eCH-0219 – IAM-Glossar

Name	IAM-Glossar
eCH-Nummer	eCH-0219
Kategorie	Standard
Reifegrad	Definiert
Version	2.0.0
Status	Genehmigt
Beschluss am	2025-12-11
Ausgabedatum	2025-10-16
Ersetzt Version	1.0 – Major Change
Voraussetzungen	---
Beilagen	---
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Fachgruppe	eCH-FG IAM
Herausgeber / Vertrieb	Verein eCH, Affolternstrasse 52, 8050 Zürich T 044 388 74 64 / info@ech.ch / www.ech.ch

Zusammenfassung

Der vorliegende Standard definiert die wichtigsten Begriffe für IAM-Lösungen in der Schweiz und bildet damit die Grundlage aller eCH-Standards im Bereich IAM.

Die aufgenommenen Begriffe umfassen Stakeholder, Prozesse, Services bis zu Implementationsdetails in föderierten und nicht föderierten IAM-Lösungen. Begriffe aus aktuellen internationalen Standards werden zu den definierten Begriffen in Beziehung gesetzt und damit verständlicher gemacht.

Version 2.0.0 enthält neu auch Begriffe zu dezentralen Identitäten und Self-Sovereign Identities (SSI).

Inhaltsverzeichnis

1 Einleitung 8
1.1 Status 8
1.2 Anwendungsgebiet 8
1.3 Abgrenzung 8
1.4 Normativer Charakter der Kapitel 8
2 Terminologie 9
2.1 Abonnent/-in 9
2.2 Akteur 9
2.3 Antragsteller/in 9
2.4 Attribut 9
2.5 Attributbasierte Zugriffskontrolle (ABAC) 10
2.6 Attributbestätigung 10
2.7 Attribute Assertion Service 11
2.8 Attribute Provider (AP) 11
2.9 Attribute Service 11
2.10 Auditing 11
2.11 Authentication Proxy 11
2.12 Authentication Service 11
2.13 Authentifizierung 12
2.14 Authentifizierungsbestätigung 12
2.15 Authentifizierungsmittel 12
2.16 Autorisation Service 14
2.17 Autorisierung 14
2.18 Behörde 14
2.19 Benutzer/-in 15
2.20 Benutzer-Account 15
2.21 Berechtigung 15
2.22 Beweismittel 15
2.23 Biometrisches Merkmal 15

2.24 Broker Service ... 16
2.25 Certificate Policy (CP) ... 16
2.26 Certificate Revocation List (CRL) ... 17
2.27 Certification Authority (CA) ... 17
2.28 Certification Practice Statement ... 17
2.29 Challenge Response ... 17
2.30 Claim ... 17
2.31 Client Plattform ... 18
2.32 Credential ... 18
2.33 Credential Service ... 19
2.34 Definitionszeit ... 19
2.35 Dezentrale Identität ... 19
2.36 Dienstanbieter ... 19
2.37 Digitale Identität ... 19
2.38 Digitaler Prozess ... 20
2.39 Digitale Ressource ... 20
2.40 Digitale-Ressource Service ... 20
2.41 Digitale Signatur ... 20
2.42 Digitales Zertifikat ... 21
2.43 Digital-Identity Service ... 21
2.44 Ding ... 21
2.45 Discovery Service ... 21
2.46 Domäne ... 21
2.47 Eigenschaft ... 21
2.48 Einmal-Passwort ... 22
2.49 Elektronische Signatur ... 22
2.50 Elektronisches Identifizierungsmittel ... 22
2.51 Elektronisches Identifizierungssystem ... 22
2.52 Elektronisches Siegel ... 22
2.53 Entität ... 23
2.54 Führung ... 23
2.55 Gerätebindung ... 23

2.56 Geregeltes Zertifikat 23
2.57 Holder 24
2.58 Holder of Key (HoK) 24
2.59 IAM-Architektur 24
2.60 IAM-Dienstanbieter 24
2.61 IAM-Führung 25
2.62 IAM-Policy 25
2.63 IAM-Regulator 25
2.64 IAM-Service 25
2.65 IAM-Support 26
2.66 IAM-System 26
2.67 Identifikator 26
2.68 Identifizierung 26
2.69 Identität 26
2.70 Identitätsdokument 27
2.71 Identitätsföderierung 28
2.72 Identity and Access Management (IAM) 29
2.73 Identity Linking 29
2.74 Identity Mapping 29
2.75 Identity Provider (IdP) 29
2.76 Inhaberbindung 30
2.77 Institution 30
2.78 Issuer 30
2.79 Juristische Person 30
2.80 Kerberos 30
2.81 Körperliches Merkmal 31
2.82 Kryptographischer Token 31
2.83 Laufzeit 31
2.84 Linking Protokoll 31
2.85 Leistungsbezüger (LB) 31
2.86 Leistungserbringer (LE) 31
2.87 Logging Service 32

2.88 Look-Up Secret 32
2.89 Magic Link 32
2.90 Memorized Secret 32
2.91 Meta-Attribut 33
2.92 Metadaten 33
2.93 Namensraum 33
2.94 Natürliche Person 33
2.95 Netzwerk 34
2.96 Nichtabstreitbarkeit 34
2.97 OAuth 2.0 34
2.98 Objekt 34
2.99 Online Certificate Status Protocol (OCSP) 34
2.100 OpenID Connect (OIDC) 34
2.101 Organisation 35
2.102 OTP-Device 35
2.103 Out-of-Band Authenticator 35
2.104 Passkey 36
2.105 Passwort 36
2.106 Passwortlose Authentifizierung 36
2.107 Physischer Ausweis 37
2.108 Policy 37
2.109 Provisionierung 37
2.110 Prozess 37
2.111 Push-Nachrichten 37
2.112 Qualifizierte elektronischen Signatur (QES) 38
2.113 Qualifiziertes Zertifikat 38
2.114 Rechte 38
2.115 Register 38
2.116 Registrierung 38
2.117 Registrierungsstelle / Registration Authority (RA) 38
2.118 Regulator 39
2.119 Relying Party (RP) 39

