Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste

Version:	1.~~2~~3.0
Revision:	~~325132~~374755
Stand:	~~19.02~~14.06.2021
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_IDP_FD

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
1.0.0	30.06.20		initiale Erstellung des Dokuments	gematik
1.1.0	12.10.20		Einarbeitung Scope-Themen zu R4.0.1	gematik
1.1.1	13.11.20		Einarbeitung P22.4	gematik
1.2.0	19.02.21		Einarbeitung P22.5	gematik
1.3.0	14.06.21		Einarbeitung IDP 2.2.0 (inkl. entsprechender Anteile aus gemF_Tokenverschlüsselung & gemF_Biometrie) und der Änderungsliste IdP_Maintenance_21.1	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb 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 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 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 8).

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.

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.

2 Systemüberblick

In der Telematikinfrastruktur (TI) werden zahlreiche Fachdienste angeboten. Anwendungsfrontends können über die Authentifizierung des Nutzers am IdP-Dienst Zugriff zu den von den Fachdiensten angebotenen Daten erhalten. Der IdP-Dienst stellt durch gesicherte JSON Web Token (JWT) attestierte Identitäten aus. Gegen Vorlage eines "ACCESS_TOKEN" erhalten Anwendungsfrontends, entsprechend der im Token attestierten professionOID, Zugriff auf die Inhalte der Fachdienste.

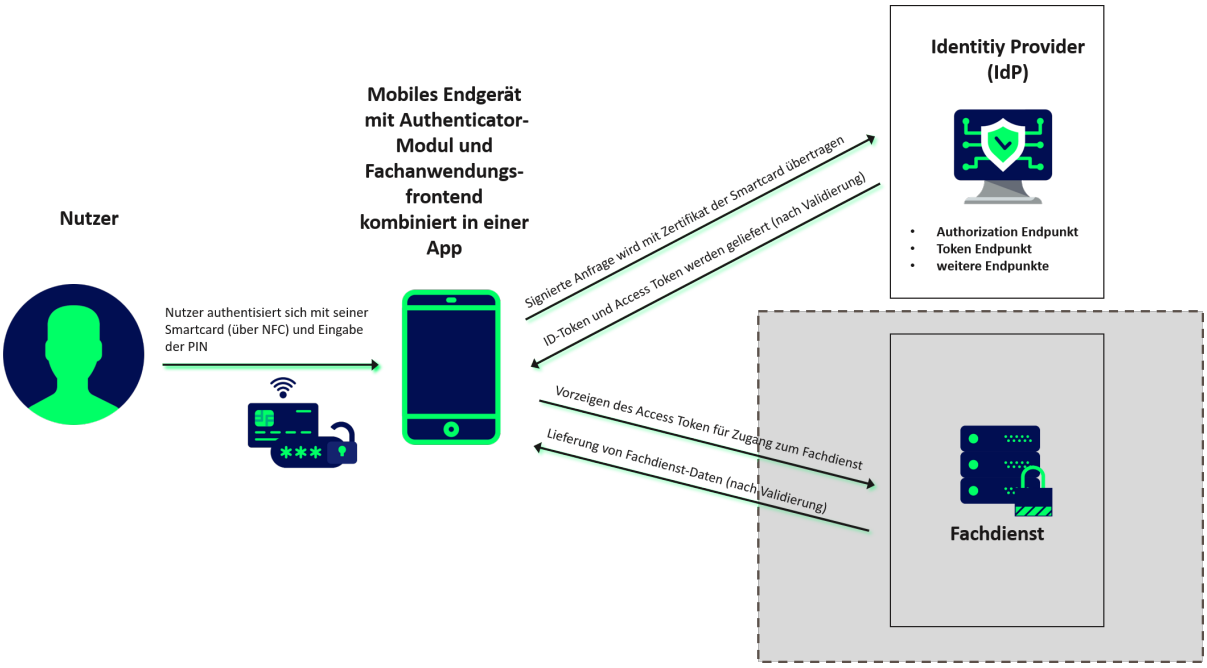

Abbildung 1: Systemüberblick (vereinfacht)

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. Der IdP-Dienst fasst die professionOID sowie weitere für den Fachdienst notwendige Attribute in signierten JSON Web Token ("ID_TOKEN", "ACCESS_-" und "SSO_TOKEN") zusammen. Fachdienste müssen keine Überprüfung des Nutzers selbst implementieren, sondern können sich darauf verlassen, dass der Besitzer des bei ihnen vorgetragenen "ACCESS_TOKEN" bereits identifiziert wurde. Des Weiteren stellt der IdP-Dienst sicher, dass die vom Nutzer vorgetragenen Attribute (aus dem Signaturzertifikat) gültig sind.

