aktuelle Gültigkeit geprüft werden soll.
"token_type_hint" (optional)
Beinhaltet einen Hinweis darauf, um welche Art von Token es sich bei der Prüfungsanfrage handelt.**[<=]**

Da es sich bei den von Fachdiensten zur Prüfung eingereichten Token-Typen ausschließlich um "ID_TOKEN" handelt, ist die Übergabe des Hinweises nicht erforderlich.

A_20000 – Token Introspection Schutz des "ID_TOKEN"
Um das Ausspähen der Informationen aus dem Token zu verhindern, MUSS der Fachdienst das "ID_TOKEN" vor dem Einreichen zur Introspection mit dem öffentlichen Schlüssel "PUK_INT" des Introspection-Endpunktes verschlüsseln.
Der Downloadpunkt des öffentlichen Schlüssels "PUK_INT" ist im Discovery Document enthalten.**[<=]**

A_19758 – Token Introspection Frequenz
Fachdienste MÜSSEN beim ersten Erhalt eines "ID_TOKEN" eine Token Introspection zu diesem durchführen. Ebenso MUSS ein Fachdienst zur Halbzeit der Gültigkeitsdauer des "ID_TOKEN" mindestens eine zweite Token Introspection durchführen, um sicherzustellen, dass das "ID_TOKEN" in der Zwischenzeit noch nicht widerrufen wurde.**[<=]**

Der IdP-Dienst, welcher das Token ausgegeben hat, überprüft anhand der eingereichten Token-ID die mit der Beantragung eingereichten Attribute (Signatur-Zertifikat) und bestätigt dem anfragenden Fachdienst gemäß [RFC7662 # section-2.2] die angefragten

ENTWURF

Attribute (siehe auch [gemSpec_IDP_Dienst # Abschnitt 5.5 Token Introspection-Endpunkt]).

6.2 Token Introspection Response

A_19759 - Inhalt der Token Introspection-Antwort

Fachdienste MÜSSEN in der Token Introspection Response folgende Attribute gemäß [RFC7662 # section-2.2] auswerten:

`"active"`

beschreibt den Gültigkeitsstatus des `"ID_TOKEN"` (siehe "Liste möglicher Werte des Attributs`"active"` einer Token Introspection-Antwort")

`"iat"`

Zeitstempel in Sekunden nach UTC 01.01.1970 T00:00:00Z, zu welchem das `"ID_TOKEN"` erstellt wurde

`"client_id"`

Beinhaltet die ID des Authenticators, von welchem aus das `"ID_TOKEN"` beantragt wurde

`"exp"`

Zeitstempel in Sekunden nach UTC 01.01.1970 T00:00:00Z, der das zeitliche Ende der Gültigkeit des `"ID_TOKEN"` bestimmt

`"sub"`

Identifier des Token Endpunkt, um Vorgänge der Subject Session zusammenzuführen.**[<=]**

A_19760 - Token Introspection unerwartete Informationen

ENTWURF

~~7 Der Fachdienst MUSS eine Formatänderung (z.B. Reihenfolge) der Token Introspection Response akzeptieren. Der Fachdienst MUSS nur diejenigen Attribute der Token Introspection Response auswerten, welche dieser selbst erwartet.~~
~~[<=]~~

~~**A_20057 - Token Introspection Response Inhalte**~~
~~Der Token Introspection Endpunkt DARF NICHT andere, als die im Claim mit dem Fachdienst vereinbarten Informationen herausgeben.~~
~~[<=]~~

~~Die Token Introspection Response kann weitere vom Fachdienst nicht erwartete Attribute enthalten.~~

~~**A_20058 - Token Introspection enthält keine schützenswerten Informationen**~~

ENTWURF

8 Der Fachdienst DARF in der Token Introspection Response schützenswerte Informationen aus dem Token oder über dessen Besitzer NICHT preisgeben. [<=]

A_19761 - Signatur der Token Introspection-Antwort
Der Fachdienst MUSS die Signatur der Token Introspection Response mit dem öffentlichen Schlüssel des Token Introspection-Endpunktes "PUK_INT" prüfen.
[<=]

A_19762 - Auswertung der positiven Token Introspection
Fachdienste MÜSSEN die Token Introspection auswerten. Weicht der Wert des Attributes "active" vom boolschen Wert "1" für "true" ab, MUSS der Fachdienst den mit dem "ID_TOKEN" in Verbindung stehenden Vorgang abbrechen.
[<=]