2.120 Ressource 39
2.121 Ressourcen-Verantwortlicher 39
2.122 Rolle 39
2.123 Rollenbasierte Zugriffskontrolle (RBAC) 40
2.124 Security Assertion Markup Language (SAML) 40
2.125 Security Token 40
2.126 Security Token Service 40
2.127 Selektive Offenlegung 40
2.128 Self-Sovereign Identity (SSI) 41
2.129 Service 41
2.130 Service Level Agreement (SLA) 41
2.131 Single Sign-On (SSO) 41
2.132 Staatlich anerkannte elektronische Identität (E-ID) 41
2.133 Stakeholder 42
2.134 Subjekt 42
2.135 Topologie 43
2.136 Trust Service 44
2.137 Trusted Third Party 44
2.138 UID-Einheit 44
2.139 Überbringer/-in 44
2.140 Verifiable Credential (VC) 45
2.141 Verifiable Data Registry 45
2.142 Verifiable Presentation (VP) 45
2.143 Verifier 46
2.144 Verlässliche Quelle 46
2.145 Vermittler 46
2.146 Vertrauen 47
2.147 Vertrauensstufe 47
2.148 Wallet 47
2.149 Widerruf 47
2.150 Zugriffsrecht Service 48
2.151 Zugriffskontrolle 48

2.152 Zero-Knowledge Proof (ZKP) 48
3 Haftungsausschluss/Hinweise auf Rechte Dritter 49
4 Urheberrechte 49
Anhang A – Referenzen & Bibliographie 50
Anhang B – Mitarbeit & Überprüfung 51
Anhang C – Abkürzungen 52
Anhang D – Änderungen gegenüber Vorversion 54
Anhang E – Abbildungsverzeichnis 56
Anhang F – Tabellenverzeichnis 56

Hinweis

Im vorliegenden Dokument wird bei der Bezeichnung von Personen eine geschlechtsneutrale Formulierung verwendet. Basis bildet der Leitfaden der Bundeskanzlei. Je nach Situation kommen Paarformen (Bürgerinnen und Bürger), geschlechtsabstrakte Formen (versicherte Person), geschlechtsneutrale Formen (Versicherte) oder Umschreibungen ohne Personenbezug zum Einsatz. Das generische Maskulin (Bürger) ist nicht zulässig. Vollformen werden in fortlaufenden Texten verwendet, also in Texten, die aus ausformulierten Sätzen bestehen. In verknappten Textpassagen, namentlich in Tabellen, können Kurzformen verwendet werden. Dabei wird die Kurzform mit Schrägstrich, aber ohne Auslassungsstrich verwendet (Referent/in). Genderstern und ähnliche Schreibweisen werden nicht verwendet.

1 Einleitung

Identity and Access Management (IAM) ist ein zentraler Bestandteil der IT-Security und regelt den Zugriff auf Ressourcen in elektronischen Prozessen. Ein effektives IAM-System gewährleistet, dass nur authentisierte und oder autorisierte Personen oder Dienste auf schützenswerte Ressourcen zugreifen können. Dazu müssen Identitäten und Berechtigungen verwaltet werden.

Dieser Standard definiert die grundlegenden Begriffe und Konzepte im Bereich IAM und dient damit als Grundlage für alle, welche IAM-Lösungen entwerfen.

1.1 Status

Genehmigt: Das Dokument wurde vom Expertenausschuss genehmigt. Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.

1.2 Anwendungsgebiet

Die in diesem Standard definierten Konzepte und Begriffe fassen die Terminologie im Bereich IAM zusammen und konsolidieren diese. Die aufgenommenen Begriffe umfassen Stakeholder, Prozesse, Services bis zu Implementationsdetails in föderierten, nicht föderierten und dezentralen IAM-Lösungen.

Der Standard ist für alle die mit IAM in Berührung kommen, vom Entwickler über den Architekten bis zum Management.

1.3 Abgrenzung

Die Begriffe in diesem Glossar werden im Kontext Identitäts- und Zugriffsverwaltung (Identity and Access Management, IAM) definiert. Lesarten der Begriffe, die über IAM hinausgehen, werden nicht berücksichtigt.

1.4 Normativer Charakter der Kapitel

Die Kapitel des vorliegenden Standards sind von normativem oder auch deskriptivem Charakter. Folgende Tabelle definiert die Einordnung der Kapitel.

Kapitel	Beschreibung
1 Einleitung	Deskriptiv
2 Terminologie	Normativ

Anhang A und Anhang C sind ebenfalls normativ. Alle anderen Anhänge dieses Standards sind deskriptiv.

2 Terminologie

2.1 Abonnent/-in

Ein **Abonnent** oder eine **Abonnentin** [1] ist ein *Subjekt*, welches nach erfolgreich abgeschlossener *Registrierung* zu einem *Akteur* in dem *IAM-System* wird.

Synonym: Subscriber (engl.)

2.2 Akteur

Ein **Akteur** [2] ist eine *Entität* oder *Subjekt* in einem *IAM-System*, welche *Prozesse* ausführt. Ein Akteur wird durch einen oder mehrere *Stakeholder* motiviert.

Akteure sind u.a.:

- *Subjekt*,
- *Relying Party*,
- *IAM-Dienstanbieter*,
- *IAM-Führung*,
- *IAM-Support*,
- *IAM-Regulator*.

2.3 Antragsteller/in

Ein **Antragsteller** oder eine **Antragstellerin** [1] ist ein *Objekt*, das in ein *IAM-System* aufgenommen werden möchte und dazu die *Registrierung* durchläuft. Wurde diese erfolgreich abgeschlossen, wird aus dem Antragsteller oder der Antragstellerin ein *Abonnent* oder eine Abonnentin.

Synonym: Applicant (engl.)

2.4 Attribut

Ein **Attribut** ist ein digitales Abbild einer einem *Subjekt* zugeordneten *Eigenschaft*, die das Subjekt näher beschreibt.

Ein Attribut setzt sich aus *Meta-Attributen* zusammen: Attributname (z. B. „Schuhgrösse“), Attributdatentyp (z. B. „Integer“) und Attributwert (z. B. „39“).

Ein *Identifikator* ist ein speziell verwendetes Attribut.

