Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
Sektoraler Identity Provider

Version:	1.0.0
Revision:	427086
Stand:	17.12.2021
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_IDP_Sek

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	17.12.21		initiale Version	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps sektoraler Identity Provider (IDP). Ein sektoraler Identity Provider basiert auf den Standards OpenID Connect (OIDC), Open Authorization 2.0 (OAuth 2) und JSON Web Token (JWT). Die hier beschriebenen Schnittstellen werden vom Authenticator-Modul und von Clients für eine Authentifizierung eines Nutzers genutzt. Diese Authentifikation ist die Voraussetzung, damit ein Client Zugang zu Fachdaten und Prozessen eines Fachdienstes erlangen kann. Ein sektoraler Identity Provider entsprechend der aktuellen Spezifikation verwaltet und steuert den Authentifizierungsprozess für das E-Rezept.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von Identity Providern, welche die Funktionen eines sektoralen Identity Provider innerhalb der Telematikinfrastruktur realisieren 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. gemPTV_ATV_Festlegungen, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekanntgegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Nicht Bestandteil des vorliegenden Dokumentes ist die konkrete Umsetzung des Authentisierungsverfahrens zwischen Nutzer und sektoralem Identity Provider.

Als Umsetzungsleitlinie ist [OpenID Connect Core 1.0] heranzuziehen. Die TI-weit übergreifenden Festlegungen – insbesondere aus Dokumenten wie beispielsweise [gemSpec_Krypt] bezüglich Algorithmen und Schlüsselstärken sowie [gemSpec_PKI] bezüglich zu verwendender Zertifikatstypen und deren Attributausprägungen – haben Bestand, sind weiterhin bindend und werden nicht in diesem Dokument beschrieben. Die konkreten, für das Produkt relevanten Anforderungen finden sich in den entsprechenden Steckbriefen.

Die Methoden zur Etablierung eines Vertrauensverhältnisses zwischen den Anwendungen, Fachdiensten und sektoralen Identity Providern sind vorerst nicht Bestandteil dieser Spezifikation. Im Rahmen der Zugänglichmachung des E-Rezepts für Versicherte ohne NFC-fähige eGK sollen ab dem 01.01.2022 Kassen-eigene Authentifizierungssysteme an das E-Rezept angebunden werden. Der zentrale IDP-Dienst wird im Rahmen dieses sogenannten "Fast-Track-E-Rezept" als Mittler zwischen dem Anwendungsfrontend, den sektoralen Identity Providern und dem E-Rezept-Fachdienst eingesetzt, um nur minimale Anforderungen an die Identity Provider zu stellen, eine Umsetzung ohne Anpassung des Fachdienstes zu ermöglichen und ohne eine Klärung aller Fragen zur zukünftigen Föderation zu starten. Die Realisierung der ersten Stufe der sektoralen Identity Provider auf dem Vertrauensniveau "substanziell" wird auf den 31.12.2022 befristet. Betreiber, welche vor Ablauf der Befristung eine Authentifizierungslösung auf Basis des fortgeschriebenen Systems föderierter Identity Provider bereitstellen, müssen die hier beschriebene E-Rezept-Authentifizierungslösung schnellstmöglich außer Betrieb nehmen.

Dieses Dokument beschreibt keine (zukünftige) Föderation mit Identity Providern (IDPs) und Nutzern aus unterschiedlichen Kontexten.

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

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

2 Systemkontext

Die untere Abbildung beschreibt den Systemkontext aus Sicht des sektoralen Identity Provider. Das Anwendungsfrontend stellt die Anfrage zur Authentifizierung des Nutzers an den IDP-Dienst. Dieser leitet die Anfrage - wenn der Nutzer im Anwendungsfrontend eine Authentisierung über ein alternatives Verfahren ohne eGK gewählt hat - an das Authenticator-Modul des entsprechenden sektoralen Identity Provider weiter und agiert diesem gegenüber als Client. Zwischen dem Authenticator-Modul des sektoralen Identity Provider und dessen Authorization-Endpunkt findet die Authentisierung des Nutzers statt. Anschließend erhält der IDP-Dienst einen ID-Token mit den notwendigen Informationen. Auf Basis dieser Identität liefert der IDP-Dienst einen "AUTHORIZATION_CODE" zurück an das Anwendungsfrontend.

Das Anwendungsfrontend erlangt gegen Vorlage des "AUTHORIZATION_CODE" beim Token-Endpunkt einen "ID_TOKEN" und einen "ACCESS_TOKEN" und erhält anschließend gegen Vorlage des "ACCESS_TOKEN" Zugang zu den Fachdaten und -prozessen des Fachdienstes.

Der Fachdienst registriert sich zuvor am IDP-Dienst in Form eines organisatorischen Prozesses. Der IDP-Dienst registriert sich einmalig in Form eines organisatorischen Prozesses bei den sektoralen Identity Providern.

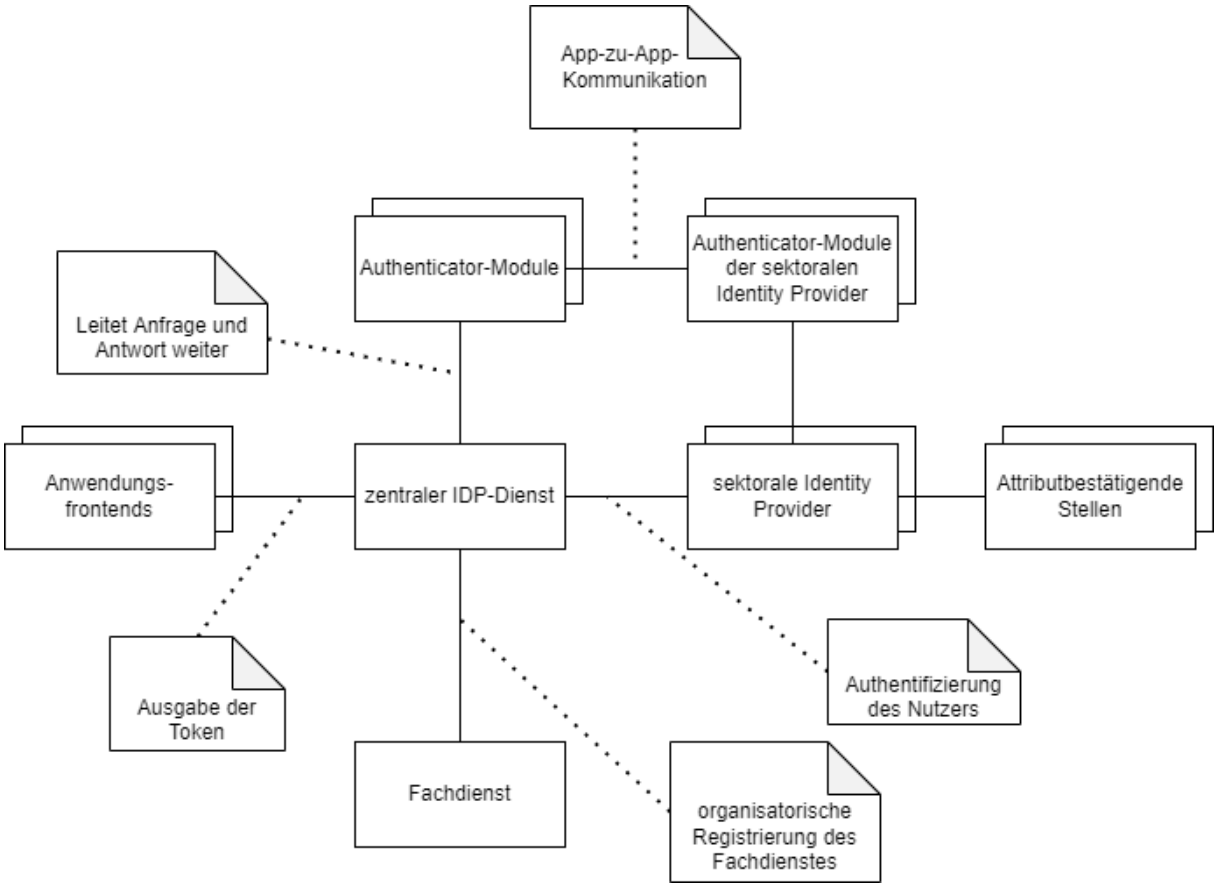

Abbildung 1: Systemkontext aus Sicht des IDP-Dienstes

2.1 Akteure und Rollen

Als sektoraler Identity Provider (IDP) wird ein Dienst bezeichnet, welcher nach vorheriger Authentifizierung Identitätsinformationen für eine bestimmte Gruppe von Nutzern innerhalb der Telematikinfrastruktur des Gesundheitswesens bereitstellt, welche anschließend verwendet werden, um auf verschiedene Fachdienste und deren Fachdaten und -prozesse zuzugreifen. Einen Sektor stellen insbesondere die Krankenkassen mit den Versicherten als Nutzer dar.Zukünftig werden allerdings auch andere Personengruppen wie z. B. Ärzte oder Pflegeinstitutionen über Identity Provider angebunden.

