IT-PLANUNGSRAT

Frankfurt am Main
28.05.2026

Glossar für APIs in der öffentlichen Verwaltung

Zentrale Begriffe und Konzepte der föderalen API-Autorisierungsinfrastruktur

Inhaltsverzeichnis

1 Einleitung

Das vorliegende Glossar definiert die zentralen Begriffe und Konzepte, die im Kontext der föderalen API-Autorisierungsinfrastruktur verwendet werden. Die Begriffe werden in der Regel in ihrem englischen technischen Terminus verwendet. Das Glossar gilt übergreifend für die Sicherheitsvorgaben inkl. Begleitdokumente, die Anforderungen, die Architekturprinzipien, die Architekturentscheidungen sowie die Zielarchitektur und schafft damit ein einheitliches Begriffsverständnis über alle Dokumente hinweg.

Ziel des Glossars ist es, eine konsistente Verwendung sicherheits-, autorisierungs- und architekturbezogener Begriffe sicherzustellen und Missverständnisse in einem föderalen, organisationsübergreifenden Kontext zu vermeiden. Die hier definierten Begriffe sind bewusst lösungs- und organisationsneutral gehalten und beschreiben Konzepte, Rollen und Mechanismen unabhängig von ihrer konkreten Ausprägung in der Zielarchitektur.

Die konkrete Anwendung, Verantwortlichkeit oder Umsetzung der beschriebenen Konzepte wird in den jeweiligen Kapiteln des Dokuments behandelt. Dort werden die im Glossar definierten Begriffe kontextualisiert und auf die föderale Zielarchitektur angewendet, ohne deren grundlegende Bedeutung zu verändern.

2 Geltungsbereich des Glossars

Das Glossar beschränkt sich auf Begriffe und Konzepte der föderalen API-Autorisierungsinfrastruktur. Es erhebt keinen Anspruch auf Vollständigkeit über darüberhinausgehende fachliche oder technische Themenbereiche. Begriffe aus angrenzenden Domänen werden – sofern relevant – ausschließlich zur begrifflichen Einordnung referenziert.

3 Begriffe

Begriff	Abkürzung	Synonym / Langform	Definition	Quelle / Referenz
Attribute-Based Access Control	ABAC	Attributbasierte Zugriffskontrolle	Zugriffskontrollverfahren, bei dem Zugriffsberechtigungen auf Basis von Attributen des anfragenden Subjekts, der angefragten Ressource, der Aktion und des Kontexts ausgewertet werden. ABAC ermöglicht eine flexible, regelbasierte Berechtigungssteuerung, die über statische Rollenzuweisungen hinausgeht.	NIST SP 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations – https://doi.org/10.6028/NIST.SP.800-207
Access Token	–	Zugriffstoken	Berechtigungsnachweis, der einem Client den Zugriff auf eine geschützte Ressource gewährt. Der Authorization Server stellt das Token nach erfolgreicher Autorisierung aus; der Client legt es bei jedem Zugriff auf die geschützte Ressource vor.	draft-ietf-oauth-v2-1: The OAuth 2.1 Authorization Framework, Abschnitt 1.4 – https://datatracker.ietf.org/doc/html/draft-ietf-oauth-v2-1
Application Programming Interface	API	Programmierschnittstelle	Definierte Schnittstelle, über die Softwarekomponenten strukturiert miteinander kommunizieren können.	–
Append-only	–	Nur-Anfügen-Prinzip	Eigenschaft eines Datenspeichers, bei dem Einträge ausschließlich hinzugefügt, aber weder geändert noch gelöscht werden können. Dies gilt auch gegenüber dem Betreiber des Speichers selbst.	–