A_20004 - Positive Token Introspection
Fachdienste MÜSSEN das "ID_Token" als gültig anerkennen, wenn die Token Introspection in der Response im Attribut "active" den boolschen Wert "1" für "true" erhält.
[<=]

Auszug einer positiven Token Introspection (Beispiel):

```
HTTP/1.1 200 OK Content-Type:
application/json
{
"active": true,
"client_id": "<IDP>_01234567890123456789",
...
}
```

A_19763 - Negative Token Introspection
Fachdienste MÜSSEN das "ID_Token" als ungültig betrachten, wenn die Token Introspection in der Response im Attribut "active" den boolschen Wert "0" für "false" erhält.[<=]

Beispiel einer negativen Token Introspection

```
HTTP/1.1 200 OK Content-Type:
application/json
{
"active": false
}
```

A_19764 - Ungültige "ID_TOKEN" bleiben ungültig
Fachdienste DÜRFEN negativ beschiedene Token Introspection-Anfragen NICHT erneut stellen. "ID_TOKEN", welche ungültig waren, bleiben ungültig.[<=]

ENTWURF

~~A_19765 - Warten auf die Token Introspection Antwort~~
~~Fachdienste SOLLEN nicht länger als 3 Sekunden auf die Token Introspection Response warten. Fachdienste SOLLEN bei fehlender Response der Token Introspection Anfrage den mit dem IT_Token verbundenen Vorgang abbrechen.~~**~~[<=]~~**

~~A_19766 - Auto-Logoff~~
~~Fachdienste SOLLEN den bereits angestoßenen Vorgang zu Ende führen und danach den Zugang deaktivieren, wenn während eines laufenden Vorgangs (z.B. File Up- oder Download) festgestellt wird, dass das "ID_TOKEN" zeitlich abgelaufen ist.~~**~~[<=]~~**

ENTWURF

~~96 "ID"~~"ACCESS_TOKEN"

Der IdP-Dienst stellt den ~~berechtigten und überprüften~~ authentifizierten Entitäten "~~ID~~ACCESS_TOKEN" aus, mit welchen diese den Zugriff auf die im Claim des Fachdienstes bereitgestellten Systeme realisieren können.

A_20362 - "ACCESS_TOKEN" generelle Struktur
~~A_19767 - "ID_TOKEN" generelle Struktur~~Fachdienste MÜSSEN die gemäß [RFC7519 # section-7.1] vorgeschriebene Struktur der "~~ID~~ACCESS_TOKEN" gemäß [RFC7519 # section-7.2] validieren.
[<=]

A_20363 - "ACCESS_TOKEN" sind verschlüsselt
~~A_19776 - "ID_TOKEN" sind verschlüsselt~~Der Fachdienst MUSS die für ihn vom IdP-Dienst gemäß [RFC6750 # section-5.2 Abs. 7] ~~mit seinem im Claim verbundenen öffentlichen Schlüsseln "PUK_FD" zielgerichtet~~ verschlüsselten "~~ID~~ACCESS_TOKEN" mit seinem privaten Schlüssel "PRK_FD" gemäß [RFC 7523 # Abschnitt 7 Absatz 1 Satz 2 i.V.m. RFC6750 # Abschnitt 5.2 Absatz 7] entschlüsseln.
[<=]

A_20364 - Unverschlüsselt eingehende ACCESS_TOKEN sind ungültig
~~A_19779 - Unverschlüsselt eingehende ID_TOKEN sind ungültig~~Fachdienste DÜRFEN unverschlüsselt eingehende "~~ID~~ACCESS_TOKEN" NICHT annehmen.
~~[<=, da diese als korrumpiert anzusehen sind.~~
~~[<=~~]

A_20365 - Die Signatur des "ACCESS_TOKEN" ist zu prüfen
~~A_19780 - Die Signatur des "ID_TOKEN" ist zu prüfen~~Fachdienste MÜSSEN die Signatur der "~~ID~~ACCESS_TOKEN" gegen den öffentlichen Schlüssel des Token-Endpunktes "PUK_TOKEN" prüfen.~~[<=]~~