Attribute lassen sich in verschiedene Gruppen einteilen, die sich teilweise überschneiden können:

- **Subjektidentifizierende und -beschreibende Attribute**:
  - Identifier und Fremdschlüssel,
  - Subjektidentifizierende Attribute, z. B. Name, Geschlecht, Geburtsdatum, …
  - Kommunikationsattribute, wie E-Mail-Adresse, Telefonnummer, Postadresse, …
  - Biometrische Attribute, wie Lichtbilder, …
  - …
- **Authentifizierende Attribute:** Dazu gehören die *Credentials* oder Referenzen auf Credentials.
- **Autorisierungsrelevante Attribute**: dazu zählen alle Attribute, die bei einer Autorisationsentscheidung dienlich sind, u. a.:
  - Kontextattribute, die die Einordnung in eine Organisation beschrieben,
  - Rollenattribute, die die Funktion in einer Organisation (Kontext) beschreiben,
  - …
- **Metadaten-Attribute**: Informationen über die Erfassung der Daten, Status und Gültigkeit.

Attribute können im IAM-System selbst oder in angehängten Systemen, z. B. in einem HR- oder CRM-System abgelegt und gepflegt werden.

Synonym: *Claim*

2.5 Attributbasierte Zugriffskontrolle (ABAC)

Die **Attributbasierte Zugriffskontrolle (ABAC)** [3] bezeichnet eine Art der *Zugriffskontrolle*, mit welcher eine *Relying Party* den Zugang zu einer *Ressource* aufgrund eines oder mehrerer *Attribute* des *Subjekts* autorisiert.

Synonym: Attribute based Access Control (engl.)

2.6 Attributbestätigung

Eine **Attributbestätigung** ist eine Bestätigung des Wertes eines *Attributs* für ein *Subjekt* durch einen *Attribute Provider (AP)*, einen *IdP* oder einen *Issuer*.

Attributbestätigungen werden häufig gemeinsam mit *Authentifizierungsbestätigungen* nach der erfolgreichen *Authentifizierung* des Subjekts ausgestellt.

Beispiele:

- *SAML*: SAML 2.0 Attribute Assertion [4]
- *OIDC*: *Claims* im ID-Token,
- *SSI*: *Claims* in *Verifiable Credentials*

Synonym: Attribute Assertion (engl.), Attributwertbestätigung

2.7 Attribute Assertion Service

Ein **Attribute Assertion Service** [2] ist ein *IAM-Service, der Attributbestätigungen* über eine definierte Schnittstelle ausstellt.

Synonym: Attributbestätigungs-Service

2.8 Attribute Provider (AP)

Ein **Attribute Provider** ist eine *Entität*, meist ein *Register* oder sonstiges Verzeichnis, mit einem *Attribute Service* zur Pflege von *Attributen* und einem *Attribute Assertion Service* zur Ausstellung von *Attributbestätigungen*.

Synonyme: Attribute Authority (AA), Datenlieferant, Informationslieferant, OIDC Claims Provider

2.9 Attribute Service

Der **Attribute Service** [2] ist ein *IAM-Service*, der für die zeitnahe Pflege von *Attributen* für definierte *Subjekte* zuständig ist.

2.10 Auditing

Auditing bezeichnet den kontinuierlichen oder periodischen Prozess der systematischen Überprüfung von *Prozessen* oder Systemen, um deren Einhaltung von Richtlinien, Standards oder gesetzlichen Anforderungen zu verifizieren.

Im IAM-Kontext umfasst Auditing beispielsweise die Aufzeichnung und Analyse von Benutzeraktivitäten, Systemzugriffen oder sicherheitsrelevanten Ereignissen, um verdächtige Aktivitäten zu erkennen, Sicherheitsrichtlinien durchzusetzen oder gesetzliche Vorgaben zu erfüllen.

2.11 Authentication Proxy

Ein **Authentication Proxy** verbindet zwei Protokollabschnitte und bildet damit einen Protokollendpunkt. Er kann Authentifizierungsanfragen und -antworten transformieren und weiterleiten. Der Authentication Proxy kann ein Teil eines *Vermittlers* sein.

2.12 Authentication Service

Der **Authentication Service** [2] ist ein *IAM-Service* und ein integraler Bestandteil des *Verifiers*. Er gleicht die präsentierten *Authentifizierungsmittel* mit den gespeicherten *Credentials* ab und kann so feststellen, ob der oder die Zugreifende (*Subjekt*), die behauptete *Digitale Identität* besitzt.

2.13 Authentifizierung

Authentifizierung ist der Prozess der Überprüfung einer behaupteten *Digitalen Identität* eines *Subjekts* nach bestimmten Vorgaben. Die angestrebte *Vertrauensstufe* der Authentifizierung bestimmt diese Vorgaben.

Dabei wird der Gültigkeit eines oder mehrerer *Authentifizierungsmittel* überprüft, die zur Beanspruchung der *Digitalen Identität* verwendet werden. Dabei wird festgestellt, ob das *Subjekt*, das versucht, auf eine *Relying Party* zuzugreifen, die Kontrolle über die zur *Authentifizierung* verwendeten Geheimnisse hat.

Um die Benutzerfreundlichkeit zu bessern, geht der Trend zu *Passwortloser Authentifizierung*.

Synonyme: Authentifikation, Authentisierung[1]

2.14 Authentifizierungsbestätigung

Eine **Authentifizierungsbestätigung** ist ein digitaler Nachweis, welcher ein *Identity Provider* (IdP) nach einer erfolgreichen *Authentifizierung* des *Subjektes* ausstellt. Die Authentifizierungsbestätigung ist für einen bestimmten Zeitraum gültig und kann den Kontext der Authentifizierung oder eine *Vertrauensstufe* enthalten.

Beispiele:

- Bei *SAML* ist die Authentifizierungsbestätigung die „Authentication Assertion“ und wird vom (SAML) Identity Provider ausgestellt.
- Bei *OIDC* ist die Authentifizierungsbestätigung das „ID-Token“ und wird vom „Authorization Server“ ausgestellt.
- Bei *Kerberos* ist die Authentifizierungsbestätigung ein „Ticket Granting Ticket“ (TGT) und wird vom Kerberos Distribution Center (KDC) ausgestellt.