Architecture Decision Record	ADR	Architekturentscheidungsdokumentation	Dokumentationsformat zur strukturierten Erfassung wesentlicher Architekturentscheidungen, einschließlich der betrachteten Alternativen, der Entscheidungstreiber und der Konsequenzen der getroffenen Wahl.	Michael Nygard, „Documenting Architecture Decisions" (2011)
Authentifizierung	–	Authentication	Authentifizierung ist der Prozess, mit dem nachgewiesen wird, dass ein Akteur tatsächlich derjenige ist, als der er sich ausgibt. Ergebnis ist eine gesicherte Identitätsaussage.	ISO/IEC 27000:2018: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27000:ed-5:v1:en
AuthZEN	–	AuthZEN Authorization API	Spezifikation der OpenID Foundation, die eine einheitliche REST-API zwischen Policy Enforcement Points (PEP) und Policy Decision Points (PDP) definiert.	https://openid.net/wg/authzen/specifications/
Authorization	–	Autorisierung	Entscheidung und Durchsetzung, welche Aktionen ein (authentifizierter) Aktuer auf einer Ressource ausführen darf („Was darfst du?").	NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations: https://doi.org/10.6028/NIST.SP.800-162
Authorization Code Flow	–	Autorisierungscode-Ablauf	OAuth-2.0-Grant-Type, bei dem der Client zunächst einen Autorisierungscode erhält, den er anschließend gegen ein Access Token eintauscht. Dieser Flow erfordert eine Interaktion mit einem Endbenutzer über einen Browser.	draft-ietf-oauth-v2-1: The OAuth 2.1 Authorization Framework, Abschnitt 4.1 – https://datatracker.ietf.org/doc/html/draft-ietf-oauth-v2-1
Bearer Token	–	Inhabertoken	Ein Sicherheitstoken, bei dem allein der Besitz des Tokens zum Zugriff auf die geschützte Ressource berechtigt. Die Verwendung eines Bearer Tokens erfordert keinen Nachweis über den Besitz kryptographischen Schlüsselmaterials.	draft-ietf-oauth-v2-1: The OAuth 2.1 Authorization Framework, Abschnitt 1.4.2 – https://datatracker.ietf.org/doc/html/draft-ietf-oauth-v2-1

Client Credentials	–	Client Credentials Grant Type	OAuth-Grant-Type für Maschine-zu-Maschine-Kommunikation, bei dem der Client sich direkt mit seinen eigenen Anmeldedaten gegenüber dem Authorization Server authentifiziert, ohne dass ein Endbenutzer involviert ist.	draft-ietf-oauth-v2-1: The OAuth 2.1 Authorization Framework, Abschnitt 4.2 – https://datatracker.ietf.org/doc/html/draft-ietf-oauth-v2-1
Combining Algorithm	–	Regelkombinationsalgorithmus	Algorithmus zur Zusammenführung der Einzelergebnisse mehrerer Policies zu einer Gesamtentscheidung für eine Zugriffsanfrage. In der Zielarchitektur folgt der Algorithmus dem Deny-Overrides-Prinzip: Jede zutreffende DENY-Policy (deren Exceptions nicht greifen) setzt alle PERMIT-Policies außer Kraft. Bei ausschließlich zutreffenden PERMIT-Policies werden die freigegebenen Scopes als Vereinigungsmenge gebildet. Trifft keine Policy zu, gilt Implicit Deny.	Projektspezifisch (Kap. 5.1.3)
Consistency Proof	–	Konsistenznachweis	Kryptographischer Nachweis, dass ein späterer Zustand eines Transparency Logs eine konsistente Erweiterung eines früheren Zustands darstellt – d.h. dass keine bestehenden Einträge geändert oder entfernt wurden.	RFC 9162: Certificate Transparency Version 2.0 – https://datatracker.ietf.org/doc/html/rfc9162
Demonstrating Proof-of-Possession	DPoP	–	Mechanismus zur kryptographischen Bindung eines Access Tokens an den Client, dem es ausgestellt wurde. Der Client erzeugt einen DPoP-Proof als signierten JWT und sendet ihn bei jeder Token-Anfrage und jedem API-Aufruf mit. Dadurch kann ein abgefangenes Token nicht von Dritten verwendet werden.	RFC 9449: OAuth 2.0 Demonstrating Proof of Possession (DPoP) – https://datatracker.ietf.org/doc/html/rfc9449
Dynamic Client Registration	DCR	Dynamische Client-Registrierung	OAuth-2.0-Protokollerweiterung, die es Clients ermöglicht, sich automatisiert bei einem	RFC 7591: OAuth 2.0 Dynamic Client Registration Protocol –