A_20504 - Reaktion bei ungültiger oder fehlender Signatur des "ACCESS_TOKEN"
~~[RFC7523 # section-3]~~
~~Ist ein "ID_TOKEN" nicht signiert oder dessen Signatur fehlerhaft, MUSS~~ Der Fachdienst MUSS alle mit dem "~~ID~~ACCESS_TOKEN" verbundenen Vorgänge abbrechen, wenn das "ACCESS_TOKEN" nicht signiert oder dessen Signatur fehlerhaft ist.
~~[<=.~~
~~[<=~~]

~~Die URI "URI_PUK_TOKEN", unter welcher der "PUK_TOKEN" verfügbar ist, ist im Discovery Document veröffentlicht.~~

A_20367 - Fehlermeldungen bei Übertragungsfehler des "ACCESS_TOKEN" melden
~~A_20228 - Übertragungsfehler ID_TOKEN~~Fachdienste MÜSSEN ~~Fehlermeldungen~~Fehler, welche bei der Annahme des ~~ID~~"ACCESS_TOKEN" entstehen, ~~herausgeben~~melden. Die Fehlermeldung MUSS mit dem privaten Schlüssel "PRK_FD" signiert ~~und mit dem öffentlichen Schlüssel "PUK_FRONT" des Anwendungsfrontends verschlüsselt erfolgen. Die Fehlermeldung MUSS~~ sein. Die Fehlermeldungen MÜSSEN für den Anwender verständlich formuliert sein. **[<=]**

ENTWURF

A_20368~~A_19801~~ - Auswertung des Claims
Fachdienste MÜSSEN die im "~~ID~~ACCESS_TOKEN" ~~bestätigten~~übertragenen Attribute mit ~~den~~ denen vergleichen, die mit dem IdP-Dienst bei der Registrierung vereinbart wurden.**[<=]**

A_20369 - Abbruch bei unerwarteten Inhalten
~~vereinbarten Claims abgleichen. Enthält das "ID_TOKEN" andere als die im Claim mit dem IdP-Dienst vereinbarten Attribute, MUSS~~ Der Fachdienst MUSS alle mit dem "~~ID~~ACCESS_TOKEN" in Verbindung stehenden Vorgänge abbrechen, wenn das "ACCESS_TOKEN" andere als die im Claim mit dem IdP-Dienst vereinbarten Attribute enthält.**[<=]**

A_20370 - Abbruch bei falschen Datentypen der Attribute
.
Fachdienste MÜSSEN "~~ID~~ACCESS_TOKEN" ablehnen, wenn die in einem Attribut vorgetragenen Werte nicht dem schematisch erwarteten Datentyp des Attributes entsprechen.**[<=]**

~~**A_19802 - Herkunft des "ID_TOKEN"**~~
~~Fachdienste MÜSSEN die Herkunft des Tokens (HTTP/1.1 Request) mit der im "ID_TOKEN" registrierten "redirect_uri" abgleichen. Wird ein "ID_TOKEN" von einer anderen Stelle eingereicht, MUSS der Fachdienst die mit dem "ID_TOKEN" in Verbindung stehenden Vorgänge abbrechen, da von einem Token-Missbrauch auszugehen ist.**~~**[<=]**~~

A_20372 - Prüfung der zeitlichen Gültigkeit des "ACCESS_TOKEN"
~~**A_19803 - Prüfung der zeitlichen Gültigkeit des "ID_TOKEN"**~~Fachdienste MÜSSEN die zeitliche Gültigkeit des "~~ID~~ACCESS_TOKEN" prüfen. Der Zeitpunkt der Überprüfung MUSS zeitlich zwischen den Zeitstempeln "iat" und "exp" liegen.
[<=]

~~Zusätzliche Prüfungsmechanismen sind im Abschnitt Token Introspection und Administratives Logoff beschrieben.~~

A_20373 - Prüfung der Gültigkeit des "ACCESS_TOKEN" für den Zugriff auf Fachdienste ohne "nbf"
Fachdienste MÜSSEN sicherstellen, dass der Zeitraum der Verwendung des Tokens zwischen den im Token mitgelieferten Werten der Attribute "iat" und "exp" liegt.**[<=]**

A_20374 - Prüfung der Gültigkeit des "ACCESS_TOKEN" für den Zugriff auf Fachdienste mit "nbf"
Fachdienste MÜSSEN sicherstellen, dass der Zeitraum der Verwendung des Tokens zwischen den im Token mitgelieferten Werten der Attribute "nbf" und "exp" liegt.**[<=]**