2.15 Authentifizierungsmittel

Authentifizierungsmittel sind Informationen und/oder *Prozesse*, die zur *Authentifizierung* eines *Subjektes* verwendet werden können. Authentifizierungsmittel können auf verschiedenen Merkmalen beruhen:

- Kenntnisabhängig: beruht auf Wissen (etwas, das das Subjekt weiss, z. B. *Passwort*, PIN)
- Besitzabhängig: beruht auf dem Besitz (etwas, das das Subjekt besitzt, z. B. Soft-Token/Hardware-Token mit privatem Schlüssel, elektronischer Pass oder ID-Karte)
- *Eigenschaft* des Subjekts: beruht auf einem *biometrischen Merkmal*,
- Verhaltensbasiert (selten eingesetzt): beruht auf Verhalten (etwas, was das Subjekt typischerweise macht, z. B. dynamisches Unterschriftenmuster).

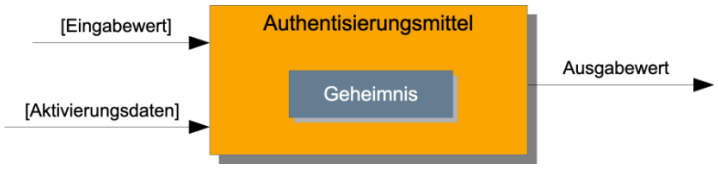
[1] Ein Subjekt authentisiert sich gegenüber einem System. Ein System authentifiziert ein Subjekt.

Ein Authentifizierungsmittel kann auf einem einzigen Faktor basieren (Single-Faktor-Authentifizierung, SFA) oder mehrere Faktoren kombinieren (Multi-Faktor-Authentifizierung, MFA), um die Sicherheit zu erhöhen.

Ein typisches Beispiel für MFA ist die Kombination aus einem Passwort und einem *Einmal-Passwort*, der an das Mobiltelefon gesendet wird.

Der vom Authentifizierungsmittel generierte Ausgabewert wird durch eine mathematische Funktion aus einem geheimen Wert (z. B. privater Schlüssel), einem oder mehreren optionalen Aktivierungsdaten (z. B. PIN oder *biometrisches Merkmal*), und einem oder mehreren optionalen Eingabewerten (z. B. Zufallswerte oder Challenges) generiert. Im Trivialfall kann das Authentifizierungsmittel der geheime Wert selbst sein (z. B. im Fall eines Passwortes).

Authentifizierungsmittel werden vom *Credential Service* ausgestellt.



Ausgabewert = Funktion (Geheimnis, [Eingabewert], [Aktivierungsdaten])

Abbildung 1 - Schematische Funktionsweise eines Authentifizierungsmittels

	Passwort	SMS	OTP	Mobile-ID	FIDO-Token	Smartcard
Authentifizierungs-Typ	SFA	MFA - 1. Faktor ist meist ein Passwort	MFA - 1. Faktor ist meist ein Passwort	MFA - 1. Faktor ist meist ein Passwort	SFA/MFA	MFA
Token-Typ	SW	SW/HW Smartphone	SW-HW	HW (e)SIM	HW	HW
Eingabewert	-	erhaltener Code	Seed des Devices	erhaltener Code	selbstgenerierte Nonce	selbstgenerie Nonce
Geheimnis	Passwort	erhaltener Code	Device Key	Private Key	Private Key	Private Ke
Aktivierungsdaten	-	-	Aktuelle Zeit oder Zähler	PIN	Präsenz, PIN oder Biometrisches Merkmal	PIN
Authentifizierungsfunktion	Keine oder Hashfunktion	Lesen und Schreiben des erhaltenen Codes	HMAC	Signatur	Signatur	Signatur

	Passwort	SMS	OTP	Mobile-ID	FIDO-Token	Smartcard
Ausgabewert	Passwort, Hash des Passwortes	erhaltener Code	erhaltener Code	Sign (erhaltener Code)	Sign (Nonce)	Sign (Nonce)
Credential[2]	Passwort beim Verifier gespeichert	Der Verifier kennt die Mobil-Nr. des Subjekts	synchroner Seed beim Verifier	Mobile-Nr. und Public Key beim Verifier gespeichert	Certificate beim Verifier gespeichert	Certificate b Verifier gesp chert

Tabelle 1: Beispiele für Authentifizierungsmittel

Synonyme: Authentifizierungsfaktor, Authentifizierungsmerkmal

2.16 Autorisation Service

Der **Autorisation Service** [2] ist ein *IAM-Service*. Er überprüft zur *Laufzeit* die Einhaltung der Rechte für die Nutzung der *digitalen Ressource* und erlaubt dem *Subjekt* die Nutzung der Ressource, wenn es die entsprechenden Rechte besitzt.

Synonym: Zugang Service, Access Service (engl.)

2.17 Autorisierung

Autorisierung ist ein zeitnaher *Prozess* zur Gewährung bzw. Verweigerung der Nutzung einer *Ressource* durch ein authentifiziertes *Subjekt* anhand von zuvor definierten Regeln.

Synonym: *Berechtigung* (im Sinne des Vorgangs), Authorization (engl.)

2.18 Behörde

Eine **Behörde** ist eine *Organisation*, ein Organ des Staates (Bund, Kanton) oder eines selbständigen Verwaltungsträgers (Bezirk, Gemeinde), das Aufgaben der öffentlichen Verwaltung des Staates oder Verwaltungsträgers wahrnimmt und diesen im zugewiesenen Zuständigkeitsbereich nach Aussen vertritt. Behörden können auf den Verwaltungsebenen von Gemeinde, Kanton oder Bund bestehen und zur Legislative, Exekutive oder Judikative gehören. (siehe auch eCH-0177 [5] – Beilage 1)

[2] Zum Credential gehört immer auch der Identifier, z. B. der Name des Benutzers bzw. der Benutzerin.

2.19 Benutzer/-in

Der **Benutzer** oder die Benutzerin ist eine *natürliche Person* (*Subjekt*), die über einen *Benutzer-Account* bei einer *RP* verfügt. Mit Hilfe des Benutzer-Accounts kann der Benutzer oder die Benutzerin aktiv an *digitalen Prozessen* der RP teilnehmen.

Synonym: User (engl.)