			Authorization Server zu registrieren, ohne dass ein manueller administrativer Eingriff erforderlich ist. Das ergänzende Dynamic Client Registration Management Protocol definiert Operationen zur nachträglichen Verwaltung (Abfrage, Aktualisierung, Löschung) registrierter Clients.	https://datatracker.ietf.org/doc/html/rfc7591; RFC 7592: OAuth 2.0 Dynamic Client Registration Management Protocol – https://datatracker.ietf.org/doc/html/rfc7592
eIDAS	–	Electronic Identification, Authentication and Trust Services	EU-Verordnung (Nr. 910/2014) zur elektronischen Identifizierung und zu Vertrauensdiensten für elektronische Transaktionen im europäischen Binnenmarkt. Sie bildet die rechtliche Grundlage für die grenzüberschreitende Anerkennung elektronischer Identitäten.	Verordnung (EU) Nr. 910/2014 – https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910
Financial-grade API 2.0	FAPI 2.0	–	Sicherheitsprofil der OpenID Foundation für OAuth 2.0 und OpenID Connect, das für Hochsicherheitsszenarien entwickelt wurde. FAPI 2.0 definiert verbindliche Vorgaben zu Client-Authentifizierung, Sender-Constraining und Token-Binding.	https://openid.net/specs/fapi-2_0-security-profile.html
Föderale API-Autorisierungsinfrastruktur	–	–	Gesamtheit der organisatorischen, technischen und prozessualen Strukturen, die eine einheitliche, standardisierte API-Autorisierung für föderale Basisdienste ermöglichen. Sie umfasst zentrale und dezentrale Systeme, gemeinsame Sicherheitsvorgaben und Registrierungsprozesse.	Projektspezifisch
Föderales Informationsmanagement	FIM	–	Rahmenwerk, mit dem Bund, Länder und Kommunen Informationen über Verwaltungshandeln strukturiert erfassen und zugänglich machen. FIM umfasst Leistungsbeschreibungen, Datenfelder und Prozessinformationen.	https://fimportal.de

ID Token	–	Identitätstoken	Sicherheitstoken im JWT-Format, das von einem OpenID Provider ausgestellt wird und Identitätsinformationen (Claims) über einen authentifizierten Endbenutzer enthält.	OpenID Connect Core 1.0, Abschnitt 2 – https://openid.net/specs/openid-connect-core-1_0.html
Implicit Deny	–	Implizite Ablehnung	Sicherheitsprinzip, nach dem ein Zugriff automatisch verweigert wird, wenn keine explizite Berechtigungsregel den Zugriff erlaubt.	–
Inclusion Proof	–	Zugehörigkeitsnachweis	Kryptographischer Nachweis, dass ein bestimmter Eintrag Teil eines Transparency Logs ist. Ermöglicht es Prüfinstanzen, die Existenz eines Eintrags zu verifizieren, ohne dem Betreiber des Logs vertrauen zu müssen.	RFC 9162: Certificate Transparency Version 2.0 – https://datatracker.ietf.org/doc/html/rfc9162
JSON Web Signature	JWS	–	Standard zur kryptographischen Signierung von Inhalten im JSON-Format.	RFC 7515: JSON Web Signature (JWS) – https://datatracker.ietf.org/doc/html/rfc7515
JSON Web Token	JWT	–	Kompaktes, URL-sicheres Token-Format zur Übertragung von Aussagen (Claims) zwischen zwei Parteien. Ein JWT kann signiert (JWS) und/oder verschlüsselt (JWE) sein.	RFC 7519: JSON Web Token (JWT) – https://datatracker.ietf.org/doc/html/rfc7519
Least Privilege	–	Prinzip der minimalen Berechtigung	Sicherheitsprinzip, nach dem ein System oder Akteur nur die Berechtigungen erhalten soll, die für die Erfüllung seiner Aufgabe zwingend erforderlich sind.	–
Level of Assurance	LoA	Vertrauensstufe	Maß für die Vertrauenswürdigkeit der Herkunft und Validierung eines Attributwerts, unabhängig vom Wert selbst.	ISO/IEC 29115: Entity authentication assurance framework – https://www.iso.org/standard/45138.html