ENTWURF

~~10~~7 Abstimmen der Rahmenbedingungen "~~ID~~ACCESS_TOKEN"-Gültigkeit

Die Registrierung eines Fachdienstes erfolgt in enger Abstimmung zwischen Fachdienst und IdP-Dienst. ~~Hierbei werden Regelungen getroffen, welchem Akteur (zu erkennen an deren im Antrag übermittelter professionOID) welche Rechte zugesprochen werden sollen. Ärzte z.B. müssen die Möglichkeit haben, neue E-Rezepte einzustellen, Versicherte dürfen diese jedoch nur auflisten, abrufen oder löschen.~~ Fachdienste geben dem IdP-Dienst gegenüber bei der Registrierung an, ~~welche professionOID~~ mit welchen ~~Rechten und~~ Gültigkeitszeiträumen ~~mit "ID~~die "ACCESS_TOKEN" ~~oder "REFRESH~~und "SSO_TOKEN" ausgestattet werden sollen. Der Fachdienst selbst sieht vor, welche ~~Nutzer~~ Nutzergruppe generell Zugriff erhalten, indem nur für diese Nutzer Claims vorgesehen sind. Registriert beispielsweise ein Fachdienst für die von ihm bereitgestellten ~~Protected Server z.B.~~Fachdaten kein Claim für Versicherte, können diese am Authorization-Endpunkt auch kein~~"ID_TOKEN" und infolge dessen auch kein "REFRESH~~ "ACCESS_TOKEN" zu diesem Fachdienst erhalten.

A_20679~~A_20009~~ - Beantragung eines Claims für Fachdienste
Der Fachdienst MUSS sich für die Beantragung eines Claims ~~die vom IdP-Dienst bereitgestellten Formulare oder das vom IdP-Dienst vorgesehene Verfahren nutzen~~beim IdP-Dienst registrieren, um ein Claim für eine bestimmte Nutzergruppe für seinen Fachdienst zu beantragen. ~~[<=~~
~~Der Fachdienst MUSS für jede Nutzergruppe "professionOID" ein eigenes Claim beantragen.[<=~~**]**

A_20375 - Angabe der Lebensdauer des "ACCESS_TOKEN"
~~**A_19804 - Token Profile**~~Fachdienste MÜSSEN bei der Registrierung der ~~Attribute, welche sie~~Claims im ~~"ID_TOKEN" erwarten, in ihrem Claim auch~~Attribut "tokenTimeout" angeben, welche Lebensdauer ~~und Erneuerungsfrequenz die von ihnen erwarteten "ID_TOKEN" und gegebenenfalls im Zusammenhang damit ausgestellte "REFRESH~~das "ACCESS_TOKEN" ~~haben soll, besitzen sollen.~~**[<=]**

~~**A_20007 - Ein Claim pro professionOID**~~
~~Der Fachdienst MUSS für jede zu erwartende professionOID ein eigenes Claim erstellen und beim IdP-Dienst mit dem Authorization-Endpunkt abstimmen.~~
~~Der Fachdienst MUSS das Attribut Berechtigung <1 Byte> in jedem Claim entsprechend der "professionOID" setzen.[<=]~~

~~Aus der folgenden Liste geht hervor, welche Token-Typen durch einen Fachdienst im Claim vereinbart sind und wie sich deren Lebenszyklus zusammensetzt [gemSpec_IDP_Dienst # Abschnitt 5.2].~~

A_20503~~A_19805~~ - Mit Fachdiensten abgestimmte Lebenszyklen
Fachdienste MÜSSEN die in ihrem Claim abgestimmten Attributwerte der folgenden Liste mit Werten aus den hier vorgegebenen Bereichen füllen.
Liste der Lebenszyklen der Token registrierter Fachdienste:

ENTWURF

Tabelle 6 AB_IDP_FD_0006 Lebenszyklen der Token

Fachdienst	~~allowRefresh~~	~~maxRefresh~~	tokenTimeout	~~lastAuth~~auth_time	~~Berechtigung~~
<STRING>	~~<Boolean>~~	~~<300-86.400>~~	<60-900>	<900-~~14.400~~43.200>	~~<1 Byte>~~
eRp	~~true~~	~~28.800~~	300	~~900~~43.200	~~<professionOID>~~ ~~*1)~~

