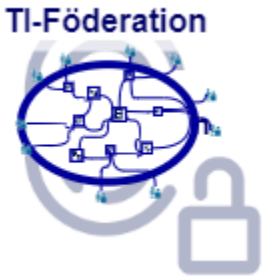
Terminologie/Glossar

Die Seite gibt einen Überblick über die in den Flowbeschreibungen häufig verwendete Terminologie und Standards.



Begriff	Erläuterung	Referenz / Standard
Access Token	Access Token werden für den Zugriff auf geschützte Ressourcen verwendet. Ein Access Token ist eine Zeichenfolge, die einem Client für den autorisierten Zugriff auf geschützte Ressourcen ausgestellt wird. Acces s Token werden vom Authorization Server eines Fachdienstes ausgestellt.	The OAuth 2.0 Authorizatio n Framework
Auth EP / Token EP	Authentication Endpunkt (Auth EP) , Token-Endpunkt (Token EP)	OpenID Connect Core 1.0 incorporatin g errata set 1
Authentic ation	Prozess zur Verifikation einer bekannten Entität und Identität.	OpenID Connect Core 1.0 incorporatin g errata set 1
Authoriz ation Code Flow	OAuth 2.0-Flow, bei dem ein Autorisierungscode vom Autorisierungsendpunkt und alle Token vom Tokenendpunkt zurückgegeben werden.	OpenID Connect Core 1.0 incorporatin g errata set 1
Authentic ation Request	Der OAuth 2.0-Authentication Request ist die Anforderung einer OpenID Connect-Relying-Party (Client) zur Authentifizierung eines Endbenutzers durch einen OpenID Connect-Provider.	OpenID Connect Core 1.0 incorporatin g errata set 1
Authoriz ation Code (AuthCo de)	Der Autorisierungscode ist ein temporärer Code, den der Client gegen ein Zugriffstoken austauscht. Der Autorisierungscode wird vom nach Authentisierung vom Autorisierungsendpunkt ausgestellt und an den Client übermittelt. Der Client kann mit dem Autorisierungscode ein Access-Token beim Tokenendpunkt des Autorisierungsserver anfordern.	The OAuth 2.0 Authorizatio n Framework
Authoriz ation Grant	Authorization Grant definierte die Festlegung, wie ein resource owner autorisiert wird, um ein Access-Token für einen Zugang zu den geschützten Resourcen zu erhalten. Die Spezifikation unterscheidet vier grant types -- authorization code, implicit, resource owner password credentials sowie client credentials.	The OAuth 2.0 Authorizatio n Framework
Authoriz ation Request	Der Client fordert die Autorisierung vom Ressourceneigentümer durch einen Authorization Request an. Der Authorization Request kann direkt an den Ressourcenbesitzer oder indirekt über den Authorization-Server als Vermittler gestellt werden.	OpenID Connect Core 1.0 incorporatin g errata set 1
Authoriz ation Server	Der Server, der Zugriffstoken an den Client ausgibt, nachdem er den Nutzer erfolgreich authentifiziert und die nach den Zugriffsregeln zulässigen Ressourcen bestimmt hat hat.	The OAuth 2.0 Authorizatio n Framework
Claim	Einzelne Information über eine Entität	OpenID Connect Core 1.0 incorporatin g errata set 1