2.20 Benutzer-Account

Ein **Benutzer-Account** umfasst *Attribute* und Daten eines *Benutzers* oder einer Benutzerin bei der RP. Er ist mit einer oder mehrere *Digitalen Identitäten* eines Benutzers oder einer Benutzerin verlinkt, die zur *Authentifizierung* gegenüber der RP genutzt werden können. Der Benutzer-Account wird bei der *Registrierung* des *Subjekts* bei der RP erstellt.

Synonym: Benutzerobjekt, Benutzerkonto

2.21 Berechtigung

Der Begriff **Berechtigung** hat zwei Bedeutungen:

1. Der Vorgang der Berechtigung als Synonym für *Autorisierung*.
2. Die Berechtigungen eines *Subjekts* sind alle Regeln, die definieren, wann das Subjekt unter welchen Bedingungen auf die *Ressourcen* einer *Relying Party* zugreifen darf.

2.22 Beweismittel

Ein **Beweismittel** (im *IAM*-Kontext) ist ein Dokument aus einer verlässlichen Quelle, das Angaben zum *Antragsteller* oder zur Antragstellerin enthält. Es kann zur Überprüfung einer *Identität* verwendet werden.

Ein Beweismittel muss den Namen des Antragsstellers oder der Antragstellerin enthalten. Es kann zusätzlich einen eindeutigen *Identifikator*, *körperliche* und *biometrische Merkmale* aber auch beliebige andere Angaben des Antragstellers oder der Antragstellerin enthalten. Es sollte Sicherheitsmerkmale enthalten, die ein Reproduzieren erschweren.

Beispiele für Beweismittel:

- Beglaubigte Urkunde, z. B. Geburtsurkunde
- Fahrausweis
- *Identitätsdokumente*

2.23 Biometrisches Merkmal

Ein **biometrisches Merkmal** ist ein einzigartiges, messbares körperliches Merkmal eines Menschen, das zur eindeutigen *Identifizierung* dieser Person genutzt werden kann. Im Gegensatz zu allgemeinen *körperlichen Merkmalen* wie Grösse oder Haarfarbe sind biometrische Merkmale oft unveränderlich und bieten eine hohe Sicherheit für Authentifizierungsverfahren.

Ein wesentlicher Nachteil der biometrischen *Authentifizierung* besteht darin, dass biometrische Merkmale im Falle einer Kompromittierung nicht für ungültig erklärt oder neu erzeugt werden können.

Beispiele für biometrische Merkmale:

- Physiologische Merkmale:
  - Fingerabdrücke
  - Gesichtsmerkmale (z. B. Augenabstand, Gesichtsform)
  - Iris- und Netzhautmuster
  - Hand- und Fingergeometrie
  - Venenmuster
  - DNA
- Verhaltensmerkmale:
  - Unterschrift
  - Tippgeschwindigkeit
  - Gangart
  - Stimme

Biometrische Merkmale können bezüglich Funktion, Sicherheit, Fälschbarkeit und Anwendungsfreundlichkeit klassifiziert werden, siehe [6].

2.24 Broker Service

Der **Broker Service** [2] ist ein *IAM-Service*, der zwischen *Subjekt*, *Ressourcen* und den *IAM-Services* der *Laufzeit* vermittelt und *Authentifizierungs*- und *Attributbestätigungen* föderiert.

2.25 Certificate Policy (CP)

Eine **Certificate Policy** ist ein Dokument (*Policy*), das die Regeln, Anforderungen und Verfahren für die Inhalte, Ausstellung, Verwaltung und Nutzung *digitaler Zertifikate*, meist innerhalb einer Public Key Infrastructure (PKI) festlegt.

CPs finden aber auch in anderen Bereichen Anwendung, in denen digitale Zertifikate oder kryptografische Identitäten verwendet werden, z. B.:

- *SSI*: CPs können Richtlinien für die Ausstellung und Verwaltung von *Verifiable Credentials* (VCs) definieren.
- IoT: CPs können Regeln für Zertifikate in vernetzten Geräten und Maschinen vorgeben.
- *Elektronische Signaturen*: CPs können Anforderungen an Zertifikate für qualifizierte elektronische Signaturen festlegen, wie z. B. im ZertES [7] oder bei eIDAS [8].

2.26 Certificate Revocation List (CRL)

Eine **CRL** ist eine Liste, die von einer oder mehreren *Zertifizierungsstellen* (*CAs*) veröffentlicht wird und alle *digitalen Zertifikate* enthält, die vor ihrem regulären Ablaufdatum widerrufen wurden (siehe *Widerruf*). Jedes Element der Liste umfasst mindestens die Seriennummer des widerrufenen Zertifikats und den Zeitpunkt des Widerrufs.

2.27 Certification Authority (CA)

Eine *Certification Authority* ist eine vertrauenswürdige *Entität*, die *digitale Zertifikate*, z. B. X.509, ausgibt, erneuert und revoziert.

Laut ZertES [7] Anbieterin von Zertifizierungsdiensten: «Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck *digitale Zertifikate* ausstellt»

Synonyme: Anbieterin von Zertifizierungsdiensten [7], Zertifizierungsdienstleister, Zertifizierungsstelle für digitale Zertifikate, Certification Service Provider (engl.)

Überbegriffe: Zertifizierungsstelle, Trust Service Provider (TSP), Vertrauensdiensteanbieter (VDA)

2.28 Certification Practice Statement

Ein **Certification Practice Statement** ist ein detailliertes Dokument (*Policy*) einer *Certification Authority* (CA), das die konkreten Verfahren, Sicherheitsmassnahmen und operativen Praktiken beschreibt, mit denen sie die in der *Certificate Policy (CP)* festgelegten Anforderungen umsetzt.

2.29 Challenge Response

Challenge Response ist ein interaktives Verfahren, um Wissen zu beweisen (Proof of Knowledge), ohne das Wissen preisgeben zu müssen.

Ohne das Wissen preiszugeben, beweist der Wissende (Prover) dem Prüfer (Verifier) sein Wissen, indem er eine oder mehrere Aufgaben (Challenges) vom Prüfer löst. Die korrekte Antwort (Response) auf die Summe aller Aufgaben kann nur der Wissende (mit grosser Wahrscheinlichkeit) erbringen.