Der IdP-Dienst prüft, ob das vorgetragene X.509-nonQES-Signatur-Zertifikat der verwendeten Prozessor-Chipkarte (eGK, HBA oder SMC-B) für die vorgesehene Laufzeit des Tokens zeitlich gültig und ob dessen Integrität sichergestellt ist.

Der IdP-Dienst stellt nur solche "ACCESS_TOKEN" aus, welche auf gültigen AUT-Zertifikaten (d.h. C.CH.AUT, C.HP.AUT oder C.HCI.AUT) basieren.

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 der Claims (Key/Value-Paare im Payload eines JSON Web Token) mit dem IdP-Dienst (organisatorischer Prozess gemäß Abschnitt 4.1)
- Abstimmen der Rahmenbedingungen für die Gültigkeit von "ACCESS_TOKEN" (siehe Abschnitt 7)

Alle Fachdienste müssen zur Absicherung der JSON Web Token gegen Einsichtnahme durch Dritte den Transportweg mit Transport Layer Security (TLS) gemäß [gemSpec_Krypt] absichern. Der Fachdienst muss sowohl im Internet, als auch innerhalb der TI über ein überprüfbares TLS-Serverzertifikat verfügen. Innerhalb der TI werden Fachdienste mit TLS-Zertifikaten durch die Komponenten-Public Key Infrastructure (PKI) ausgestattet. Im Internet müssen die Fachdienste durch ein öffentlich prüfbares Serverzertifikat gesichert werden.

Fachdienste sind ebenfalls Nutzer des IdP-Dienstes 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 "ACCESS_TOKEN", um Nutzern Zugriff auf die von ihnen bereitgestellten geschützten Ressourcen, die Fachdaten, zu gewähren.

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.

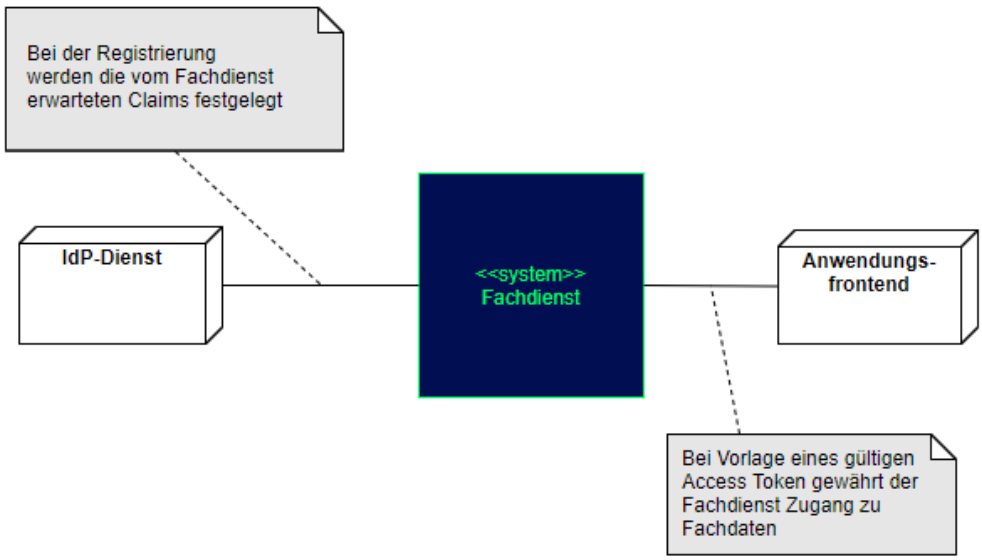

Abbildung 2: Systemkontext aus Sicht des Fachdienstes

3.1 Akteure und Rollen

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

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.