~~Diese sind durch die Vorgaben des IdP-Dienstes limitiert auf:~~ ~~[<=]~~

~~Fachdienst~~	~~allowRefresh~~	~~maxRefresh~~	~~tokenTimeout~~	~~lastAuth~~	~~Berechtigung~~
~~alle_Dienste~~	~~true~~	~~86.400~~	~~900~~	~~14.400~~	~~<vier Rechte>~~ ~~*2)~~

~~*1) Fachdienste MÜSSEN für jede zu erwartende "professionOID" ein eigenes Claim stecken [A_20007].~~

~~*2) Die vier Rechte beschränken sich auf "Vererbung", "Lesen", "Schreiben" und "Löschen"~~ ~~[<=]~~

Beschreibung am Beispiel E-Rezept (eRp~~)~~):

Der Fachdienst E-Rezept sieht vor, dass Nutzer mit "~~ID~~ACCESS_TOKEN" und "~~REFRESH~~SSO_TOKEN" ausgestattet werden. Die Gültigkeit des "~~REFRESH~~SSO_TOKEN" beträgt ~~28.800~~immer 43.200 Sekunden = ~~8~~ 12 Stunden ~~und ist im Attribut "maxRefresh" hinterlegt~~.

Für diesen Zeitraum ~~darf~~braucht das ~~mit der Anmeldung verbundene Anwendungsfrontend nach der Authentisierung gegen das zugelassene Authentisierungsmerkmal "ID~~Authenticator-Modul keine erneute Nutzer-Authentifizierung durchzuführen, um beim IdP-Dienst einen neuen "ACCESS_TOKEN" ~~am TOKEN_ENDPOINT einfordern und beim~~ für den Fachdienst ~~eRp vorstellig werden~~zu erlangen.

Die Gültigkeitsdauer ~~der mit einem "REFRESH_TOKEN" oder dem "ACCESS_CODE" erworbener "ID~~des "ACCESS_TOKEN" beträgt im Beispiel E-Rezept 300 Sekunden = 5 Minuten.

~~Berechtigung: Die Spalte 'Berechtigung' beinhaltet in Abhängigkeit der professionOID des vorgetragenen Signaturzertifikates die damit verbundenen Berechtigungen. Sind diese unterschiedlich, muss für jede professionOID ein eigenes Claim mit dem IdP-Dienst abgestimmt werden.~~

ENTWURF

~~11~~8 Anhang A – Verzeichnisse

~~11.1~~8.1 Abkürzungen

Kürzel	Erläuterung
AVS	Apothekenverwaltungssystem
DDOS	Distributed Denial of Service
eGK	Elektronische Gesundheitskarte
eRp	E-Rezept
HBA	Heilberufsausweis
IdP	Identity Provider
ISP	Internet Service Provider
JSON	JavaScript Object Notaion
JWT	JSON Web Token
KVNR	Krankenversichertennummer
NFC	Near Field Communication
OAuth 2.0	Open Authorization 2.0
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PVS	Praxisverwaltungssystem
QES	Qualifizierte Elektronische Signatur
SMC-B	Security Module Card Typ B, Institutionenkarte
TI	Telematikinfrastruktur
TLS	Transport Layer Security
URI	Uniform Resource Identifier

ENTWURF

~~11.2~~8.2 Glossar

Begriff	Erläuterung
Access Token	Ein Access Token (nach [RFC6749 # section-1.4]) wird vom Client (Anwendungsfrontend) benötigt, um auf geschützte Daten eines Resource Servers zuzugreifen. Die Representation kann als JSON Web Token erfolgen.
Authorization Server	OAuth2 Rolle (siehe [RFC6749 # section-1.1]): Der Authorization Server ist Teil des IdP-Dienstes. Der Server authentifiziert den Resource Owner (Nutzer) und stellt Access Tokens für den vom Resource Owner erlaubten Anwendungsbereich (Scope) für einen Resource Server bzw. eine auf einem Resource Server existierende Protected Resource aus.
Claim	Ein Key/Value-Paar im Payload eines JSON Web Token.
Client	OAuth2 Rolle (siehe [RFC6749 # section-1.1]): Eine Anwendung (Relying Party), die auf geschützte Ressourcen des Resource Owners zugreifen möchte, die vom Resource Server bereitgestellt werden. Der Client kann auf einem Server (Webanwendung), Desktop-PC, mobilen Gerät etc. ausgeführt werden.
~~Claim~~Discovery Dokument	~~Das Claim ist die zwischen Fachdienst und IdP-Dienst abgestimmte Menge von Attributen nach Art und Umfang, also welche und mit welchen Wertebereichen die Attribute geliefert werden müssen.~~Ein OpenID Connect Metadatendokument (siehe [openid-connect-discovery 1.0]), das den Großteil der Informationen enthält, die für eine App zum Durchführen einer Anmeldung erforderlich sind. Hierzu gehören Informationen wie z.B. die zu verwendenden URLs und der Speicherort der öffentlichen Signaturschlüssel des Dienstes.
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
ID Token	Ein auf JSON basiertes und nach [RFC7519] (JWT) genormtes Identitäts-Token, mit dem ein Client (Anwendungsfrontend) die Identität eines Nutzers überprüfen kann.
Open Authorization 2.0	Ein Protokoll zur Autorisierung für Web-, Desktop und Mobile Anwendungen. Dabei wird es einem Endbenutzer (Resource Owner) ermöglicht, einer Anwendung (Client) den Zugriff auf