Maschine-zu-Maschine	M2M	Machine-to-Machine	Kommunikationsmuster, bei dem kein menschlicher Akteur als Subjekt involviert ist und bei dem auch kein menschlicher Akteur als Subjekt in der Kommunikation auftritt.	–
Merkle-Tree	–	Merkle-Baum, Hash-Baum	Kryptographische Datenstruktur, bei der Datenblöcke paarweise gehasht und zu einem Wurzel-Hash zusammengeführt werden. Ermöglicht effiziente und fälschungssichere Überprüfung der Integrität und Vollständigkeit großer Datenmengen.	Ralph Merkle (1979)
Mutual TLS	mTLS	Gegenseitige TLS-Authentifizierung	Erweiterung des TLS-Protokolls, bei der sich nicht nur der Server, sondern auch der Client mittels Zertifikates authentifiziert. mTLS ermöglicht eine beidseitige Identitätsprüfung auf Transportebene und wird häufig zur Absicherung von Maschine-zu-Maschine-Kommunikation eingesetzt.	–
OAuth 2.0 / 2.1	–	–	Autorisierungsframework, das es einer Anwendung ermöglicht, im Namen eines Ressourcenbesitzers oder in eigenem Namen begrenzten Zugriff auf eine geschützte Ressource zu erlangen.	draft-ietf-oauth-v2-1: The OAuth 2.1 Authorization Framework – https://datatracker.ietf.org/doc/html/draft-ietf-oauth-v2-1
Onlinedienst	–	–	Fachliche Anwendung, die Bürgerinnen, Bürgern oder Unternehmen eine digitale Verwaltungsleistung bereitstellt und dazu einen oder mehrere föderale Basisdienste über deren APIs nutzt.	Projektspezifisch
OpenID Connect	OIDC	–	Identitätsschicht auf Basis von OAuth 2.0, die es Clients ermöglicht, die Identität eines Endbenutzers anhand der von einem OpenID Provider durchgeführten Authentifizierung zu verifizieren und grundlegende Profilinformationen abzurufen.	OpenID Connect Core 1.0 – https://openid.net/specs/openid-connect-core-1_0.html

Policy	–	Berechtigungsregel	Strukturiertes Regelobjekt, das Bedingungen und Zugriffsregeln für eine bestimmte Ressource zusammenfasst und über einen Effekt (z.B. Erlauben oder Verweigern) festlegt, wie mit Zugriffsanfragen umgegangen wird, die seine Bedingungen erfüllen.	OASIS XACML 3.0: eXtensible Access Control Markup Language Version 3.0 – https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html
Policy-based Access Control	PBAC		PBAC ist ein Zugriffskontrollmodell, bei dem Entscheidungen darüber, wer auf welche Ressourcen zugreifen darf, nicht fest in Rollen oder Identitäten kodiert sind, sondern anhand von deklarativen Policies getroffen werden.	NIST SP 800-95: Guide to Secure Web Services
Policy Administration Point	PAP	–	Zentrale Verwaltungsschnittstelle für Berechtigungsregeln. Der PAP bildet die einzige autorisierte Schreibschnittstelle gegenüber dem Policy Store und stellt sicher, dass Policies ausschließlich über kontrollierte, nachvollziehbare Prozesse verwaltet werden.	OASIS XACML 3.0 – https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html; NIST SP 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations – https://doi.org/10.6028/NIST.SP.800-207
Policy Decision Point	PDP	–	Komponente, die Berechtigungsentscheidungen trifft. Der PDP bewertet eingehende Autorisierungsanfragen anhand geltender Policies und verfügbarer Attribute und gibt eine Entscheidung zurück.	OASIS XACML 3.0 – https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html; NIST SP 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations – https://doi.org/10.6028/NIST.SP.800-207
Policy Enforcement Point	PEP	–	Komponente, die Berechtigungsentscheidungen durchsetzt. Der PEP fängt Zugriffsanfragen ab, leitet sie zur Entscheidung an den PDP weiter und setzt das Ergebnis um.	OASIS XACML 3.0 – https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html; NIST SP 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations – https://doi.org/10.6028/NIST.SP.800-207