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

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:

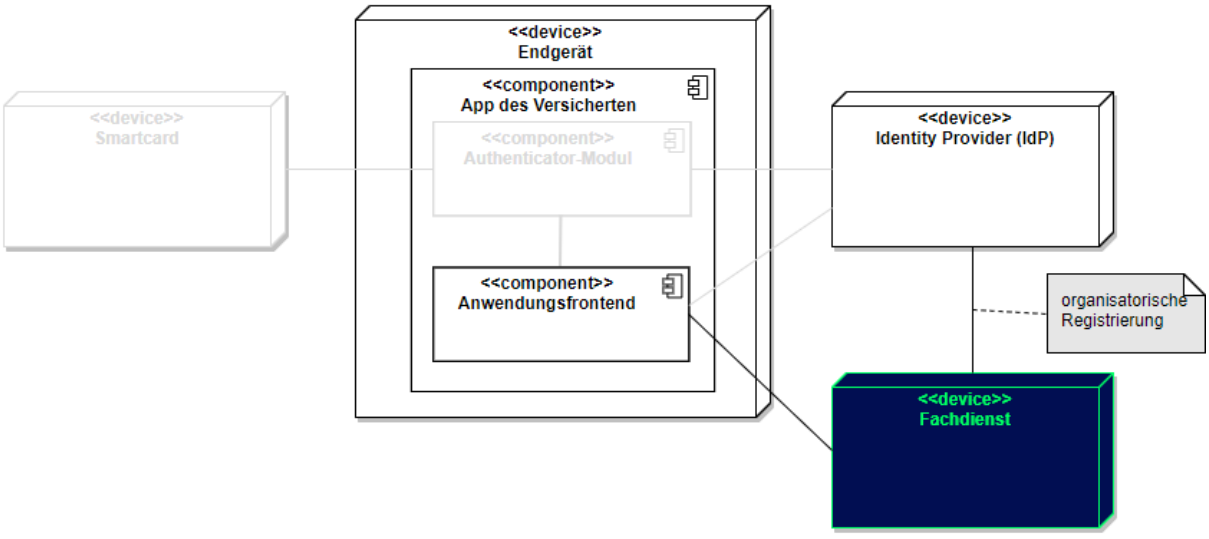

Abbildung 3: Nachbarsysteme des Fachdienstes

4 Registrierung des Fachdienstes beim IdP-Dienst

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 - Adressen des Dienstes werden registriert
Der Anbieter des Fachdienstes MUSS, um die Erreichbarkeit des Fachdienstes zu gewährleisten, entsprechende Adressen im TI-Namensraum beantragen. In Fällen, in denen der Fachdienst ebenfalls aus dem Internet erreichbar sein soll, MUSS der 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~~eine sprechende Fachdienstbezeichnung~~ eine statische IP-Adresse, auf deren Basis die URI adressiert wird~~. Die URI des Fachdienstes "URI_FD" muss dem Authorization Server, welcher Teil des IdP-Dienstes ist, bekanntgegeben werden.

~~**A_20296 - 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 "ACCESS_TOKEN" zielgerichtet für den entsprechenden Fachdienst verschlüsseln kann.~~**~~[<=]~~**

A_20739 - Registrierung der Claims des Fachdienstes
Anbieter von Fachdiensten 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 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. 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.

Die Claims beinhalten die für diesen Fachdienst abgestimmten Attribute (die Claims werden pro Fachdienst in einem organisatorischen Prozess gesondert vom jeweiligen Fachdienst mit dem IdP-Dienst abgestimmt) 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):

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

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.

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

A_20297-02~~A_20297-01~~ - Inhalte des Claims für Versicherte (eGK)
Fachdienste MÜSSEN bei ihrer Registrierung am IdP-Dienst sicherstellen, dass für Versicherte mit einer eGK als Nutzer die fachlich benötigten Attribute aus der folgenden ~~Attribute~~Auswahl als Claims beantragt ~~sind~~ werden. Standardclaims sind mit "public", eigene Claims mit "private" gekennzeichnet:

Tabelle 3: TAB_IDP_FD_0003 Inhalte des ~~Claims~~Claim für Versicherte (eGK)