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

Tabelle 1: TAB_IDP_Sek_0001 Akteure und Rollen

Akteur	Rolle "äußerer Flow"	Rolle "innerer Flow"
Nutzer (z.B. Versicherte)	Resource Owner	Resource Owner
Fachdienst	Resource Server	-
Anwendungsfrontend	Client	-
Authenticator-Modul des IDP-Dienstes	Frontend des Authorization Server	-
Authenticator-Modul des sektoralen Identity Provider	-	Frontend des Authorization Server
sektoraler Identity Provider	-	Authorization Server
IDP-Dienst	Authorization Server	Client
Fachdaten und -Prozesse	Protected Resource	
Attributbestätigende Stelle	-	-

Der innere Flow und der äußere Flow sind in Abschnitt 2.2 erläutert.

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 und Prozesse (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 (Rolle: Client)

Das Anwendungsfrontend (OIDC Relying Party bzw. OAuth2 Client) greift auf Fachdienste (Resource Server) und ihre geschützten Fachdaten (Protected Resource) zu. Das Anwendungsfrontend könnte prinzipiell auf einem Server als Webanwendung (Primärsystem als Terminalserver), auf einem Desktop-PC oder einem mobilen Gerät (z.B. Smartphone) ausgeführt werden. Im Fokus der aktuellen Spezifikationen liegt jedoch allein die Kommunikation mit dem E-Rezept-FdV. Der IDP-Dienst tritt gegenüber den sektoralen Identity Providern ebenfalls in der Rolle des Client auf. Als Anwendungsfrontend wird jedoch zum besseren Verständnis nur das E-Rezept-FdV unter direkter Kontrolle des Nutzers bezeichnet.

Sektoraler Identity Provider mit dem Authenticator-Modul als Frontend (Rolle: Authorization Server)

Der Authorization Server authentifiziert den Resource Owner (Nutzer) und stellt "ID_TOKEN" für den vom Resource Owner erlaubten Anwendungsbereich (SCOPE) aus. Im Rahmen der aktuellen Einbindung von sektoralen Identity Providern in die Telematikinfrastruktur stellt der IDP-Dienst für diese ID_TOKEN eigene ID_TOKEN, ACCESS_TOKEN und SSO_TOKEN aus.

IDP-Dienst (Rollen: Authorization Server und Client)

Der zentrale IDP-Dienst tritt im Rahmen der aktuellen Einbindung von sektoralen Identity Providern in der Telematikinfrastruktur als Vermittler auf, welcher die Identitätsinformationen, die ein sektoraler Identity Provider bestätigt in für die bereits etablierten Strukturen verwendbare "ID_TOKEN" und "ACCESS_TOKEN" umwandelt. Diese werden durch das Anwendungsfrontend verarbeitet oder beim Fachdienst eingereicht, um Zugriff auf die Fachdaten und -prozesse zu erhalten.

In der Rolle des Authorization Server authentifiziert der IDP-Dienst den Nutzer (Resource Owner) und autorisiert den anfragenden Client zum Zugriff auf den Fachdienst. In der Rolle des Client ruft der IDP-Dienst beim sektoralen Identity Provider einen ID-Token ab (im Austausch gegen einen Authorization Code).

Weitere Akteure im Kontext des sektoralen Identity Provider sind:

Fachdaten und Prozesse (Rolle: Protected Resource)

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

Attributbestätigende Stelle

Attributbestätigende Stellen sind legitimierte Organisationen, welche die Korrektheit der Attribute verantworten, die durch sie für einen Nutzer beim sektoralen Identity Provider bestätigt werden.

Als Teilprozess der Registrierung ist die zuverlässige und eindeutige Identifikation der Nutzer zwingend notwendig. Hierbei werden eindeutige Identifikationsmerkmale der realen Identitäten benötigt.

Die eindeutigen Identitäten von natürlichen Personen (Versicherte, Leistungserbringer) bzw. juristischen Personen (medizinische Institutionen, Gesellschafterorganisations- und Kostenträgergeschäftsstellen) werden innerhalb der Telematikinfrastruktur über die Krankenversichertennummer des Versicherten und die Telematik-ID eines Leistungserbringers bzw. einer medizinischen Institution oder Organisation des Gesundheitswesens repräsentiert.

2.2 Nachbarsysteme und Interaktion

Ein sektoraler Identity Provider bietet zahlreiche Schnittstellen gegenüber unterschiedlichen Akteuren an, weswegen es notwendig ist, die einzelnen Schnittstellen so zu beschreiben, dass andere Akteure deren Funktionsweise leichter verstehen können.

Die erste Token-bezogene Anfrage an den sektoralen Identity Provider geht am Authorization-Endpunkt [RFC6749 # section-3.1] ein. Das Authenticator-Modul des sektoralen Identity Provider reicht dort am Endpunkt den "SCOPE" der anfragenden Anwendung ein, mit welchem die Token erstellt werden sollen, sowie die "CODE_CHALLENGE". In der ersten Phase werden Anfragen an die sektoralen Identity Provider nur durch den zentralen IDP-Dienst gestellt. Der Nutzer wird dann aufgefordert, sich unter Nutzung des Authenticator-Moduls des sektoralen Identity Provider, zu authentisieren. Nach erfolgreicher Authentisierung erstellt der sektorale Identity Provider den "AUTHORIZATION_CODE_IDP" und liefert diesen zurück. Dieser wird an den IDP-Dienst übermittelt, welcher ihn am Token-Endpunkt [RFC6749 # section-3.2] des sektoralen Identity Provider einreicht. Der sektorale Identity Provider überprüft den "AUTHORIZATION_CODE_IDP" und stellt bei positiver Validierung einen "ID_TOKEN" aus.

Der sektorale Identity Provider kann auf eine erneute Authentisierung des Nutzers verzichten, wenn diese bereits vor kurzem erfolgte. Ist der Zeitpunkt der letzten Authentisierung zu lange her oder wird das Authenticator-Modul zum ersten Mal gestartet, muss eine Authentisierung des Nutzers erfolgen.

Vorbereitende Maßnahmen: Das Authenticator-Modul des sektoralen Identity Provider und das Anwendungsfrontend sind auf dem gleichen Endgerät installiert. Der IDP-Dienst hat bei der Registrierung an den sektoralen Identity Providern seine öffentlichen Schlüssel hinterlegt.

Der IDP-Dienst kennt die Discovery-Dokumente der sektoralen Identity Provider und hat bei der Registrierung dort seine öffentlichen Schlüssel hinterlegt.

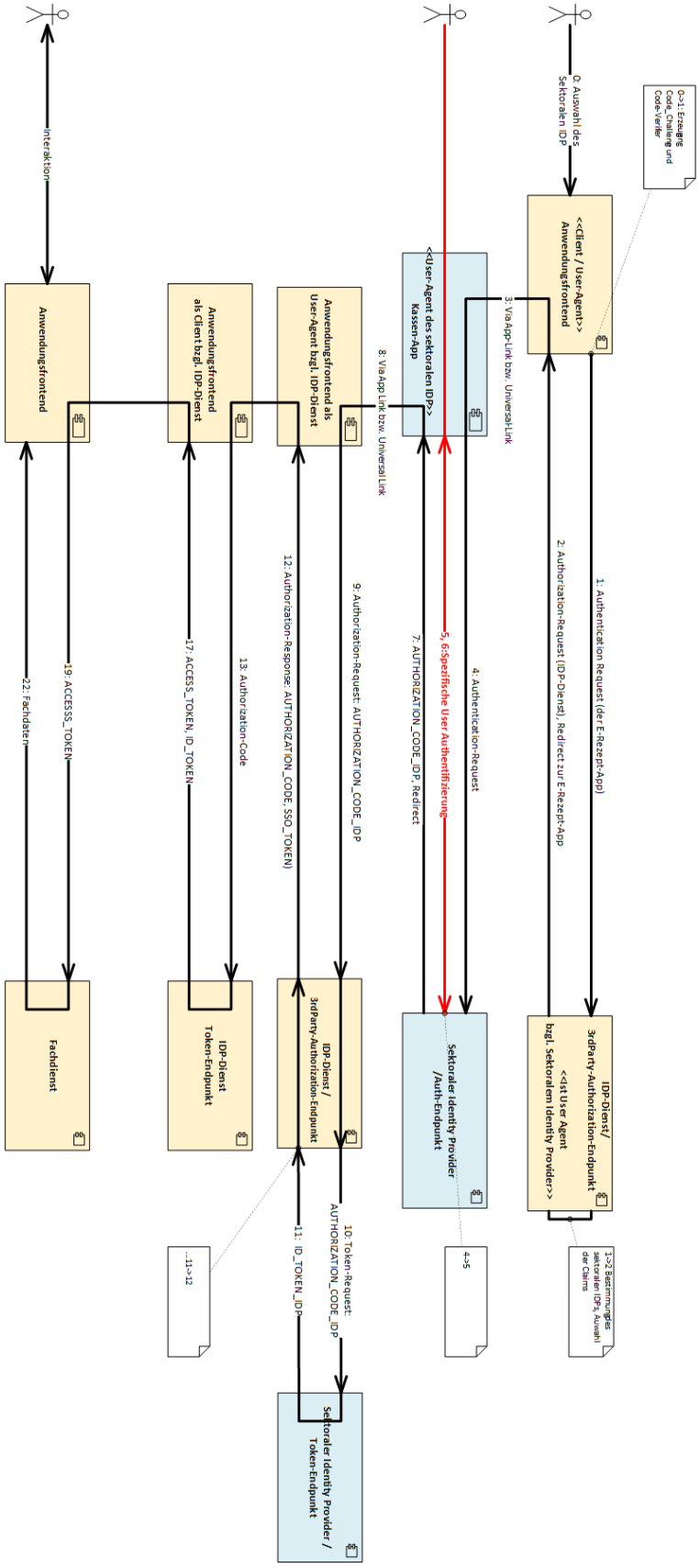

Abbildung 2: Ablauf der Transaktionen zwischen beteiligten Komponenten

Der gesamte Authentifizierungsprozess basiert im ersten Schritt aus Gründen der Entkoppelung zwischen den Authentifizierungsmethoden und Token-Formaten der sektoralen Identity Provider und des E-Rezept-FdV aus zwei ineinander geschachtelten OAuth2-Flows vom Typ "Authorization Code Grant".