Client	Eine Anwendung, die geschützte Ressourcenanforderungen im Namen des Ressourceneigentümers und mit seiner Autorisierung durchführt. Der Begriff „Client“ impliziert keine besonderen Implementierungsmerkmale (z. B. ob die Anwendung auf einem Server, einem Desktop oder anderen Geräten ausgeführt wird). Im Kontext der TI-Föderation ist das Anwendungsfrontend einer Fachanwendung der (OAuth)-Client bezüglich des Authorization-Servers bzw. des Resourceserver der Fachanwendung. Der Authorization-Server der Fachanwendung ist gleichzeitig auch der (OIDC)-Client bezüglich des sektoralen IDP.	The OAuth 2.0 Authorization Framework
Code Challenge	Die code challenge wird vom Code Verifier abgeleitet und bei einer Autorisierungsanfrage an den Autorisierungsserver gesendet. Der Autorisierungsserver merkt sich die code challenge zu dem von ihm ausgegeben Authorization Code. Beim Eintausch des Authorization Code gegen ein Access Token wird durch den Code Verifier die Legitimität der Anfrage verifiziert.	Proof Key for Code Exchange by OAuth Public Clients
Code Challenge Method	Die code challenge method ist die Methode, mit der die code challenge aus dem code verifier erstellt wurde.	Proof Key for Code Exchange by OAuth Public Clients
Code Verifier	Code Verifier ist eine kryptografisch zufällige Zeichenfolge. Bei einer Autorisierungsanforderung wird letztlich gegen diese Zeichenfolge validiert.	Proof Key for Code Exchange by OAuth Public Clients
Credential	Daten, die als Beweis für das Recht zur Nutzung einer Identität oder anderer Ressourcen präsentiert werden.	OpenID Connect Core 1.0 incorporating errata set 1
End-User (Nutzer/Anwender)	Nutzende natürliche Person (Mensch)	OpenID Connect Core 1.0 incorporating errata set 1
Entität	Etwas, das eine separate und eindeutige Existenz hat und das in einem Kontext identifiziert werden kann. Alle Entitäten in einem OpenID Connect-Verbund haben einen global eindeutigen Bezeichner Entitätsbezeichner	OpenID Connect Federation 1.0 (draft)
Entity Identifier / URI	Ein URI, der global eindeutig ist und an eine Entität gebunden ist.	OpenID Connect Federation 1.0 (draft)
Entity Statement	Ein Entity Statement - Entitätsaussage - wird von einer Entität ausgegeben, die sich auf eine Subjekt-Entität und Blatt-Entitäten bezieht. Ein Entitätsstatement ist immer ein signiertes JWT.	OpenID Connect Federation 1.0 (draft)
Fachdienst / Fachanwendung	Fachdienste bzw. Fachanwendungen sind die Anwendungen, mit denen ein Nutzer arbeiten möchte. So sind z. B. E-Rezept und die elektronische Patientenakte TI-Fachanwendungen. Ebenso sind die digitalen Gesundheitsanwendungen (DiGA) Fachdienste. Die Fachdienste /Fachanwendungen benötigen eine Nutzerauthentifizierung um sicherzustellen, dass ein Nutzer die Anwendung überhaupt nutzen darf. Im OAuth/OIDC-Kontext besteht der Fachdienst aus einem Authorizationserver (zur Abwicklung der Authentifizierung über einen IDP) und der eigentlichen Fachanwendung (mit Daten und Prozessen). Aus OAuth/OIDC Sicht agiert der Authorizationserver als Relying Party , die eigentliche Fachanwendung als Ressource Server. Für die Nutzerinteraktion verfügen Fachdienste bzw. Fachanwendungen über User Interfaces (UI) in Form von nativen Apps, Web-Frontends oder Desktopanwendungen.	OpenID Connect Federation 1.0 (draft)