ENTWURF

	Daten oder Dienste (Resources) zu ermöglichen, die von einem Dritten (Resource Server) bereitgestellt werden.
OpenID Connect	OpenID Connect (OIDC) ist eine Authentifizierungsschicht, die auf dem Autorisierungsframework OAuth 2.0 basiert. Es ermöglicht Clients, die Identität des Nutzers anhand der Authentifizierung durch einen Autorisierungsserver zu überprüfen (siehe [openid-connect-core 1.0]).
JSON Web Token	Ein auf JSON basiertes und nach [RFC7519] (JWT) genormtes Access-Token. Das JWT ermöglicht den Austausch von verifizierbaren Claims innerhalb seines Payloads.
Resource Owner	OAuth2-Rolle (siehe [RFC6749 # section-1.1]): Eine Entität (Nutzer), die einem Dritten den Zugriff auf ihre geschützten Ressourcen gewähren kann. Diese Ressourcen werden durch den Resource Server bereitgestellt. Ist der Resource Owner eine Person, wird dieser als Nutzer bezeichnet.
Resource Server	OAuth2 Rolle (siehe [RFC6749 # section-1.1]): Der Server (Dienst), auf dem die geschützten Ressourcen (Protected Resources) liegen. Er ist in der Lage, auf Basis von Access Tokens darauf Zugriff zu gewähren. Ein solcher Token repräsentiert die delegierte Autorisierung des Resource Owners.
SSO Token	Gegen Vorlage eines gültigen SSO Token ist keine erneute Nutzerauthentifizierung für die Ausstellung eines Access Tokens am IdP-Dienst nötig.

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

~~11.3~~8.3 Abbildungsverzeichnis

~~11.4~~8.4 Tabellenverzeichnis

ENTWURF

~~11.5~~8.5 Referenzierte Dokumente

~~11.5.1~~8.5.1 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: Einführung der Gesundheitskarte – Glossar
[gemSpec_IDP_Dienst]	gematik: Spezifikation Identity Provider-Dienst
[gemSpec_IDP_Frontend]	gematik: Spezifikation Identity Provider-Frontend
[gemSpec_Krypt]	gematik:Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_PKI]	gematik: Übergreifende Spezifikation Spezifikation PKI

~~11.5.2~~8.5.2 Weitere Dokumente

~~Die weiteren zu beachtenden Dokumente sind im zentralen Dokument des Produktyps IdP-Dienst beschrieben.~~

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[openid-connect-core]	OpenID Connect Core 1.0 (November 2014) https://openid.net/specs/openid-connect-core-1_0.html

ENTWURF

[openid-connect-discovery]	OpenID Connect Discovery 1.0 (November 2014) https://openid.net/specs/openid-connect-discovery-1_0.html
[RFC6749]	The OAuth 2.0 Authorization Framework (Oktober 2012) https://tools.ietf.org/html/rfc6749
[RFC6750]	The OAuth 2.0 Authorization Framework: Bearer Token Usage (Oktober 2012) https://tools.ietf.org/html/rfc6750
[RFC7519]	JSON Web Token (Mai 2015) https://tools.ietf.org/html/rfc7519
[RFC7523]	JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants (Mai 2015) https://tools.ietf.org/html/rfc7523

942

ENTWURF