Im äußeren Flow (Schritt 1) wendet sich das E-Rezept-FdV als Client initial an den IDP-Dienst und signalisiert diesem über einen zusätzlichen Parameter den zur Authentifizierung zu verwendenden sektoralen Identity-Provider. Der IDP-Dienst delegiert die Authentifizierung an das spezifische Authenticator-Modul des sektoralen IDP. Der IDP-Dienst tritt bzgl. des inneren Flows als Client auf. Der innere Flow beginnt mit der Token-Anfrage in Schritt 2 und endet mit Schritt 11, der Herausgabe eines ID-Token vom sektoralen Identity Provider an den IDP-Dienst. Anschließend integriert der IDP-Dienst die Informationen aus dem ID-Token in einen Authorization-Code, der an das E-Rezept-FdV zurückgegeben wird. Der äußere Flow endet mit der Herausgabe des Access-Token an das E-Rezept-FdV in Schritt 17. Der weitere fachliche Ablauf zum Einreichen der Token und zur Nutzung der Fachdaten und Prozesse ist anwendungsspezifisch.

Die Prozessschritte, welche notwendig sind, damit ein mobiles Anwendungsfrontend einen Token erhält, sind entsprechend der Abbildung:

0→1: Der Nutzer wählt eine zu nutzende Anwendung zur alternativen Authentisierung im Anwendungsfrontend aus. Das Anwendungsfrontend erzeugt sich einen "CODE_VERIFIER" [RFC7636 # section-4.1] und bildet darüber den Hash "CODE_CHALLENGE" mit dem Hash-Algorithmus S256 gemäß [RFC 7636 # section-4.2].

1: Das Anwendungsfrontend überträgt die "CODE_CHALLENGE" gemäß [RFC8252 # Anhang B] sowie einen Identifier für die gewählte Anwendung zur alternativen Authentisierung als Teil eines Authentication_Request an den Authorization-Endpunkt des IDP-Dienstes.

1→2: Der Authorization-Endpunkt des IDP-Dienstes bestimmt anhand des Identifier für den gewählten sektoralen Identity Provider die URL für dessen Authorization-Endpunkt und wählt die für diese Anfrage notwendigen Scopes aus. Bei dieser Anfrage kommt ebenfalls PKCE nach [RFC7636] zur Anwendung.

2: Dann antwortet der IDP-Dienst dem Anwendungsfrontend mit einem Redirect, der seine eigene Anfrage nach einem ID-Token an den Authorization-Endpunkt des gewählten sektoralen Identity Provider enthält.

3: Der Aufruf der im Redirect übermittelten URI durch das Anwendungsfrontend auf dem Gerät des Benutzers startet über einen App-Link bzw. Universal-Link die Authentisierung am gewählten Authenticator-Modul des sektoralen Identity Provider.

4: Das Authenticator-Modul des sektoralen Identity Provider stellt den Authentication_Request des IDP-Dienstes an den Authorization-Endpunkt des sektoralen Identity Provider.

4→5: Der Authorization-Endpunkt des sektoralen Identity Provider stellt entsprechend den angefragten Scopes einen Consent (Zustimmung des Nutzers zur Verarbeitung der angezeigten Daten) zusammen.

5: Der Authorization-Endpunkt des sektoralen Identity Provider überträgt die Consent-Abfrage und ggf. für die Authentisierung des Nutzers notwendige Daten zu seinem

Authenticator-Modul.

5→6: Das Authenticator-Modul des sektoralen Identity Provider fordert den Nutzer zur Consent-Freigabe und zur Authentisierung auf und führt diese nach den Verfahren des sektoralen Identity Provider durch.

6: Das Authenticator-Modul des sektoralen Identity Provider bestätigt dem sektoralen IDP die erfolgreiche Durchführung der Authentisierung.

Hinweis: Schritte 5 und 6 sind beispielhaft und werden durch dieses Dokument nicht spezifiziert.

6→7: Der Authorization-Endpunkt des sektoralen Identity Provider erstellt den "AUTHORIZATION_CODE_IDP".

7: Der Authorization-Endpunkt des sektoralen Identity Provider antwortet seinem Authenticator-Modul mit einem Redirect zum Anwendungsfrontend.

8: Das Authenticator-Modul des sektoralen Identity Provider ruft über einen App-Link bzw. Universal-Link entsprechend der Redirect-URL (und der in Schritt 3 zwischengespeicherten Adresse) das Authenticator-Modul des IDP-Dienstes im Anwendungsfrontend auf und übergibt den "AUTHORIZATION_CODE_IDP".

9: Das Anwendungsfrontend überträgt den "AUTHORIZATION_CODE_IDP" an den Authorization-Endpunkt des IDP-Dienstes.

10: Der Authorization-Endpunkt des IDP-Dienstes reicht den "AUTHORIZATION_CODE_IDP" beim Token-Endpunkt des sektoralen Identity Provider ein.

11: Der Authorization-Endpunkt des IDP-Dienstes erhält vom Token-Endpunkt des sektoralen Identity Provider einen "ID_TOKEN_IDP" mit den gewünschten Claims.

11->12: Der Authorization-Endpunkt des IDP-Dienstes prüft den "ID_TOKEN_IDP" und erzeugt, basierend auf den gefüllten Claims, einen eigenen "AUTHORIZATION_CODE".

12: Der Authorization-Endpunkt des IDP-Dienstes antwortet dem Authenticator-Modul des IDP-Dienstes im Anwendungsfrontend und überträgt ihm den "AUTHORIZATION_CODE" sowie einen SSO_TOKEN.

12->13: Das Authenticator-Modul des IDP-Dienstes überträgt den "AUTHORIZATION_CODE" zum Anwendungsfrontend.

Ab diesem Punkt verläuft der Prozess ohne Anpassungen wie in der bisherigen Implementierung zwischen E-Rezept-App und IDP-Dienst.

13: Das Anwendungsfrontend erzeugt sich einen AES256-"Token Key", verknüpft ihn mit dem "CODE_VERIFIER" zum "KEY_VERIFIER" und sendet diesen unter Nutzung des öffentlichen Schlüssels PUK_IDP_ENC verschlüsselt zusammen mit dem "AUTHORIZATION_CODE" zum Token-Endpunkt des IDP-Dienstes.

14: Der Token-Endpunkt entschlüsselt den "AUTHORIZATION_CODE" und validiert ihn anhand des öffentlichen Schlüssels "PUK_IDP_SIG" des Authorization-Endpunktes.

15: Der Token-Endpunkt entschlüsselt und validiert den "KEY_VERIFIER", entnimmt aus

diesem den "CODE_VERIFIER" und gleicht diesen mit der "CODE_CHALLENGE" aus dem "AUTHORIZATION_CODE" ab.

16: Der Token-Endpunkt erzeugt die erforderlichen Token, signiert sie mit seinem privaten Schlüssel "PrK_IDP_SIG" und verschlüsselt sie mit dem "Token Key" des Anwendungsfrontend, welchen er dem "KEY_VERIFIER" entnimmt.

17: Der Token-Endpunkt überträgt ACCESS_TOKEN und ID_TOKEN an das Anwendungsfrontend.

18: Das Anwendungsfrontend entschlüsselt die Token mit seinem "Token Key" und prüft die Token-Signatur anhand des öffentlichen Schlüssels "PUK_IDP_SIG" des Token-Endpunktes.

19: Das Anwendungsfrontend reicht das gültige "ACCESS_TOKEN" auf Anwendungsebene verschlüsselt beim Fachdienst ein.

20: Der Fachdienst entschlüsselt das "ACCESS_TOKEN" entsprechend dem für diese Anwendung vorgesehenen Verfahren.

21: Der Fachdienst validiert das "ACCESS_TOKEN" anhand des öffentlichen Schlüssels "PUK_TOKEN" des Token-Endpunktes.

22: Der Fachdienst zieht die Claims (d. h. die Key/Value-Paare im Payload eines Token) aus dem "ACCESS_TOKEN" und gibt bei positiver Validierung den Zugriff auf die Fachdaten frei.

2.3 Ausblick auf die weitere Entwicklung

Im Rahmen der kontinuierlichen Erweiterung der Vorgaben für sektorale Identity Provider innerhalb der TI werden diese weiter angepasst werden. Dies beinhaltet Festlegungen zur Einführung einer Föderation der Identity Provider, die Unterstützung weiterer Anwendungen und Nutzungsszenarien, Vorgaben für zulässige Authentisierungsverfahren auf unterschiedlichen Vertrauensniveaus, sowie die mögliche Einführung weiterer Endpunkte entsprechend [openid-connect-core].