2.30 Claim

1. Ein **Claim** ist eine Aussage über eine *Eigenschaft* eines *Subjekts*. Claims können durch einen *IdP* oder einen *Issuer* bestätigt werden und dann als *Attributbestätigung* fungieren.

2. Im *SSI*-Kontext werden Claims als Subjekt-Attribut-Wert Beziehung dargestellt. Einzelne Claims können verknüpft werden und bilden dann einen Graphen mit Aussagen über ein oder mehrere *Subjekte* (siehe Abbildung 2*).*

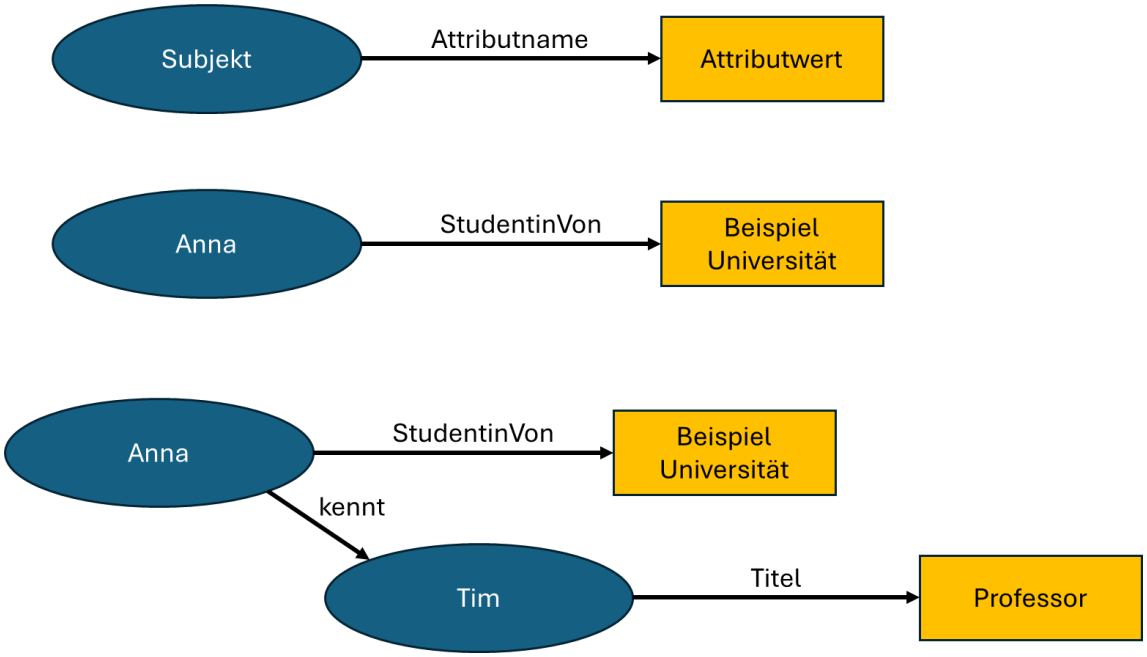


Abbildung 2 - Einzelne und verknüpfte Claims im Kontext SSI

Synonym: Aussage, Behauptung

2.31 Client Plattform

Die **Client Plattform** ist das System oder Gerät, von welchem das *Subjekt* einen Authentisierungsprozess anstösst. Dies kann beispielsweise ein Browser auf einem PC/Laptop oder eine Applikation auf einem mobilen Gerät sein.

Synonym: Client, user agent (engl.)

2.32 Credential

Ein **Credential** stellt eine Menge von Daten (keine Hardware oder andere physische Container) dar, mit der eine *Digitale Identität* an ein *Authentifizierungsmittel* gebunden wird, welches vom *Subjekt* kontrolliert wird. Die Bindung erfolgt über den *Identifikator* der Digitalen Identität.

Das Credential wird vom *Verifier* zusammen mit dem Ausgabewert des Authentifizierungsmittels zum Nachweis der behaupteten *Digitalen Identität* verwendet.

Beispiele sind der Hash eines *Passwortes*, ein Abbild eines *biometrischen Merkmals* oder ein *Digitales Zertifikat* (siehe Tabelle 1).

Ein Credential muss immer auf Authentizität und Vertrauenswürdigkeit überprüft werden, bevor es verwendet wird. (siehe auch ISO 29115 [9], Annex B und NIST SP 800-63B [1], Kap 3).

Synonym: Identitätsnachweis, ugs. Anmeldedaten

2.33 Credential Service

Der **Credential Service** [2] ist ein *IAM-Service* und zuständig für die Ausgabe und Verwaltung von *Authentifizierungsmittel* für *Subjekte*. Er ermöglicht auch eine benutzerfreundliche Erneuerung bzw. den Ersatz von Authentifizierungsmitteln.

2.34 Definitionszeit

In der **Definitionszeit** wird das *IAM-System* eingerichtet und konfiguriert. Zusätzlich werden *Digitale Identitäten* etabliert. Die Definitionszeit umfasst damit die Prozesse zur Bereitstellung aller notwendigen Informationen für alle beteiligten Komponenten sowie der Komponenten selbst.

Siehe auch *Laufzeit*.

2.35 Dezentrale Identität

Dezentrale Identität ist ein digitales Identitätskonzept, bei dem *Digitalen Identitäten* dezentral gespeichert werden, meist in einem *Wallet*. Dies ermöglicht die Entkopplung von Ausstellung und Nutzung der Identität.

Beispiele für dezentrale Identitäten sind:

- *Verifiable Credentials (VC)* mit *Inhaberbindung*
- X.509 Zertifikate
- nPA [10]

Synonym: Benutzerzentrierte Identität

2.36 Dienstanbieter

Der (IAM-)**Dienstanbieter** [2] ist ein *Stakeholder* in einem *IAM-System* und möchte IAM-Leistungen anbieten.

Synonym: *IAM-Dienstanbieter*

2.37 Digitale Identität

Eine **digitale Identität** ist eine digitale Repräsentation von *Eigenschaften* eines *Subjekts* (siehe *Identität*). Mittels einer digitalen Identität kann ein *Subjekt* in einem *digitalen Prozess* handeln.