Attribut	Inhalt
"iss" (public)	Beinhaltet die URL des IdP-Dienstes als HTTPS-Adresse mit Pfad und Angabe des Ports, wenn dieser vom Standard abweicht. Zusätzliche Query-Parameter sind nicht erlaubt.
"sub" (public)	Beinhaltet einen ~~verschlüsselten~~ Identifikator~~,~~. Es werden 3 Eingangswerte verwendet: der ~~sich aus der "client_id"~~Fachdienstidentifier (konfiguriert), ein Fachdienst-spezifischer Salt (konfiguriert) und ~~dem Host-Teil~~der Claim "idNummer". Diese Eingangswerte werden verkettet in der ~~"redirect_uri" des Anwendungsfrontends zusammensetzt.~~ Reihenfolge: Fachdienstidentifier, Claim "idNummer" und Fachdienst-spezifischer Salt. Dieser verkettete Text wird mit SHA-256 gehasht, das Ergebnis ist der Claim "sub". SHA256(fd_identifier + idNummer + fd_salt) Dieser zusammengesetzte 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.~~zusammengestellt.
"nonce" (public)	Beinhaltet einen Zufallswert, welchen der IdP-Dienst nach den Vorgaben des Anwendungsfrontends befüllt und anhand dessen das Anwendungsfrontend seine Vorgänge unterscheiden kann. (Dieser Claim ist nur in ID-Token enthalten.)
"acr" (public)	Authentication Context Class Reference gemäß [openid-connect-core-1_0 # IDToken~~]~~] mit dem konkreten Wert "gematik-ehealth-loa-high".
"amr" (public)	Authentication Method Refererence gemäß [https://tools.ietf.org/html/rfc8176] und [https://openid.net/specs/openid-connect-modrna-authentication-1_0.html]
"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 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 "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 "jti" kann als eindeutiger Identifikator für einen Replay-Schutz genutzt werden. Anhand des Attributs "jti" lassen sich "ID_TOKEN" und "SSO_TOKEN" einem bestimmten Vorgang zuordnen.

Die Aufbau von ACCESS_TOKEN und ID_TOKEN entspricht [gemSpec_IDP_Dienst#Kapitel 7.6 Token Response].

A_20505-02~~A_20505-01~~ - Inhalte der Claims für Leistungserbringer (HBA)
Fachdienste MÜSSEN bei ihrer Registrierung am IdP-Dienst sicherstellen, dass für Leistungserbringer mit einer HBA als Nutzer ~~,~~ die fachlich benötigten Attribute aus der folgenden ~~Attribute~~Auswahl als Claims beantragt ~~sind~~werden - 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 IdP-Dienstes als HTTPS-Adresse mit Pfad und Angabe des Ports, wenn dieser vom Standard abweicht. Zusätzliche Query-Parameter sind nicht erlaubt.
"sub" (public)	Beinhaltet einen ~~verschlüsselten~~ Identifikator~~,~~. Es werden 3 Eingangswerte verwendet: der ~~sich aus der "client_id"~~Fachdienstidentifier (konfiguriert), ein Fachdienst-

	spezifischer Salt (konfiguriert) und ~~dem Host-Teil~~der Claim "idNummer". Diese Eingangswerte werden verkettet in der ~~"redirect_uri" des Anwendungsfrontends zusammensetzt.~~ Reihenfolge: Fachdienstidentifier, Claim "idNummer" und Fachdienst-spezifischer Salt. Dieser verkettete Text wird mit SHA-256 gehasht, das Ergebnis ist der Claim "sub". SHA256(fd_identifier + idNummer + fd_salt) 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.~~ zusammengestellt.
"nonce" (public)	Beinhaltet einen Zufallswert, welchen der IdP-Dienst nach den Vorgaben des Anwendungsfrontends bzw. Primärsystems befüllt und anhand dessen das Primärsystem seine Vorgänge unterscheiden kann. (Dieser Claim ist nur in ID-Token enthalten.)
"acr" (public)	Authentication Context Class Reference gemäß [openid-connect-core-1_0 # IDToken] mit dem konkreten Wert "gematik-ehealth-loa-high".
"amr" (public)	Authentication Method Reference gemäß [https://tools.ietf.org/html/rfc8176] und [https://openid.net/specs/openid-connect-modrna-authentication-1_0.html]
"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 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.
"organizationName" (private)	~~leer~~leer - Der Wert des Claims ist immer NULL, da der Wert im AUT-Zertifikat immer leer ist. Der NULL-Wert darf nicht zur Ablehnung des Tokens durch den Fachdienst führen.
"idNummer" (private)	Beinhaltet die Telematik-ID des Leistungserbringers~~—~~: der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus.
"jti"	ID des ~~Tokens~~Token

~~[<=]~~
[<=]

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~~zugesprochenen 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.
- Das Attribut `"idNummer"` wird mit den Informationen aus dem Signaturzertifikat durch den IdP-Dienst befüllt.
- Das Attribut `"jti"` kann als eindeutiger Identifikator für einen Replay-Schutz genutzt werden. Anhand des Attributs `"jti"` lassen sich Zugriffs- und SSO-Token einem bestimmten Vorgang zuordnen.