3 Zerlegung des Produkttyps

Der Produkttyp besteht aus einer zentralen Komponente (sektoraler Identity Provider). Diese wird bei der Durchführung des Authentifizierungsprozesses vom Authenticator-Modul unterstützt. Das Authenticator-Modul übernimmt die Ausführung der Nutzerauthentisierung.

Der sektoraler Identity Provider stellt die zentralisierte Identitätsprüfung der auf die Fachdienste zugreifenden Nutzer bereit. Als weitere Teile der Gesamtlösung sind neben dem IDP-Dienst die Clients (Anwendungsfrontend/Primärsystem) und die Fachdienste zu nennen, auf denen Fachdaten für den Zugriff durch die Nutzer (z. B. Versicherte oder Bediener eines AVS, PVS oder KVS) bereitgestellt werden. Ein sektoraler Identity Provider bietet Fachdiensten seine Dienste an, auf welche Millionen Nutzer zeitgleich zugreifen. Eine wesentliche Ergänzung des IDP-Dienstes ist das Authenticator-Modul, welches auf den dezentralen Komponenten in den Praxen, Kliniken, Apotheken und bei den Versicherten betrieben wird.

4 Übergreifende Festlegungen

Der sektorale Identity Provider muss die folgenden übergreifenden Anforderungen erfüllen.

A_22233 - Produkt ist geeignet für Vertrauensniveau "substanziell" gemäß eIDAS-Verordnung
Der Hersteller des sektoralen Identity Provider MUSS sein Produkt so implementieren, dass ein Anbieter die Anforderungen der Verordnung (EU) Nr. 910/2014 bzw. der [TR-03107-1] an elektronische Identifizierungsmittel mit einem Vertrauensniveau von mindestens "substanziell" erfüllen kann.**[**<=**]**

A_22234 - Vertrauensniveau "substanziell" gemäß eIDAS-Verordnung
Der Anbieter des sektoralen Identity Provider MUSS für den angebotenen sektoralen Identity Provider die Anforderungen der Verordnung (EU) Nr. 910/2014 bzw. der [TR-03107-1] an elektronische Identifizierungsmittel mit einem Vertrauensniveau von mindestens "substanziell" erfüllen.**[**<=**]**

A_22329 - Entgegennahme von Sperrmeldungen
Der Anbieter des sektoralen Identity Provider MUSS Sperrmeldungen von Sperrberechtigten jederzeit entgegennehmen und das betroffene Authentisierungsmittel oder auch den gesamten Zugang des Nutzers daraufhin unverzüglich sperren lassen.**[**<=**]**

Die Durchführungsverordnung (EU) 2015/1502 [eIDAS 2015/1502] gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 [eIDAS 910/2014] legt die Mindestanforderungen an technische Spezifikationen und Verfahren für Vertrauensniveaus elektronischer Identifizierungsmittel fest. Die Vertrauensniveaus der [TR-03107-1] entsprechen im Wesentlichen den eIDAS LOA [TR-03107-1#Anhang A#Tabelle 13].

Die Anmeldung des elektronischen Identifizierungsmittels inklusive Identitätsnachweis und -überprüfung des Versicherten erfolgt durch die Attributbestätigende Stelle auf Grundlage der GKV-SV Richtlinie "Kontakt mit Versicherten" nach § 217f Abs. 4b SGB V.

Im Rahmen der Anbieterzulassung prüft der unabhängige Sicherheitsgutachter, dass die vom Anbieter verwendeten elektronischen Identifizierungsmittel die Mindestanforderungen des Vertrauensniveaus "substanziell" erfüllen.

Eine Notifizierung des elektronischen Identifizierungssystems, welches die elektronischen Identifizierungsmittel ausstellt, ist nicht gefordert. Ebenso ist nicht gefordert, dass der Anbieter ein qualifizierter oder nicht-qualifizierter Vertrauensdiensteanbieter gemäß Verordnung (EU) Nr. 910/2014 ist.

A_22235 - Information des Versicherten über Änderungen an Authentifizierungsfaktoren
Der Anbieter des sektoralen Identity Provider MUSS den Versicherten über Änderungen an Authentifizierungsfaktoren informieren.
Die Information des Versicherten kann dabei auch über die Attributbestätigende Stelle erfolgen, welche den Anbieter des sektoralen Identity Provider mit der Erstellung des elektronischen Identifizierungsmittels beauftragt hat.**[**<=**]**

Hinweis: Dies könnten z. B. Änderungen von E-Mail-Adressen, Mobilfunknummern, registrierten Geräten oder Kennwörtern sein.

A_22236 - Auskunft an Versicherten
Der Anbieter des sektoralen Identity Provider MUSS dem Versicherten auf dessen Verlangen Auskunft geben über

- erfolgte Zugriffe auf das elektronische Identifizierungsmittel des Versicherten und
- Änderungen der Authentifizierungsfaktoren des Versicherten.

[<=]

Hinweis: Die Auskunft des Versicherten kann auch über die Attributbestätigende Stelle erfolgen, der den Anbieter des sektoralen Identity Provider mit der Erstellung des elektronischen Identifizierungsmittels beauftragt hat.

A_22237 - Darstellen der Voraussetzungen für sicheren Betrieb des Produkts im Handbuch
Der Hersteller des sektoralen Identity Provider MUSS für sein Produkt im dazugehörigen Handbuch leicht ersichtlich darstellen, welche Voraussetzungen vom Betreiber und der Betriebsumgebung erfüllt werden müssen, damit ein sicherer Betrieb des Produktes gewährleistet werden kann.**[<=]**

A_22238 - Sicherer Betrieb des Produkts nach Handbuch
Der Anbieter eines sektoralen Identity Provider MUSS die im Handbuch des eingesetzten sektoralen Identity Provider beschriebenen Voraussetzungen für den sicheren Betrieb des Produktes gewährleisten.**[<=]**

A_22333 - Schutz der Attribute während des Transports
Der Anbieter des sektoralen Identity Provider MUSS sicherstellen, dass die von der Attributbestätigende Stelle enthaltenen personenbezogenen oder sensiblen Daten während des Transports von der Attributbestätigende Stelle zum sektoralen Identity Provider gegen Abhören, Manipulation und Replay-Angriffe geschützt werden.
[<=]

A_22334 - Verifikation des Versicherten vor erster Nutzung
Der Anbieter des sektoralen Identity Provider MUSS den Versicherten, mittels der von der Attributbestätigende Stelle im Auftrag übermittelten Verifikationsdaten vor der ersten Nutzung authentifizieren, um dessen digitale Identität zu aktivieren**[<=]**

4.1 Sicherheitsanforderungen für den operativen Betrieb

A_22239 - Schützenswerte Objekte
Der Anbieter eines sektoralen Identity Provider MUSS die folgenden kryptographischen Objekte als schützenswerte Objekte in seinem Sicherheitskonzept berücksichtigen: (a) Private Schlüssel, (b) Öffentlicher Schlüssel, (c) Öffentliche Schlüssel von registrierten Clients, (d) Datensätze zu den einzelnen Nutzern, (e) Authentisierungsinformationen von Sperrberechtigten, (f) Dokumentation über beauftragte und durchgeführte Sperrungen, (g) Statusinformationen, (h) Authentisierungsinformationen zur Authentisierung von internen Akteuren bzw. Rollen, (i) Protokolldaten, (j) Konfigurationsdaten.**[<=]**

A_22240 - Berücksichtigung OWASP-Top-10-Risiken
Der Anbieter des sektoralen Identity Provider MUSS Maßnahmen zum Schutz vor den zum Zulassungszeitpunkt aktuellen OWASP-Top-10-Risiken umsetzen und dokumentieren, wie es vorgesehen ist, ebenfalls auf die nach dem Zulassungszeitpunkt aktuellen OWASP-Top-10-Risiken zu reagieren.**[<=]**

Hinweis: Die Nichtanwendbarkeit eines OWASP-Top-10-Risikos ist zu begründen. Für Informationen zum Umgang mit den OWASP-Top-10-Risiken wird auf den aktuellen [OWASP Top 10 Report] und die darin enthaltenen Vorgehensweisen für z. B. Entwickler und Tester verwiesen.

A_22241 - Interner Datenaustausch der Komponenten des sektoralen Identity Provider
Der Anbieter eines sektoralen Identity Provider MUSS beim internen Datenaustausch die Integrität, Authentizität und Vertraulichkeit der Daten sichern.**[<=]**

A_22242 - Gesicherte externe Schnittstellen des sektoralen Identity Provider
Der Anbieter eines sektoralen Identity Provider MUSS für den Datenaustausch mit anderen Rollen und Diensten Mechanismen zur Sicherung der Datenintegrität, der Authentizität und der Vertraulichkeit der Daten zur Verfügung stellen. Hierzu gehören explizit die Schnittstellen vom Anbieter eines sektoralen Identity Provider zur Attributbestätigenden Stelle für die Übermittlung der Attribute bei der Einrichtung eines Nutzers sowie von Sperrinformationen.**[<=]**

A_22243 - Nutzung bestehender SGB-Datensätze bei Registrierung für Endanwender (Versicherte)
Der sektorale Identity Provider SOLL für die Registrierung der Endanwender die bestehenden Datensätze der Endanwender (Versicherte) beim Kostenträger verwenden, so wie sie im Rahmen der Vorgaben des Sozialgesetzbuches (SGB) erhoben wurden.**[<=]**

Der Kostenträger verantwortet als Attributbestätigende Stelle die Korrektheit dieser Daten. Eine erneute Identifizierung der Versicherten ist aufgrund der datenschutzrechtlichen Vorgaben nicht geboten.