Eine digitale Identität ist über ein *Credential* an ein *Authentifizierungsmittel* gebunden, so dass sich ein Subjekt damit authentifizieren kann (siehe *Authentifizierung*).

Ein *Subjekt* kann mehrere Identitäten haben, zu denen wiederum mehrere digitale Identitäten gehören können (siehe Abbildung 4 - Identität). Ein Subjekt hat i.d.R. eine Identität pro *Domäne*.

Beispiele:

- Ein *Benutzer-Account* bei einem Online-Shop ist mit einer digitalen Identität verlinkt, die aus einem *Identifikator* (z. B. E-Mail-Adresse), Angaben zur *Person* (Namen, Geburtsdatum, …) sowie einem Passwort als *Authentifizierungsmittel* besteht.
- Ein Mitarbeiter oder eine Mitarbeiterin hat eine Identität, die in einer HR-Anwendung verwaltet wird. Daraus entstehen digitale Identitäten z. B. in einem AD oder einem SAP-System.

Synonyme:

- Elektronische Identität
- Engl. Digital Identity, Electronic Identity

2.38 Digitaler Prozess

Ein **digitaler Prozess** bezeichnet eine definierte Abfolge von Aktivitäten oder Arbeitsschritten, die zur Erreichung eines bestimmten Ziels durchgeführt werden. Im Kontext des *Identity and Access Management (IAM)* dienen diese Prozesse der Verwaltung und Kontrolle des Zugriffs auf geschützte *Ressourcen* durch *Subjekte*.

An einem solchen Prozess sind beteiligt:

- Direkt und aktiv**:** *Subjekte*,
- Indirekt oder passiv**:** *Objekte*, *Ressourcen*,
- Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder die logisch mit ihnen verknüpft sind und zu deren *Authentifizierung* dienen.

Synonym: elektronischer Prozess

2.39 Digitale Ressource

Eine **Digitale Ressource** ist die *Identität* einer *Ressource*. Eine digitale Ressource hat einen *Identifikator* (eindeutiger Name, oft URL/URI), welcher innerhalb eines *Namensraumes* eindeutig einer Ressource zugewiesen werden kann. Eine Ressource kann mehrere digitale Ressourcen haben.

2.40 Digitale-Ressource Service

Der **Digitale-Ressource Service** [2] ist ein *IAM-Service, der digitale Ressourcen* zu *Ressourcen* ausstellt und verwaltet.

2.41 Digitale Signatur

Eine **digitale Signatur** ist eine spezielle Form der *elektronischen Signatur*. Eine digitale Signatur beruht auf einem technischen Verfahren, das kryptographische Methoden verwendet, um die Integrität einer Nachricht oder eines Dokuments zu prüfen und die Authentizität des Unterzeichners zu garantieren. Oft werden *digitale Zertifikate* verwendet, um digitale Signaturen zu erstellen.

2.42 Digitales Zertifikat

Ein **Digitales Zertifikat** ist eine von einer *Certification Authority* signierte, elektronische Datei, die zur Bestätigung der Identität einer Person, eines Unternehmens oder einer Website dient.

Digitale Zertifikate haben verschiedene Verwendungszwecke, wie Verschlüsselung, *Authentifizierung*, und *elektronische Signatur*. Ausgestellt werden solche digitalen Zertifikate von Firmen oder dedizierten Zertifizierungsstellen (siehe *Certification Authority*). Letztere können staatlich anerkannt sein und werden regelmässig überprüft. [7]

Synonyme: Identitäts-Zertifikat, Public-Key-Zertifikat

2.43 Digital-Identity Service

Der **Digital-Identity Service** [2] ist ein *IAM-Service*, der *digitale Identitäten* zu *Subjekten* ausstellt und diese verwaltet.

2.44 Ding

Ein **Ding** im IAM-Kontext ist ein physischer Gegenstand, welcher über ein *Netzwerk* erreichbar gemacht werden kann. Innerhalb des Netzwerkes ist das Ding mit einem *Identifikator* eindeutig identifizierbar. Mehrere Dinge, welche über ein Netzwerk verknüpft sind, bilden ein Internet der Dinge (Internet of Things, IoT). Dinge können weitere Dinge enthalten. Ein Ding gehört immer zu einer *Organisation* oder zu einer *natürlichen Person*.

Synonyme: Objekt, engl. Thing (IoT)

2.45 Discovery Service

Der **Discovery Service** [2] ist ein *IAM-Service*, der dafür zuständig ist, das *Subjekt* zu einem *IdP* seiner Wahl - zwecks *Authentifizierung* - zu leiten.

Synonym: WAYF (Where Are You From) Service

2.46 Domäne

Eine **Domäne** im IAM-Kontext bezeichnet einen abgegrenzten Bereich von *Ressourcen*, *Identitäten* und Regeln, der unter einer gemeinsamen Verwaltungsstruktur und Autorität organisiert ist.

Synonym: Ökosystem

2.47 Eigenschaft

Eigenschaften sind Merkmale oder Kennzeichen eines *Subjekts* oder *Objekts* *(siehe* Abbildung 4*)*, die in ihrer Summe spezifisch sind.

2.48 Einmal-Passwort

Ein **Einmal-Passwort** ist ein einmalig verwendbares Passwort, das für eine kurze Zeitspanne gültig ist. Es gibt zeitbasierte Einmal-Passwörter und zufällig generierte Einmal-Passwörter. Einmal-Passwörter werden häufig in Zwei-Faktor-Authentifizierung (2FA) zusammen mit einem Passwort verwendet (siehe Kap. 2.15 *Authentifizierungsmittel*).

Synonym: Einmalcode, engl. One-Time Password (OTP)

2.49 Elektronische Signatur

Elektronische Signaturen sind «Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder die logisch mit ihnen verknüpft sind und zu deren Authentifizierung dienen.» [7]

Elektronische Signaturen können zur Überprüfung der *Identität* der oder des Unterzeichnenden verwendet werden.

Der Begriff «Elektronische Signatur» ist juristischer Natur und ist ein Oberbegriff für alle Arten von Signaturen in digitaler Form. Elektronische Signaturen umfassen also auch nicht-kryptografische Verfahren (z.B. eingescannte handschriftliche Unterschrift - Faksimile). Mit *digitalen Signaturen* lassen sich sichere elektronische Signaturen erstellen.