Die Aufbau von ACCESS_TOKEN und ID_TOKEN entspricht [gemSpec_IDP_Dienst#Kapitel 7.6 Token Response].

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

A_20506-02~~A_20506-01~~ - Inhalte der Claims für Leistungserbringerinstitutionen (SMC-B)
Fachdienste MÜSSEN bei ihrer Registrierung am IdP-Dienst sicherstellen, dass für Leistungserbringerinstitutionen mit einer SMC-B für Nutzer ~~,~~ die fachlich benötigten Attribute aus der folgenden ~~Attribute~~Auswahl als Claims beantragt ~~sind~~ werden (Standardclaims sind mit "public", eigene Claims mit "private" gekennzeichnet~~:~~):

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

Attribut	Inhalt
`"iss"` (public)	Beinhaltet die URL des IdP-Dienstes als HTTPS-Adresse mit Pfad und Angabe des Ports, wenn dieser vom Standard abweicht. Zusätzliche Query-Parameter sind nicht erlaubt.
`"sub"` (public)	Beinhaltet einen ~~verschlüsselten~~ Identifikator~~,~~. Es werden 3 Eingangswerte verwendet: der ~~sich aus der "client_id"~~Fachdienst-Identifier (konfiguriert), ein Fachdienst-spezifischer Salt (konfiguriert) und ~~dem Host-Teil~~der Claim "idNummer". Diese Eingangswerte werden verkettet in der ~~"redirect_uri" des~~

	~~Anwendungsfrontends zusammensetzt.~~ Reihenfolge: Fachdienst-Identifier, Claim "idNummer" und Fachdienst-spezifischer Salt. Dieser verkettete Text wird mit SHA-256 gehasht. Das Ergebnis ist der Claim "sub". SHA256(fd_identifier + idNummer + fd_salt) 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.~~ zusammengestellt.
"nonce" (public)	Beinhaltet einen Zufallswert, welchen der IdP-Dienst nach den Vorgaben des Anwendungsfrontends befüllt und anhand dessen das Anwendungsfrontend seine Vorgänge unterscheiden kann. (Dieser Claim ist nur in ID-Token enthalten.)
"acr" (public)	Authentication Context Class Reference gemäß [openid-connect-core-1_0 # IDToken] mit dem konkreten Wert "gematik-ehealth-loa-high".
"amr" (public)	Authentication Method Refererence gemäß [https://tools.ietf.org/html/rfc8176] und [https://openid.net/specs/openid-connect-modrna-authentication-1_0.html]
"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 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. Sollte der Wert nicht im Zertifikat vorhanden sein, wird der Wert des Claims mit NULL gefüllt. Der NULL-Wert darf nicht zur Ablehnung des Tokens durch den Fachdienst führen.
"family_name" (public)	Nachname des Verantwortlichen/Inhabers~~—~~: der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus. Sollte der Wert nicht im Zertifikat vorhanden sein, wird der Wert des Claims mit NULL gefüllt. Der NULL-Wert darf nicht zur Ablehnung des Tokens durch den Fachdienst führen.
"organizationName" (private)	Beinhaltet die Bezeichnung der Institution, so wie diese im nonQES-Signaturzertifikat im Attribut "subject/organisationName" eingetragen ist. Der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus. Sollte der Wert nicht im Zertifikat vorhanden sein, wird der Wert des Claims mit NULL gefüllt. Der NULL-Wert darf nicht zur Ablehnung des Tokens durch den Fachdienst führen.

"idNummer" (private)	Beinhaltet die Telematik-ID der Leistungserbringerinstitution~~—~~: der IdP-Dienst liest dies aus dem nonQES-Signaturzertifikat aus.
"jti"	ID des ~~Tokens~~Token

[<=]

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 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~~403] aufgeführten OID sind in diesem Attribut nicht zulässig.
- Das Attribut "idNummer" wird mit den Informationen aus dem Signaturzertifikat durch den IdP-Dienst befüllt.
- Das Attribut "jti" kann als eindeutiger Identifikator für einen Replay-Schutz genutzt werden. Anhand des Attributes "jti" lassen sich "ACCESS_TOKEN" und "SSO_TOKEN" einem bestimmten Vorgang zuordnen.