Policy Information Point	PIP	–	Komponente, die dem PDP die für Berechtigungsentscheidungen benötigten Attributwerte bereitstellt. Der PIP bezieht Attribute aus autoritativen Quellen und liefert sie an den PDP aus.	OASIS XACML 3.0 – https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html; NIST SP 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations – https://doi.org/10.6028/NIST.SP.800-207
private_key_jwt	–	Private-Key-JWT-Client-Authentifizierung	Methode zur Client-Authentifizierung gegenüber einem Authorization Server, bei der der Client einen mit seinem privaten Schlüssel signierten JWT als Nachweis seiner Identität sendet.	OpenID Connect Core 1.0, Abschnitt 9 – https://openid.net/specs/openid-connect-core-1_0.html; RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants – https://datatracker.ietf.org/doc/html/rfc7523
Proof Key for Code Exchange	PKCE	–	OAuth-2.0-Sicherheitserweiterung, die den Authorization Code Flow gegen Abfangen des Autorisierungscodes absichert. Der Client erzeugt einen kryptographischen Verifier und sendet dessen Hash (Challenge) mit der Autorisierungsanfrage; beim Token-Tausch wird der Verifier zur Prüfung übermittelt.	RFC 7636: Proof Key for Code Exchange by OAuth Public Clients – https://datatracker.ietf.org/doc/html/rfc7636
Public Key Infrastructure	PKI	Public-Key-Infrastruktur	System zur Ausstellung, Verwaltung, Verteilung und Prüfung von digitalen Zertifikaten und kryptographischen Schlüsseln.	–
Relationship-Based Access Control	ReBAC	Beziehungsbasierte Zugriffskontrolle	Zugriffskontrollmodell, bei dem Berechtigungen auf Basis der Beziehungen zwischen Entitäten gewährt werden, z. B. Organisationszugehörigkeit oder Delegationsketten.	Zanzibar: Google's Consistent, Global Authorization System

Scope	–	Geltungsbereich, Berechtigungsumfang	Parameter in OAuth 2.0, der den Umfang der vom Client beantragten Zugriffsberechtigungen beschreibt.	draft-ietf-oauth-v2-1: The OAuth 2.1 Authorization Framework, Abschnitt 1.4.1 – https://datatracker.ietf.org/doc/html/draft-ietf-oauth-v2-1
Security Assertion Markup Language	SAML	–	XML-basiertes Framework zum Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Parteien, insbesondere zwischen einem Identity Provider und einem Service Provider.	OASIS SAML 2.0: Security Assertion Markup Language – https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
Security Event Token	SET	Sicherheitsereignistoken	JWT-basiertes Token-Format zur standardisierten Darstellung sicherheitsrelevanter Ereignisse.	RFC 8417: Security Event Token (SET) – https://datatracker.ietf.org/doc/html/rfc8417
Security Information and Event Management	SIEM	–	Kategorie von Sicherheitslösungen, die sicherheitsrelevante Ereignisse aus verschiedenen Quellen sammeln, korrelieren und auswerten, um Bedrohungen zu erkennen und darauf zu reagieren.	–
Sender-Constraining	–	Absenderbindung	Sicherheitsmechanismus, der die Nutzung eines Access Tokens an einen bestimmten Absender bindet. Der Absender muss die Kenntnis eines bestimmten Geheimnisses als Voraussetzung für die Akzeptanz des Tokens beim Empfänger nachweisen.	draft-ietf-oauth-v2-1: The OAuth 2.1 Authorization Framework, Abschnitt 1.4.3 – https://datatracker.ietf.org/doc/html/draft-ietf-oauth-v2-1
Session	–	Sitzung	Zeitlich begrenzter Zustandskontext zwischen einem Benutzer und einem System, der nach erfolgreicher Authentifizierung eingerichtet wird und wiederholte Interaktionen ohne erneute Anmeldung ermöglicht.	–
Shared Signals Framework	SSF	–	Spezifikation der OpenID Foundation für den standardisierten Austausch sicherheitsrelevanter	https://openid.net/specs/openid-sharedsignals-framework-1_0.html

			Ereignissignale zwischen kooperierenden Systemen. Das SSF definiert Transmitter- und Receiver-Rollen sowie Stream-basierte Konfiguration für die Weiterleitung von Security Event Tokens (SETs).	
Single Sign-On	SSO	Einmalanmeldung	Authentifizierungsverfahren, bei dem sich ein Benutzer einmalig anmeldet und anschließend ohne erneute Authentifizierung auf mehrere zusammengeschlossene Systeme oder Dienste zugreifen kann.	–
Software Statement	SSA	Software Statement Assertion	Digital signierter oder MAC-geschützter JSON Web Token (JWT), der Metadaten über eine Client-Software enthält. Ein Software Statement kann vom Client-Entwickler selbst oder von einer vertrauenswürdigen Drittpartei ausgestellt werden und dient bei der dynamischen Client-Registrierung als Vertrauensnachweis gegenüber dem Authorization Server. Die signierte Variante wird als Software Statement Assertion (SSA) bezeichnet.	RFC 7591: OAuth 2.0 Dynamic Client Registration Protocol, Abschnitt 2.3 – https://datatracker.ietf.org/doc/html/rfc7591
System for Cross-domain Identity Management	SCIM	–	Offener Standard zur Automatisierung des Austauschs von Benutzeridentitätsinformationen zwischen IT-Systemen und Identitätsdomänen.	RFC 7644: System for Cross-domain Identity Management: Protocol – https://datatracker.ietf.org/doc/html/rfc7644
Token Exchange	–	Token-Austausch	OAuth-2.0-Protokollerweiterung, die den Austausch eines bestehenden Tokens gegen ein neues Token mit anderem Geltungsbereich oder anderen Eigenschaften ermöglicht.	RFC 8693: OAuth 2.0 Token Exchange – https://datatracker.ietf.org/doc/html/rfc8693