A_22244 - Trennung der Betriebsumgebungen
Der Anbieter eines sektoralen Identity Provider MUSS sicherstellen, dass das Testsystem von dem Produktivsystem technisch, organisatorisch und betrieblich so getrennt wird, dass keine gegenseitige Beeinflussung und keine Verwechslung möglich sind. **[<=]**

A_22245 - Datenschutzgerechte Einrichtungs- und Sperrprozesse
Der Anbieter eines sektoralen Identity Provider MUSS die Einrichtungs- und Sperrprozesse datenschutzgerecht ausgestalten, d.h. insbesondere sind für die Verarbeitung der Antrags- und Sperrauftragsdaten die Datenschutzgrundsätze gemäß Art. 5 DSGVO zu berücksichtigen, sowie die technischen und organisatorischen Maßnahmen nach Art. 25 und Art. 32 DSGVO zu treffen.**[<=]**

A_22246 - Löschung von Nutzerinformationen
Der Anbieter eines sektoralen Identity Provider MUSS die Attributsdaten und Sperraufträge zu einem Nutzer unverzüglich löschen, sobald die gesetzlichen oder vertraglichen Aufbewahrungsfristen erreicht sind.**[<=]**

A_22247 - Fehlerprotokollierung
Falls es erforderlich sein sollte, dass der Anbieter eines sektoralen Identity Provider eine Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung durchführt, MÜSSEN die Protokolldaten entsprechend des Datenschutzgrundsatzes der Datenminimierung gemäß Art. 5 Abs. 1 Satz 1 lit.c) DSGVO unter Berücksichtigung der Art. 25, 32 DSGVO derart gestaltet sein, dass nur personenbezogene Daten in der Art und dem Umfang enthalten sind, wie sie zur Behebung erforderlich sind.**[<=]**

Der sektorale Identity Provider wird für Anfragen des IDP-Dienstes und seines Authenticator-Moduls über das Internet erreichbar gemacht. Die folgenden Anforderungen beschreiben die für diesen Netzübergang erforderlichen Sicherheitsmechanismen. Für den Netzübergang aus dem Internet als Transportnetz zum sektoralen Identity Provider-Dienst ist ein Paketfilter erforderlich.

A_22248 - Richtlinien für den Paketfilter zum Internet
Der Anbieter eines sektoralen Identity Provider MUSS beim Paketfilter die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf das HTTPS- Protokoll beschränken. **[<=]**

A_22249 - Verhalten bei Vollauslastung
Der Anbieter eines sektoralen Identity Provider MUSS den Paketfilter so konfigurieren, dass bei Vollauslastung der Systemressourcen im sektoralen Identity Provider keine weiteren Verbindungen angenommen werden.**[<=]**

Hinweis: Durch die Zurückweisung von Verbindungen wird sichergestellt, dass Clients einen Verbindungsaufbau mit einer anderen Instanz des Dienstes versuchen, bei der die erforderlichen Systemressourcen zur Verfügung stehen.

A_22250 - Schutz der Verbindung zum sektoralen Identity Provider
Der Anbieter eines sektoralen Identity Provider MUSS sicherstellen, dass die Schnittstellen des sektoralen Identity Provider nur über eine gegen Abhören, Manipulation und Replay-Angriffe geschützte Verbindung genutzt werden können.**[<=]**

4.2 Registrierung der Authenticator-Module

Zur Anmeldung ruft das Anwendungsfrontend ein separates Authenticator-Modul des sektoralen Identity Provider auf. Dieser Aufruf wird vom IDP-Dienst vermittelt und dazu muss das Authenticator-Modul zuvor dem IDP-Dienst bekannt gemacht werden.

A_22251 - Registrierungsdaten beim IDP-Dienst
Der Anbieter des sektoralen Identity Provider MUSS alle unterstützten Authenticator-Module mit der auf dem Gerät registrierten Adresse (kk_app_uri), einem vom Benutzer interpretierbaren Namen (kk_app_name) und einer Referenz auf den verknüpften sektoralen Identity Provider (idp_iss) auf organisatorischem Weg beim IDP-Dienst bekanntmachen.

kk_app_name	kk_app_id	kk_app_uri	idp_iss
Name der Krankenkasse/Kassen-App, zur Anzeige in der E-Rezept-App (max. 128 Zeichen)	eindeutiger interner Identifier der anzufragenden App, wird durch IDP-Dienst festgelegt	aufzurufende URI für die Authentisierung	iss-Wert des sektoralen Identity Provider

[<=]

A_22272 - Registrierungsdaten des IDP-Dienstes
Der Anbieter des sektoralen Identity Provider MUSS für die registrierte Client-ID des IDP-Dienstes die verwendeten redirect-Adressen aller unterstützen sektoralen Authenticator-Module als verknüpfte "redirect_uri" pflegen.**[<=]**

Diese Registrierung ist notwendig, weil die Authenticator-Module die Anfrage an den sektoralen Identity Provider im Namen des IDP-Dienstes, aber mit ihrer eigenen redirect-Adresse stellen können. So können sie die Fehlerbehandlung unabhängig von der konkreten internen Realisierung selbst durchführen.

A_22353 - Ermöglichung einer organisatorischen Registrierung
Der Anbieter des sektoralen Identity Provider MUSS eine organisatorische Registrierung des IDP-Dienstes sowie von Anwendungsfrontends und Fachdiensten ermöglichen.**[<=]**

4.3 Identifikation des Clientsystems

A_22252 - Erkennung Clientsystem User-Agent
Der sektorale Identity Provider MUSS das vom aufrufenden Nutzer verwendete Clientsystem erkennen und in den Einträgen zur Performance-Rohdatenerfassung gemäß [gemSpec_Perf] protokollieren. Der sektorale Identity Provider MUSS bei fehlendem Information über das Client System den Request mit dem HTTP-Status-Code 403 beantworten, damit in der Betriebsüberwachung des sektoralen Identity Provider die Nutzung unzulässiger Clientsysteme erkannt werden kann.**[<=]**

Hinweis: Die Information über das Client System kann anhand des im HTTP-Request enthaltenen Header-Feld "User-Agent" gemäß [RFC7231] übermittelt werden.

A_22253 - Ausschluss bestimmter Clientsystem-Versionsnummern von der Kommunikation
Der sektorale Identity Provider MUSS die aus dem Internet vom Clientsystem mitgeteilte Versionsnummer erkennen und festgelegte Versionsnummern über ein Blocklisting von einer Kommunikation ausschließen können. Der sektorale Identity Provider MUSS in diesen Fällen eine entsprechende Fehlermeldung an das Clientsystem geben.**[<=]**

A_22254 - Ausschluss von Clientsystem-Versionen
Der sektorale Identity Provider MUSS auf Anweisung der gematik Clientsysteme mit bestimmten Versionsnummern von einer Kommunikation mit dem sektoralen Identity Provider ausschließen können.**[<=]**

5 Funktionsmerkmale

5.1 Authorization Server Metadata (Discovery Document)

A_22255 - Inhalt des Discovery Document des sektoralen Identity Provider
Der sektorale Identity Provider MUSS in seinem Discovery Document gemäß [RFC8414 # section-2 / OpenID Connect Discovery #3] mindestens die folgenden Metadaten und Werte aufnehmen und dieses im Internet verfügbar machen:

issuer	**URL**	
authorization_endpoint	URI des Authorization-Endpunktes gemäß [RFC6749]	
token_endpoint	URI des Token-Endpunktes gemäß [RFC6749]	
jwks_uri	URL	Schlüssel für die Signatur der ID_Token
subject_types_supported	[public]	weitere Werte sind möglich
id_token_signing_alg_values_supported	[ES256]	weitere Werte sind möglich
response_types_supported	[code]	weitere Werte sind möglich
scopes_supported	[openid, erp_sek_auth]	weitere Werte sind möglich
response_modes_supported	[query]	
grant_types_supported	[authorization_code]	
token_endpoint_auth_methods_supported	[private_key_jwt]	weitere Werte sind möglich

claims_parameter_supported	[false]	Die Unterstützung des Claims-Parameter ist nicht notwendig.
code_challenge_methods_supported	[S256]	weitere Werte sind möglich

[<=]

A_22256 - Vorlaufzeit bei geplantem Schlüsselwechsel
Der Anbieter des sektoralen Identity Provider MUSS Signaturschlüssel im Rahmen eines geplanten Schlüsselwechsels mindestens 3 Stunden vor Verwendung in seinem jwks-Schlüsselsatz veröffentlichen.**[<=]**

A_22354 - Discovery Document - Prüfung der angebotenen URLs
Der sektorale Identity Provider MUSS alle von ihm im Discovery Document angebotenen URLs stündlich auf bloße Erreichbarkeit prüfen.**[<=]**

5.2 Authorization-Endpunkt

5.2.1 Anforderungen an die Authentisierung der Nutzer

Für die Anwendung E-Rezept gelten die im Folgenden dargestellten Vorgaben. Die Möglichkeit der Authentisierung nach diesen Kriterien ist auf den 31.12.2022 befristet. Eine erneute Bewertung der Frist und der technischen Möglichkeiten erfolgt spätestens in Q4/2022 in Abstimmung mit dem BSI.