~~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.~~

~~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.~~

```
~~{~~
~~"sub": "subject",~~
~~"organizationName": "gematik GmbH NOT-VALID",~~
~~"professionOID": "1.2.276.0.76.4.49",~~
~~"idNummer": "X114428530",~~
~~"iss": "http://idp-dienst.de",~~
~~"response_type": "code",~~
~~"code_challenge_method": "S256",~~
```

```
"given_name": "Juna",
"client_id": "oidc_client",
"acr": "eidas-loa-high",
"aud": "erp.zentral.erp.ti-dienste.de",
"auth_time": 1605081534,
"scope": "openid e-rezept",
"redirect_uri": "http://localhost:8081/test",
"state": "af0ifjsldkj",
"exp": 1605081834,
"family_name": "Fuchs",
"code_challenge": "1IYYNZrIPZVySx0b9VzRz89EAghbtBWJI-qvdNCyCiM",
"iat": 1605081534
}
```


Hinweise zu obigem Token-Beispiel :

Das Attribut "organizationName" enthält hier den Hinweis "NOT-VALID" welcher dem Umstand geschuldet ist, dass zur Erstellung des Beispiels eine nicht gültige elektronische Gesundheitskarte (Laborkarte) genutzt wurde.

Das Attribut "nbf" ist im Beispiel derzeit noch nicht mit aufgenommen.

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

Base64-Darstellung des Token-Header, bestehend aus den JWT-Standard-Headern (siehe [RFC7519 # section-3.1]) "alg" = "BP256r1" und "typ" = "JWT"


```
eyJhbGciOiJCUDI1NlIxIn0
```


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


```
eyJzdWIiOiJzdWJqZWN0Iiwib3JnYW5pemF0aW9uTmFtZSI6ImdlbWF0aWsgR21
iSCBOT1QtVkFMSUQiLCJwcm9mZXNzaW9uT0lEIjoiMS4yLjI3Ni4wLjc2LjQuND
kiLCJpZE51bW1leiI6IlgxMTQ0Mjg1MzAiLCJpc3MiOiJodHRwOi8vaWRwLWRpZ
W5zdC5kZSIsInJle3BvbnNlX3R5cGUiOiJjb2RlIiwiY29kZV9jaGFsbGVuZ2V
bWV0aG9kIjoiUzI1NiIsImdpdmVuX25hbWUiOiJKdW5hIiwiY2xpZW50X2lkIjo
ib2lkY19jbGllbnQiLCJhY3IiOiJlaWRhcy1sb2EtaGlnaCIsImF1ZCI6ImVycC
56ZW50cmFsLmVycC50aS1kaWVuc3RlLmRlIiwiYXV0aF90aW1lIjoxNjA1MDgxN
TM0LCJzY29wZSI6Im9wZW5pZCBlLXJlemVwdCIsInJlZGlyZWN0X3VyaSI6Imh0
dHA6Ly9sb2NhbGhvc3Q6ODA4MS90ZXN0Iiwic3RhdGUiOiJhZjBpZmpzbCRraiI
sImV4cCI6MTYwNTA4MTgzNCwiZmFtaWx5X25hbWUiOiJGdWNoeyIsImNvZGVfY2
hhbCxlbmdlIjoiMUlZWU5ackl0Wlz5U3gwYjlWelJ6ODlFQWdoYnRCV0pJLXF2Z
E5HeUdpTSIsImlhdCI6MTYwNTA4MTUzNH0
```


. Trennzeichen (Punkt) gefolgt von der Signatur des Tokens


```
mc5xMBR7Kl2KZrFhARN5fqAHCvdisnmQYgoHazq8N1to_kARYLocN6rguDs3EQP
dlH0TJTelFoaWXRSiZ2p7HQ
```


Hinweis:

Der bei der Erstellung verwendete Algorithmus ist hier mit dem Kurzbezeichner "BP256r1" für brainpoolP256r1 angegeben und bezieht sich auf OID:1.3.36.3.3.2.8.1.1.7 woraus sich ergibt, dass der öffentlichen Schlüssel mit OID 1.2.840.10045.2.1 zu kennzeichnen ist.
Dieser Kurzbezeichner ist noch nicht bei der IANA in die Liste der zulässigen Algorithmen (siehe [https://www.iana.org/assignments/jose/jose.xhtml#web-key-elliptic-curve]) aufgenommen, die Aufnahme ist jedoch schon in der Beantragung und wird perspektivisch in Kürze erfolgen.