Token Introspection	–	Token-Prüfung	OAuth-2.0-Protokollerweiterung, die es einem geschützten Ressourcenserver ermöglicht, beim Authorization Server den aktuellen Zustand und die Metadaten eines Access Tokens abzufragen.	RFC 7662: OAuth 2.0 Token Introspection – https://datatracker.ietf.org/doc/html/rfc7662
Transparency Log	–	Transparenzprotokoll	Append-only-Datenstruktur auf Basis eines Merkle-Trees, die Ereignisse manipulationssicher und kryptographisch verifizierbar protokolliert. Die Integrität des Logs kann ohne Vertrauen in den Betreiber geprüft werden.	–
User Interface	UI	Benutzeroberfläche	Grafische Schnittstelle zur Interaktion zwischen einem System und menschlichen Nutzern, z.B. Web-Formulare oder Self-Service-Portale.	–
Wertstrom	–	Value Stream	Ende-zu-Ende-Abfolge von Aktivitäten, die notwendig sind, um einem bestimmten Stakeholder einen konkreten Nutzen zu liefern.	BIZBOK Guide, Business Architecture Guild – https://www.businessarchitecture-guild.org/page/BIZBOK
Zero Trust	–	–	Sicherheitsparadigma, bei dem kein System, kein Netzwerkbereich und kein Akteur ohne explizite Verifikation als vertrauenswürdig gilt. Jede Anfrage wird unabhängig von Netzwerkherkunft oder institutioneller Zugehörigkeit authentifiziert und autorisiert.	NIST SP 800-207: Zero Trust Architecture – https://doi.org/10.6028/NIST.SP.800-207

4 Ergänzende Hinweise zur Verwendung und Einordnung des Glossars

4.1 Verwendung in der Zielarchitektur

Die Zielarchitektur konkretisiert ausgewählte im Glossar definierte Begriffe in spezifischen Zusammenhängen:

- Kapitel 4.3.1 stellt die zentralen Datenobjekte übersichtlich dar.
- Kapitel 6.1.3 beschreibt föderale Basisdienste als Nutzungskontext der Infrastruktur.

4.2 Verwendung in den Sicherheitsvorgaben inkl. Begleitdokumente

Die in den Sicherheitsvorgaben und Begleitdokumenten enthaltenen Kapitel „Symbole und Abkürzungen" dienen der Lesbarkeit der jeweiligen Dokumente. Sie führen verwendete Abkürzungen und Akronyme auf, stellen jedoch keine eigenständigen begrifflichen Definitionen dar.

Sofern Begriffe oder Abkürzungen sicherheits- oder architekturrelevant sind, sind sie im vorliegenden Glossar definiert oder durch Verweis auf ihre normative Ursprungsquelle (z. B. RFCs oder Spezifikationen der OpenID Foundation) eingeordnet. Die Sicherheitsprofile setzen diese Begriffe voraus und verwenden sie konsistent im jeweiligen Schutzbedarfs- und Bedrohungskontext.

4.3 Referenz auf Begriffe aus internationalen Standards

Für Begriffe, die durch internationale Standards normativ definiert sind, gelten die jeweiligen Definitionen der referenzierten Spezifikationen, insbesondere der relevanten RFCs (u. a. OAuth 2.x, OpenID Connect) sowie ausgewählter ISO-Normen, sofern sie in diesem Glossar nicht auf den Kontext der föderalen API-Autorisierungsinfrastruktur konkretisiert wurden.