A_22257 - Operationsaufruf erfordert erfolgreiche Authentifizierung
Der sektorale Identity Provider MUSS sicherstellen, dass Authorization Requests nur nach vorheriger erfolgreicher Authentifikation des Nutzers mit einem "AUTHORIZATION_CODE" beantwortet werden.**[<=]**

A_22258 - Authentifikationsverfahren genügen Vertrauensniveau "substanziell"
Der Anbieter eines sektoralen Identity Provider MUSS sicherstellen, dass nur Authentifikationsverfahren genutzt werden, die vom BSI in der [TR-03107-1] für ein Vertrauensniveau von mindestens "substanziell" als geeignet eingestuft werden.**[<=]**

A_22345 - Maximale Gültigkeit einer Authentifikation
Der sektorale Identity Provider MUSS sicherstellen, dass nach erfolgreicher Authentifikation des Nutzers die Session maximal 12 Stunden ohne erneute Authentifikation gültig bleibt.**[<=]**

5.2.2 Schnittstelle Authenticator-Modul

Es können je sektoralem Identity Provider ein oder mehrere Authenticator-Module existieren, welche die Authentisierung des Benutzers durchführen. Über die generellen Vorgaben zum Authentifizierungsverfahren hinaus werden hier keine funktionalen

Vorgaben gemacht. Lediglich die Schnittstellen zum Aufruf durch das Authenticator-Modul des IDP-Dienstes sowie zur Rückgabe der Antwort werden festgelegt. Beide Kommunikationen erfolgen über direkte App-2-App-Kommunikation auf dem Endgerät des Benutzers.

5.2.3 Anforderungen an Authenticator-Module sektoraler Identity Provider

A_22274 - Authenticator-Module: HTTP-Header user-agent
Authenticator-Module des sektoralen Identity Provider MÜSSEN in alle HTTP-Requests den HTTP-Header user-agent befüllen, um dem sektoralen Identity Provider die Möglichkeit zu geben, die Version des Clients zu identifizieren.**[**<=**]**

A_22276 - Authenticator-Module: Anzeige des "user_consent"
Authenticator-Module des sektoralen Identity Provider MÜSSEN die Willenserklärung des Nutzers einholen, zur Übermittlung seiner in den Claims angeforderten Daten zum IDP-Dienst.**[**<=**]**

Hinweis: Die erfolgte Zustimmung des Nutzers darf gespeichert werden und weitere Abfragen können entfallen.

A_22277 - Authenticator-Module: Schutz vor überalterter Software
Der Anbieter des sektoralen Identity Provider MUSS dafür Sorge tragen, dass die von ihm in App Stores veröffentlichten Authenticator-Module bei Änderungen automatisiert aktualisiert werden.**[**<=**]**

A_22273 - Freischaltung vorzeitig beenden
Authenticator-Module des sektoralen Identity Provider MÜSSEN dem Nutzer die Möglichkeit bieten, seine Sitzung (die des Authenticator Moduls mit dem sektoralen IDP) explizit zu beenden, sodass beim nächsten Token Request durch diesen Nutzer eine erneute Authentisierung erforderlich ist.**[**<=**]**

Hinweis: Sitzungen am zentralen IDP-Dienst werden von dieser Anforderung nicht betroffen.

Im Fall der Wahl eines Authenticator-Moduls durch den Nutzer, das nicht auf dessen Endgerät installiert ist, erfolgt ein Aufruf der am zentralen IDP-Dienst hinterlegten URL durch einen Webbrowser des Endgerätes.

A_22306 - Information des Nutzers bei fehlender Installation des gewählten Authenticator-Moduls
Der Anbieter des sektoralen Identity Provider MUSS auf der unter `redirect_uri` des Authenticator-Moduls erreichbaren Webseite darstellen, aus welcher Quelle das jeweilige Authenticator-Modul des sektoralen Identity Provider zu beziehen ist, auf welchen Geräten/Plattformen er installiert werden kann und welche Voraussetzungen für die Verwendung zur Authentifizierung zu erfüllen sind (z. B. erforderliche Registrierungsprozeduren beim Anbieter des sektoralen Identity Provider).**[**<=**]**

5.2.4 Zusammenspiel von Authenticator-Modulen des IDP-Dienstes und des sektoralen Identity Provider

Im Kontext der vorliegenden Spezifikation wird angenommen, dass zu einem sektoralen Identity Provider-Dienst mindestens ein dediziertes Authenticator-Modul existiert, welches in der Lage ist, die Authentifizierung eines Nutzers zu übernehmen, d. h. den Nutzer mit spezifischen Methoden gegenüber dem sektoralen Identity Provider-Dienst zu

authentifizieren und eine hiernach vom sektoralen Identity Provider-Dienst produzierte Attestierungen in Form eines Authorization_Code über das Authenticator-Modul an den anfragenden IDP-Dienst zurückzugeben. Unter einem sektoralen Authenticator-Modul werden hierbei eigenständige Anwendungen auf dem Endgerät des Benutzers verstanden. Die Delegierung der Authentifizierung an ein Authenticator-Modul und den zugehörigen sektoralen Identity Provider erfolgt auf Initiative des Nutzers.

Zur Realisierung des in Abschnitt 2.2 definierten Flows einschließlich der hierbei erforderlichen Übergabe des Authorization_Code und anderer Daten, bedürfen eines wechselseitigen Aufrufs zwischen dem Authenticator-Modul des IDP-Dienstes und dem gewählten Authenticator-Modul des sektoralen Identity Provider. Dies wird im folgenden als App2App-Kommunikation bezeichnet (siehe [RFC8252], Abschnitt "7.2. Claimed "https" Scheme URI Redirection", https://datatracker.ietf.org/doc/html/rfc8252#section-5). Die genaue Interaktionsform ist von den Spezifika des verwendeten Betriebssystems abhängig. Der folgende Abschnitt definiert Anforderungen an:

- die zur Verfügung zu stellenden Registrierungsdaten der E-Rezept-App (z. B. die Adressierung),
- die zur Verfügung zu stellenden Registrierungsdaten des Authenticator-Moduls auf dem Endgerät,
- die Interaktion zwischen E-Rezept-App und einem Authenticator-Modul.

Aufgrund der genannten Abhängigkeiten sind zu den folgenden Anforderungen jeweils die geforderten Ausgestaltungen für Android und iOS genannt. Bei beiden Betriebssystemen werden Apps - analog zu web-basierten Anwendungen - über URLs adressiert, die von den installierten Apps beansprucht werden. Die Eindeutigkeit der Zuordnung zwischen URL und App wird in beiden Fällen durch Daten innerhalb der Distribution und unter der URL abrufbaren Informationen hergestellt (sog. Asset-Link-Dateien im Fall von Android bzw. Apple-App-Site-Association-Dateien im Fall Apple/iOS).

Sicherheitsziele:

- Die Auswahl eines sektoralen Identity Provider und einem zugeordneten Authenticator-Modul obliegt dem Nutzer.
- Die Auswahl beschränkt sich auf solche sektorale Identity Provider und Authenticator-Module, die aus Sicht der Fachanwendung E-Rezept als vertrauenswürdig zum Zweck der Authentifizierung angesehen werden.
- Das E-Rezept-FdV muss in Kombination mit Betriebssystem-Mechanismen und dem zentralen IDP-Dienst sicherstellen, dass ausschließlich das zugehörige Authenticator-Modul des vom Nutzer gewählten sektoralen Identity Provider verwendet wird.
- Authenticator-Module der sektoralen Identity Provider müssen sicherstellen, dass im Zuge der Authentifizierung erstellte Authorization Codes nach Abschluss der Authentifizierung ausschließlich an die aufrufende Anwendung übergeben werden.