Die Aufbau von ACCESS_TOKEN und ID_TOKEN entspricht [gemSpec_IDP_Dienst#Kapitel 7.6 Token Response].

5 Blacklisting von Client-IP-Adressen

Bekommt ein Fachdienst Kenntnis davon, dass ein "ACCESS_TOKEN" zur Durchführung eines Angriffs, z. B. einer Distributed Denial of Service DDOS-Attacke (DDOS), verwendet wird, muss der Fachdienst die IP-Adresse des Absenders in eine Blacklist eintragen, um sich vor weiteren Angriffen von dieser Adresse ausgehend zu schützen. Der Fachdienst muss diese IP-Adresse nach einer Stunde wieder aus der Blacklist 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_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
Fachdienste DÜRFEN Netzadressen NICHT aus der Blackliste streichen, wenn es sich hierbei um Blacklisting auf Basis von Geo-IP-Adressbereichen handelt.**[**<=**]**

6 "ACCESS_TOKEN"

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

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

A_20363-01~~A_20363~~ - "ACCESS_TOKEN" sind verschlüsselt
Der Fachdienst MUSS die für ihn vom ~~IdP-Dienst gemäß [RFC6750 # section-5.2 Abs. 7]~~Anwendungsfrontend verschlüsselten "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]~~entsprechend dem für diese Übertragung vorgesehenen Verfahren entschlüsseln.
[<=]

Hinweis: Hierbei können je nach Anwendung unterschiedliche Verfahren zum Einsatz kommen. Im Fall des E-Rezeptes wird der "ACCESS_TOKEN" im Rahmen des VAU-Protokolls übertragen und ist damit ausreichend geschützt.

A_20364 - Unverschlüsselt eingehende ACCESS_TOKEN sind ungültig
Fachdienste DÜRFEN unverschlüsselt eingehende "ACCESS_TOKEN" NICHT annehmen.
[<=]

A_20365-01~~A_20365~~ - Die Signatur des "ACCESS_TOKEN" ist zu prüfen
Fachdienste MÜSSEN die Signatur der "ACCESS_TOKEN" gegen den öffentlichen Schlüssel des Token-Endpunktes "PUK_IDP_SIG" prüfen. Fachdienste MÜSSEN den öffentlichen Schlüssel „PUK_IDP_SIG" dabei dem Discovery Document des IdP-Dienstes entnehmen.**[<=**~~TOKEN" prüfen.~~**[<=]**

A_20504 - Reaktion bei ungültiger oder fehlender Signatur des "ACCESS_TOKEN"
Der Fachdienst MUSS alle mit dem "ACCESS_TOKEN" verbundenen Vorgänge abbrechen, wenn das "ACCESS_TOKEN" nicht signiert oder dessen Signatur fehlerhaft ist.
[<=]

A_20367 - Fehlermeldungen bei Übertragungsfehler des "ACCESS_TOKEN" melden
Fachdienste MÜSSEN Fehler, welche bei der Annahme des "ACCESS_TOKEN" entstehen, melden. Die Fehlermeldung MUSS mit dem privaten Schlüssel "PRK_FD" signiert sein. Die Fehlermeldungen MÜSSEN für den Anwender verständlich formuliert sein.**[<=]**

A_20369-01 - Abbruch bei unerwarteten Inhalten
~~**A_20368 - Auswertung des Claims**~~Der Fachdienst MUSS~~Fachdienste MÜSSEN~~ die im "ACCESS_TOKEN" übertragenen Attribute mit denen vergleichen, die mit dem IdP-Dienst bei der Registrierung vereinbart wurden und alle mit dem "ACCESS_TOKEN" in Verbindung stehenden Vorgänge abbrechen, wenn dem "ACCESS_TOKEN" für die Verarbeitung notwendige Claims fehlen oder aber andere als die mit dem IdP-Dienst vereinbarten personenbezogenen Attribute vorhanden sind.**[<=**~~.[<=~~**]**

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

Hinweis: Als personenbezogenes Attribute gelten gemäß Tabelle : TAB_IDP_DIENST_0005 die Claims "given_name", "family_name", "organizationName", "professionOID" und "idNummer.