Föderaler IDP	Allgemeiner Begriff für die IDP der Föderation. Konkret ist jeder IDP der Föderation für die Verwaltung von Identitäten bestimmter Sektoren (also = sektoraler IDP) zuständig.	
GesundheitsID	Die GesundheitsID ist die digitale Identität im Gesundheitswesen für Versicherte, welche durch die eigene Krankenversicherung bereitgestellt wird. Sie dient zur Anmeldung an TI-Anwendungen und weiteren versorgungsrelevanten Fachanwendungen und kann perspektivisch auch als Versicherungsnachweis - analog zur elektronischen Gesundheitskarte - verwendet werden.	
HSM	Hardware Security Module, Hardware-Sicherheitsmodul	
ID Token	JSON Web Token (JWT), welches Eigenschaften zur angefragten Identität und ggf. weitere Informationen enthält.	OpenID Connect Core 1.0 incorporating errata set 1
Intermediate Entity	Intermediäre Entität: Eine Entität, die eine Entitätserklärung ausstellt, die zwischen den vom Vertrauensanker und der Blattentität in einer Vertrauenskette ausgestellten Erklärungen liegt. (Wird in der aktuellen Architektur nicht verwendet)	OpenID Connect Federation 1.0 (draft)
Issuer	Ausstellende Entität für ein Token oder Entity Statement (über sich selbst oder eine andere Entität - dann als Subject bezeichnet)	OpenID Connect Core 1.0 incorporating errata set 1 OpenID Connect Federation 1.0 (draft)
Leaf Entity	Blatt-Entität: Eine Entität, die durch ein bestimmtes Protokoll definiert ist, z. B. OpenID Connect Relying Party oder Provider.	OpenID Connect Federation 1.0 (draft)
OpenID Provider (OP)	OAuth 2.0-Autorisierungsserver, der in der Lage ist, den Endbenutzer zu authentifizieren und einer vertrauenden Seite Informationen zur Authentifizierung und zum Endbenutzer bereitzustellen.	OpenID Connect Core 1.0 incorporating errata set 1
PAR	Beim Pushed Authorization Request werden im Vorfeld des eigentlichen OpenID Authorization Code Flow die Parameter direkt zwischen RP und OP ausgetauscht und diese gegenseitig Authentisiert.	OAuth 2.0 Pushed Authorization Requests
PKCE	Proof Key for Code Exchange ist eine Erweiterung des Autorisierungscodeflusses, um CSRF- und Authorization- Code-Injection-Angriffe zu verhindern. Bei dieser Technik erstellt der Client zunächst bei jeder Autorisierungsanforderung ein Geheimnis und verwendet dieses Geheimnis dann erneut, wenn er den Autorisierungscode gegen ein Access Token austauscht.	Proof Key for Code Exchange by OAuth Public Clients
Refresh Token	Refresh Token sind credentials, welche zum Abrufen von Access Token verwendet werden. Refresh Token werden vom Autorisierungsserver an den Client ausgegeben und verwendet, um ein neues Access Token zu erhalten, wenn das aktuelle Access Token ungültig wird oder abläuft, oder um zusätzliche Access Token mit identischem oder engerem Umfang zu erhalten. Access Token können eine kürzere Lebensdauer haben und weniger Berechtigungen als vom Ressourceneigentümer autorisiert. Das Ausstellen eines Refresh Token ist optional.	The OAuth 2.0 Authorization Framework
Relying Party (RP)	OAuth 2.0-Clientanwendung, die eine Endbenutzerauthentifizierung und Informationen von einem OpenID-Anbieter erfordert.	OpenID Connect Core 1.0 incorporating errata set 1

Request URI	URL, die auf eine Ressource verweist, welche vom Autorisierungsserver abrufbar sein muss.	OpenID Connect Core 1.0 incorporating errata set 1
Resource Owner	Entität, die Zugriff auf eine geschützte Ressource gewähren kann. Wenn der Ressourceneigentümer eine Person ist, wird er als Endbenutzer bezeichnet.	The OAuth 2.0 Authorization Framework
Resource Server	Der Server, der die geschützten Ressourcen hostet und in der Lage ist, Anforderungen für geschützte Ressourcen mithilfe von Zugriffstoken zu akzeptieren und darauf zu antworten.	The OAuth 2.0 Authorization Framework
sektoraler IDP	Jeder IDP verwaltet die Identitäten zu einem bestimmten Sektor. So verwalten die IDPs der Krankenkassen beispielsweise den Sektor der Versicherten, während andere IDPs die verschiedenen Sektoren der Leistungserbringer abdecken können.	
Subject	Entität über welche ein Token oder Entity Statement ausgestellt wurde und für welche die darin genannten Informationen gelten.	OpenID Connect Core 1.0 incorporating errata set 1 OpenID Connect Federation 1.0 (draft)
Scope	Bezeichnung für eine bestimmte Berechtigung (OAuth2) oder einen Satz von Informationen (OpenID) welche angefragt werden.	OpenID Connect Core 1.0 incorporating errata set 1 The OAuth 2.0 Authorization Framework
Trust Anchor	Vertrauensanker: Eine Entität, die eine vertrauenswürdige dritte Partei darstellt. (Der Federation Master)	OpenID Connect Federation 1.0 (draft)
Trust Chain	Vertrauenskette: Eine Folge von Entitätsaussagen, die eine Kette darstellt, die bei einer Blatt-Entität beginnt und bei einem Vertrauensanker endet.	OpenID Connect Federation 1.0 (draft)

Links zu den Terminologie-Kapiteln der Standards

- https://openid.net/specs/openid-connect-core-1_0.html#Terminology
- https://openid.net/specs/openid-connect-federation-1_0.html#name-terminology
- https://datatracker.ietf.org/doc/html/rfc7636#section-3