A_22278 - Realisierung der App2App-Kommunikation im Fall Android
Im Kontext von Android-Anwendungen MÜSSEN Authenticator-Module zu sektoralen Identity Providern und das E-Rezept-FdV für die wechselseitige Verlinkung den unter [ANDROIDAPPLINKS] beschriebenen App-Link-Mechanismus verwenden.**[<=]**

A_22279 - Realisierung der App2App-Kommunikation im Fall Apple/iOS
Im Kontext von iOS-Anwendungen MÜSSEN Authenticator-Module zu sektoralen Identity Providern und das E-Rezept-FdV für die wechselseitige Verlinkung den unter [APPLEUNIVERSAL] beschriebenen Universal-Link-Mechanismus verwenden. **[<=]**

5.2.4.1 Anforderungen an Authenticator-Module sektoraler Identity Provider zur App2App-Kommunikation

A_22305 - Serverseitige Registrierungsdaten
Anbieter von sektoralen IDP-Diensten MÜSSEN sicherstellen, dass die durch das Betriebssystem notwendigen Voraussetzungen für die Funktionsfähigkeit ihres Authenticator-Moduls erfüllt sind (z.B. Registrierung der Anwendung zur App2App-Kommunikation entsprechend der Mechanismen unter [ANDROIDAPPLINKS] bzw. [APPLEUNIVERSAL] zur Verknüpfung der Anwendung mit einer Webseite).**[**<=**]**

5.2.5 Anforderung an die Interaktion zum Authenticator-Modul des IDP-Dienstes

A_22275 - Authenticator-Module: Übergabe des Authorization Request an den Authorization-Endpunkt
Authenticator-Module des sektoralen Identity Provider MÜSSEN den Authorization Request, welchen sie mittels App2App-Kommunikation vom Authenticator-Modul des IDP-Dienstes erhalten, TLS-verschlüsselt an den Authorization Server des sektoralen Identity Provider weiterleiten.
Mit Ausnahme der `redirect_uri` MÜSSEN alle Parameter des Authorization Request dabei unverändert bleiben.**[**<=**]**

Anstelle der `redirect_uri` des IDP-Dienstes kann das Authenticator-Modul eine eigene Adresse einfügen, um die Fehlerbehandlung unabhängig von der konkreten internen Realisierung selbst durchführen zu können.

A_22307 - "redirect_uri" beim Authorization Request zum sektoralen Identity Provider
Authenticator-Module des sektoralen Identity Provider KÖNNEN beim Aufruf des sektoralen Identity Provider den Parameter "`redirect_uri`" mit der URL belegen, unter der sie selber im Betriebssystem registriert sind.**[**<=**]**

A_22308 - Beschränkung des Authenticator-Moduls eines sektoralen Identity Provider auf die Authentifizierung
Authenticator-Module von sektoralen Identity Providern DÜRFEN bei Aufruf durch das Anwendungsfrontend KEINE anderen Funktionalitäten anbieten, als solche die direkt oder indirekt zur Authentifizierung des Nutzers dienen (z.b. Einrichtung, Registrierung, dafür relevante Informationen). Insb. Werbung für andere Leistungen oder Funktionen DARF NICHT angezeigt werden.**[**<=**]**

A_22309 - Absicherung des Aufrufs zum Authenticator-Modul des IDP-Dienstes
Authenticator-Module von sektoralen Identity Providern MÜSSEN für Aufrufe zum Authenticator-Modul des IDP-Dienstes die Verifikationsmechanismen des Betriebssystems verwenden und dazu die folgenden Parameter setzen:
Android: Keine weiteren.
iOS: .universalLinksOnly:true**[**<=**]**

A_22310 - Übergabe des Authorization Code an das Authenticator Modul des IDP-Dienstes
Authenticator-Module von sektoralen Identity Providern MÜSSEN bei Aufruf des Authenticator-Moduls des IDP-Dienstes die vom sektoralen Identity Provider erhaltenen Daten (state und AUTHORIZATION_CODE) sowie den Parameter

"kk_app_redirect_uri" übergeben. Dieser ist mit dem Wert der "redirect_uri" des zugehörigen Aufrufs an den sektoralen Identity Provider zu befüllen.**[**<=**]**

A_22311 - Verwendung der ursprünglichen Adresse zur Übergabe des Authorization_Code
Authenticator-Module von sektoralen Identity Providern MÜSSEN die bei der Übergabe des Authorization-Request erhaltene redirect_uri für die Übergabe des Authorization_Code verwenden. Außer für diesen Aufruf DARF er NICHT an andere Anwendungen übergeben werden.**[**<=**]**

5.2.6 Schnittstelle Authorization-Endpunkt

Ein Client liefert seine Anfrage über das Authenticator-Modul an den Authorization-Endpunkt des sektoralen Identity Provider.

Inhalt der Anfrage ist:

- die "`redirect_uri`", an welche der Authorization Request beantwortet werden soll.
- die eigene Hersteller-ID, Programmkürzel und Versionsnummer (im HTTP-Header-Feld "User-Agent").
- der über das eigene "`CODE_VERIFIER`" [RFC7636 # section-4.1] gebildete HASH "`code_challenge`" [RFC7636 # section-4.2] mit Angabe des Algorithmus "`code_challenge_method`" [RFC7636 # section-4.3] entsprechend dem gewählten Authorization Code Flow (response_type=code).
- der "`STATE`"-Parameter [RFC8252 # section-8.9] wird genutzt, um CSRF (Cross-Site-Request-Forgery) zu verhindern.
- der "scope" der Anfrage, welcher einen definierten Satz von benötigten Attributen für die entsprechende Anwendung beinhaltet.

A_22312 - Einhaltung der Standards bei der Realisierung des Authorization-Endpunkts
Der sektorale Identity Provider MUSS die Schnittstelle "Authorization-Endpunkt" gemäß [RFC6749 "The OAuth 2.0 Authorization Framework"] und [RFC8252 "OAuth 2.0 for Native Apps"] und weiteren darin festgelegten Standards implementieren. Hierbei MÜSSEN nur im Rahmen der gemSpec_IDP_Sek relevante Aspekte (Authorization Code Flow ohne User Info Endpoint) berücksichtigt werden.**[**<=**]**

5.2.6.1 Authorization Server Eingangsdaten

A_22297 - Annahme des Authorization Request durch sektoralen IDP
Der sektorale Identity Providert MUSS die im Authorization Request des Authenticator-Moduls korrekt mitgelieferten Parameter State, "CODE_CHALLENGE" und "SCOPE" annehmen.**[**<=**]**

Hinweis: Der Aufbau der Anfrage entspricht [gemSpec_IDP_Dienst#Kapitel 7.1 Authorization Request], jedoch mit dem Scope "erp_sek_auth+openid".

A_22315 - Prüfung der "redirect_uri" durch sektoralen IDP
Der sektorale Identity Provider MUSS bei Erhalt eines Authorization Request die enthaltene "redirect_uri" gegen die eines der bekannten Authenticator-Module auf Gleichheit prüfen. Stimmen diese nicht überein, MUSS die weitere Verarbeitung mit einem Fehler-Response abgebrochen werden (vgl. https://openid.net/specs/openid-connect-core-1_0.html#AuthError).**[<=]**

Hinweis: Nach [openid-connect-core-1_0.html # AuthRequest] ist es zulässig, dass ein Client mehrere "redirect_uri" bei der Registrierung hinterlegt. Der sektorale Identity Provider muss laut der OIDC-Spezifikation prüfen, ob die im Request gelieferte "redirect_uri" mit exakt einer der hinterlegten "kk_app_redirect_uri" übereinstimmt. Die Prüfung muss über eine 'Simple String Comparison' nach [RFC3986#section-6.2.1] erfolgen.

5.2.7 Authorization-Endpunkt Ausgangsdaten

Sind alle im Scope geforderten Attribute vorhanden und die Gültigkeit der Attribute geprüft sowie eine erfolgreiche Authentifizierung des Nutzers erfolgt, erstellt der Authorization-Endpunkt einen "AUTHORIZATION_CODE" und sendet diesen an das Anwendungsfrontend.

A_22324 - Verwendung des Attributes "state" durch sektoralen IDP
Der Authorization-Endpunkt des sektoralen Identity Provider MUSS den "state"-Parameter [RFC6749 # section-10.12] der Anfrage in allen darauf basierenden Responses verwenden.**[<=]**

A_22325 - Senden des "AUTHORIZATION_CODE" an das Authenticator-Modul
Der sektorale Identity Provider MUSS den "AUTHORIZATION_CODE" und den "state" der Anfrage zur Weiterleitung an sein Authenticator-Modul senden.**[<=]**

5.3 Token-Endpunkt

Der Token-Endpunkt des sektoralen Identity Provider nimmt die Anfrage des zentralen IDP-Dienstes entgegen und prüft neben deren Integrität, ob der eingereichte "CODE_VERIFIER" bei Nutzung des Hash-Verfahrens S256 (nach [RFC7636 # section-4.2]) zum bitgleichen Hash-Wert führt. Stimmt der Hash-Wert aus dem initialen Aufruf über das Authenticator-Modul - die "CODE_CHALLENGE" - mit dem gebildeten Hash-Wert überein, ist sichergestellt, dass Aufrufer und Initiator identisch sind. Der Token-Endpunkt gibt daraufhin das"ID_TOKEN" an den IDP-Dienst heraus.

5.3.1 Token-Endpunkt Eingangsdaten

A_22320 - Annahme von AUTHORIZATION_CODE und CODE_VERIFIER
Der Token-Endpunkt des sektoralen Identity Provider MUSS die vom IDP-Dienst übertragenen AUTHORIZATION_CODE und CODE_VERIFIER annehmen.**[<=]**

A_22321 - Prüfung des CODE_VERIFIER
Der Token-Endpunkt des sektoralen Identity Provider MUSS die Überprüfung des CODE_VERIFIER gegen die CODE_CHALLENGE mit S256 (Algorithmus nach [RFC7636 # section-4.2]) durchführen.**[<=]**

A_22322 - Prüfung "private_key_jwt"
Der Token-Endpunkt des sektoralen Identity Provider MUSS den im "client_assertion"-Parameter übertragenen "private_key_jwt" wir folgt überprüfen:

- Der Parameter "iss" MUSS der Client-ID des registrierten IDP-Dienstes entsprechen.
- Der Parameter "aud" MUSS der Issuer-URL des jeweiligen sektoralen IDP entsprechen.
- Die aktuelle Zeit MUSS kleiner als der im Parameter "exp" angegebene Zeitpunkt sein.
- Der identische "private_key_jwt" (jti Claim) darf nicht bereits eingereicht worden sein (Replay-Schutz).