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

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

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.**[<=]**

A_21520 - Prüfung des "aud" Claim des ACCESS_TOKEN mit der vom Fachdienst registrierten URI
Fachdienste MÜSSEN den Claim "aud" des "ACCESS_TOKEN" mit ihrer beim IdP-Dienst registrierten URI prüfen. Nur wenn diese übereinstimmen, gilt diese Prüfung als positiv validiert.**[<=]**

A_21521 - Fachdienst: Prüfung der Signatur des Discovery Document
Fachdienste MÜSSEN die Signatur des Discovery Document mathematisch prüfen und auf ein zeitlich gültiges C.FD.SIG-Zertifikat mit der Rollen-OID *"oid_idpd"* zurückführen können, welches von einer ihm bekannten Komponenten-PKI ausgestellt wurde.**[<=]**

7 Abstimmen der Rahmenbedingungen "ACCESS_TOKEN"-Gültigkeit

Die Registrierung eines Fachdienstes erfolgt in enger Abstimmung zwischen Fachdienst und IdP-Dienst. Fachdienste geben dem IdP-Dienst gegenüber bei der Registrierung an, mit welchen Gültigkeitszeiträumen die "ACCESS_TOKEN" und "SSO_TOKEN" ausgestattet werden sollen. Der Fachdienst selbst sieht vor, welche Nutzergruppe generell Zugriff erhalten, indem nur für diese Nutzer Claims vorgesehen sind.Registriert beispielsweise ein Fachdienst für die von ihm bereitgestellten Fachdaten kein Claim für Versicherte, können diese am Authorization-Endpunkt auch kein "ACCESS_TOKEN" zu diesem Fachdienst erhalten.

A_20679-01~~A_20679~~ - Beantragung eines Claims für Fachdienste
Der ~~Fachdienst~~ Anbieter des Fachdienstes MUSS sich für die Beantragung eines Claims beim IdP-Dienst registrieren, um ein Claim für eine bestimmte Nutzergruppe für seinen Fachdienst zu beantragen.**[<=]**

A_20375-01~~A_20375~~ - Angabe der Lebensdauer des "ACCESS_TOKEN"
~~Fachdienste MÜSSEN~~Der Anbieter des Fachdienstes MUSS bei der Registrierung der Claims im Attribut "tokenTimeout" angeben, welche Lebensdauer das "ACCESS_TOKEN" haben soll.**[<=]**

A_20503-01~~A_20503~~ - Mit Fachdiensten abgestimmte Lebenszyklen
~~Fachdienste MÜSSEN~~Der Anbieter des Fachdienstes MUSS die in ~~ihrem~~seinem Claim abgestimmten Attributwerte der folgenden Liste mit Werten aus den hier vorgegebenen Bereichen füllen.
Liste der Lebenszyklen der Token registrierter Fachdienste:

Tabelle 6: AB_IDP_FD_0006 Lebenszyklen der Token

Fachdienst	tokenTimeout	auth_time
<STRING>	<60-900>	<900-43.200>
eRp	300	43.200

[<=]

Beschreibung am Beispiel E-Rezept (eRp):

Der Fachdienst E-Rezept sieht vor, dass Nutzer mit "ACCESS_TOKEN" und "SSO_TOKEN" ausgestattet werden. Die Gültigkeit des "SSO_TOKEN" beträgt immer 43.200 Sekunden = 12 Stunden.

Für diesen Zeitraum braucht das Authenticator-Modul keine erneute Nutzer-Authentifizierung durchzuführen, um beim IdP-Dienst einen neuen "ACCESS_TOKEN" für den Fachdienst zu erlangen.

Die Gültigkeitsdauer des "ACCESS_TOKEN" beträgt im Beispiel E-Rezept 300 Sekunden = 5 Minuten.

8 Anhang A – Verzeichnisse

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

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.
Discovery Dokument	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 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.

8.3 Abbildungsverzeichnis

8.4 Tabellenverzeichnis

8.5 Referenzierte Dokumente

8.5.1 Dokumente der gematik

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

8.5.2 Weitere Dokumente

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