[<=]

A_22323 - Protokollierung der Token-Ausgabe in allen Fällen
Der Token-Endpunkt des sektoralen Identity Provider MUSS im Positivfall die Herausgabe der Token und im Negativfall die Token-Anfrage protokollieren.**[<=]**

Das Protokoll wird intern und ggf. für Audits verwendet.

5.3.2 Token-Endpunkt Ausgangsdaten

A_22316 - Maximale Gültigkeitsdauer von ID_TOKEN
Der sektorale Identity Provider DARF ID_TOKEN mit einer Gültigkeitsdauer von mehr als 300 Sekunden (5 Minuten) NICHT ausstellen.**[<=]**

A_22317 - Claims der ID_TOKEN des sektoralen Identity Provider
Der sektorale Identity Provider MUSS ID_TOKEN mit den folgenden Claims befüllen:

- given_name: Vorname des Nutzers, maximal 64 Zeichen,
- family_name: Nachname des Nutzers, maximal 64 Zeichen,
- organization_number: IK-Nummer der Kasse, maximal 64 Zeichen,
- idNummer: unveränderlicher Teil der KVNR des Nutzers, 10 Zeichen

[<=]

A_22318 - ID-Token des sektoralen Identity Provider
Der sektorale Identity Provider MUSS nach erfolgreicher Prüfung des erhaltenen Authorization-Code ein ID-Token mit den angefragten Claims ausstellen. Das ID-Token MUSS die zuvor übermittelte Nonce enthalten. Das ID-Token MUSS an den IDP-Dienst zurückgegeben werden.**[<=]**

A_22319 - Signatur des ID-Token des sektoralen Identity Provider
Der sektorale Identity Provider MUSS selbst erstellte ID-Token unter Verwendung eines privaten Schlüssels der im Discovery Document unter "jwks_uri" referenzierten öffentlichen Schlüssel signieren. Das zu verwendende Verfahren MUSS ECDSA auf Basis der NIST-Kurve P-256 sein (vergleiche https://openid.net/specs/draft-jones-json-web-signature-04.html#DefiningECDSA).**[<=]**

6 Anhang A – Verzeichnisse

6.1 Abkürzungen

Kürzel	Erläuterung
AVS	Apothekenverwaltungssystem (ein Primärsystem)
FdV	Frontend des Versicherten
KVS	Krankenhausverwaltungssystem (ein Primärsystem)
PVS	Praxisverwaltungssystem (ein Primärsystem)
SGB	Sozialgesetzbuch

6.2 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 Repräsentation kann als JSON Web Token erfolgen.
AES256	Der Advanced Encryption Standard (AES) ist eine kryptographische Blockchiffre. AES256 bezeichnet deren Anwendung mit einer Schlüssellänge von 256Bit.
Anwendungsfrontend	Die Applikation durch welche ein Nutzer die Dienste einer Anwendung der Telematikinfrastruktur wie etwa das E-Rezept nutzt.
App2App-Kommunikation	Eine direkte Nachrichtenübertragung zwischen zwei Anwendungen auf einem Endgerät, welche durch Mechanismen des Betriebssystems ermöglicht wird.
Authenticator-Modul	Komponente, durch welche der Nutzer die Authentifizierung gegenüber dem Identity Provider vornimmt.
Authentifizierung des Nutzers am Gerät oder lokale Authentifizierung	Authentifizierungsmittel des Nutzers zur Nutzung eines Kontos auf einem Mobilgerät.

Authentifizierungszertifikat	Unter einem Authentifizierungszertifikat werden Kontext der Registrierung und Verwendung von alternativen Authentisierungsmittel-Zertifikate vom Typ C.CH.AUT der eGK verstanden.
Authorization-Endpunkt	Der Authorization-Endpunkt führt nach der initialen Anfrage die Authentifizierung des Nutzers durch und stellt einen Authorization_Code aus, welcher zum Abrufen der eigentlichen Token verwendet wird.
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 Token für den vom Resource Owner erlaubten Anwendungsbereich (Scope) für einen Resource Server bzw. eine auf einem Resource Server existierende Protected Resource aus.
Autorisierte Anwendung eines Schlüssels	Anwendung eines kryptographischen Schlüssels auf Daten durch einen berechtigten Nutzer.
Betriebssystem (oder Plattform)	Der Name des Betriebssystems eines Geräts.
Besitz (eines Geräts)	Verwendungshoheit eines Nutzers über ein Mobilgerät.
Blocklisting	Das führen einer Liste von Eigenschaften, welche definieren, unter welchen Umständen Anfragen am Dienst abgelehnt werden.
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. Im Fokus der aktuellen Spezifikationen liegt jedoch allein die Kommunikation mit dem E-Rezept-FdV.
Consent	Zustimmung des Nutzers zur Verarbeitung der angezeigten Daten. Der Consent umfasst die Attribute, welche vom IDP-Dienst bezogen auf die im Claim des jeweiligen Fachdienstes eingeforderten Attribute zusammenfasst. Es besteht Einigkeit zwischen dem, was gefordert wird, und welche Attribute im Token bestätigt werden.
Discovery Document	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.
Gerät	Alle Arten von mobilen oder stationären Endgeräten.
ID-Token	Ein auf JSON basiertes und nach [RFC7519] (JWT) genormtes Identitäts-Token, mit dem ein Client (Anwendungsfrontend) die Identität eines Nutzers überprüfen kann.
Löschung	Unter Löschung eines Schlüssels sollen pauschal alle Operationen verstanden werden, die einer Anwendung einen kryptographischen Schlüssel dauerhaft entziehen.
Name (eines Geräts)	Ein vom Nutzer vergebener Name eines Geräts.
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.
sektoraler Identity Provider	Als sektoraler Identity Provider (IDP) wird ein Dienst bezeichnet, welcher nach vorheriger Authentifizierung Identitätsinformationen für eine bestimmte Gruppe von Nutzern innerhalb der Telematikinfrastruktur des Gesundheitswesens bereitstellt, welche anschließend verwendet werden, um auf verschiedene Fachdienste und deren Fachdaten und -prozesse zuzugreifen.
SSO Token	Gegen Vorlage eines gültigen SSO Token ist keine erneute Nutzerauthentisierung für die Ausstellung eines Access Tokens am IDP-Dienst nötig.
Token-Endpunkt	Ein Endpunkt des Authorization Servers, welcher für die Ausstellung von Token ("ID_TOKEN" und "ACCESS_TOKEN") zuständig ist.

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

6.3 Abbildungsverzeichnis

6.4 Tabellenverzeichnis

6.5 Referenzierte Dokumente

6.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	Elektronische Gesundheitskarte und Telematikinfrastruktur - Glossar der Telematikinfrastruktur
[gemSpec_IDP_Dienst]	Elektronische Gesundheitskarte und Telematikinfrastruktur - Spezifikation Identity Provider-Dienst
[gemSpec_IDP_FD]	Elektronische Gesundheitskarte und Telematikinfrastruktur - Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste
[gemSpec_IDP_Frontend]	Elektronische Gesundheitskarte und Telematikinfrastruktur - Spezifikation Identity Provider - Frontend
[gemSpec_OM]	Elektronische Gesundheitskarte und Telematikinfrastruktur - Übergreifende Spezifikation Operations und Maintenance
[gemSpec_SST_LD_BD]	Elektronische Gesundheitskarte und Telematikinfrastruktur - Spezifikation Logdaten- und Betriebsdatenerfassung

6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ANDROIDAPPLINKS]	https://developer.android.com/studio/write/app-link-indexing
[APPLEUNIVERSAL]	https://developer.apple.com/ios/universal-links/
Verordnung (EU) Nr. 910/2014 auch eIDAS Verordnung genannt	VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
Duchführungsverordnung (EU) 2015/1502	DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

GKV-SV Richtlinie "Kontakt mit Versicherten"	Richtlinie des GKV-Spitzenverbandes zu Maßnahmen zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme nach § 217f Absatz 4b SGB V (GKV-SV Richtlinie Kontakt mit Versicherten) vom 14.12.2018
[ietf-oauth-iss-auth-resp]	https://datatracker.ietf.org/doc/html/draft-ietf-oauth-iss-auth-resp-00
[RFC3986]	https://datatracker.ietf.org/doc/html/rfc3986
[RFC6749]	https://datatracker.ietf.org/doc/html/rfc6749
[RFC7515]	https://datatracker.ietf.org/doc/html/rfc7515
[RFC7519]	https://datatracker.ietf.org/doc/html/rfc7519
[RFC7636]	https://datatracker.ietf.org/doc/html/rfc7636
[RFC8252]	https://datatracker.ietf.org/doc/html/rfc8252
[RFC8414]	https://datatracker.ietf.org/doc/html/rfc8414
[TR-03107-1]	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf;jsessionid=FFBC05B6EE23EE8461127AC755D621FC.internet461?__blob=publicationFile&v=1