2.50 Elektronisches Identifizierungsmittel

Begriff aus eIDAS 2024/1183 [8]: «‚**Elektronisches Identifizierungsmittel**‘ ist eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten oder gegebenenfalls bei Offline-Diensten verwendet wird.»

2.51 Elektronisches Identifizierungssystem

Begriff aus eIDAS 2024/1183 [8]: «**Elektronisches Identifizierungssystem**‘ ist ein System für die elektronische Identifizierung, in dessen Rahmen natürlichen oder juristischen Personen oder natürlichen Personen, die andere natürliche Personen oder juristische Personen vertreten, elektronische Identifizierungsmittel ausgestellt werden.»

2.52 Elektronisches Siegel

Ein **elektronisches Siegel** ist eine *elektronische Signatur*, die speziell für *Organisationen*, Unternehmen oder *Behörden* entwickelt wurde. In der Schweiz ist das elektronische Siegel an ein *geregeltes Zertifikat* gebunden. Im EU-Raum sind - aus Kompatibilitätsgründen zu Mitgliedstaaten - Siegel mit qualifizierten Zertifikaten möglich.

2.53 Entität

Eine **Entität**[3] ist ein Element eines IT-Systems, z. B. eine Komponente oder ein Teilsystem, welche als *digitale Identität* in einem *digitalen Prozess* handelt (siehe Abbildung 7 - Objekt und Subjekt).

Beispiele für Entitäten sind:

- *Identity Provider*,
- *RP*s,
- *Services*,
- Applikationen,
- Autonome Bots.

Synonym: Entity

2.54 Führung

Die **Führung** [2] ist ein *Stakeholder* in einem *IAM-System*. Sie möchte ein funktionierendes und stabiles IAM-System, das allen Stakeholdern gerecht wird. Dazu führt sie die darin beteiligten *Akteure*.

2.55 Gerätebindung

Gerätebindung stellt sicher, dass eine *dezentrale Identität* oder ein *VC* eindeutig an ein bestimmtes Gerät (*Entität*) gebunden wird und sich nicht auf ein anderes Gerät übertragen lässt.

Im Gegensatz zur *Inhaberbindung* garantiert die Gerätebindung dabei nicht, dass das *Subjekt* auch der Inhaber bzw. die Inhaberin (*Holder*) der *dezentralen Identität* oder des VC ist.

Synonym: Device Binding (engl.)

2.56 Geregeltes Zertifikat

Ein **geregeltes Zertifikat** ist ein auf eine *natürliche Person* oder eine *UID-Einheit* ausgestelltes *digitales Zertifikat*, welches die entsprechenden Vorschriften des ZertES [7] erfüllt. Geregelte Zertifikate können z. B. für *elektronische Siegel* oder zur Website-Authentisierung eingesetzt werden.

[3] Der Begriff “Entität” wird im Kontext IAM anders verwendet als allgemein in der Datenmodellierung. In der Datenmodellierung bezeichnet der Begriff Entität ein eindeutig identifizierbares Objekt oder eine Informationseinheit. Eine Entität repräsentiert dabei ein physisches oder abstraktes Ding, wie z. B. eine Person, ein Produkt, ein Auftrag oder ein Buch.

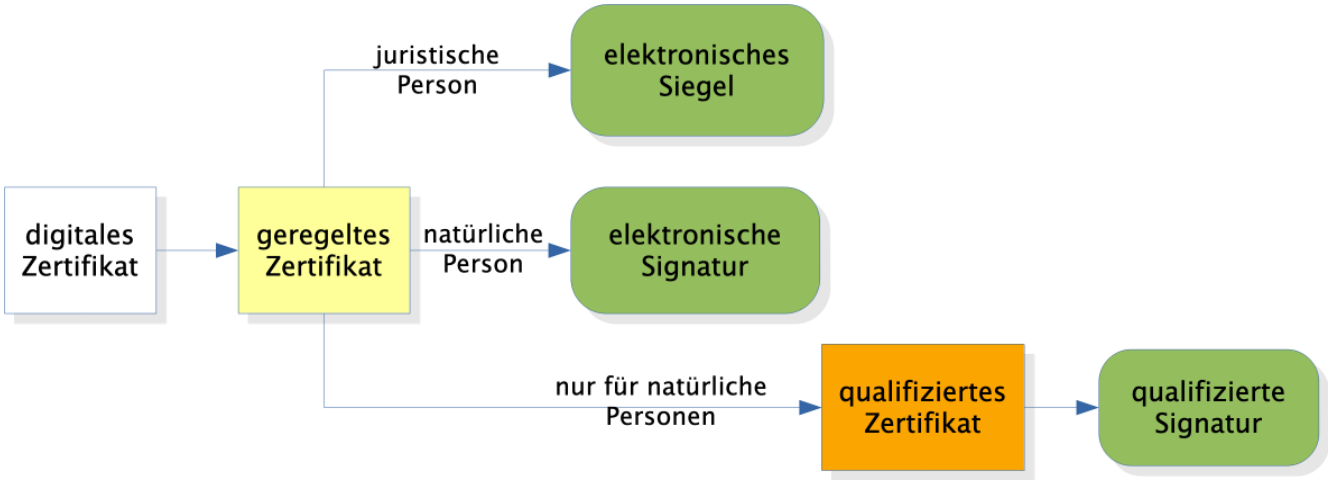


Abbildung 3 - Übersicht der verschiedenen digitalen Zertifikate

2.57 Holder

Ein **Holder** ist eine *Rolle*, welche ein *Subjekt* im *SSI*-Kontext übernimmt. Der Holder speichert *Verifiable Credentials (VCs)* an einem dezentralen, vom ihm kontrollierten Speicherort (*Wallet*). Dadurch hat der Holder Kontrolle über seine VCs und kann sie oder Teile davon mit Hilfe seines *Wallets* einem *Verifier* präsentieren.

Synonym: Inhaber/-in, Halter/-in

2.58 Holder of Key (HoK)

Ein **Holder of Key (HoK)** ist ein *Subjekt*, das eine vom *IdP* ausgestellte *Authentifizierungsbestätigung* an die RP übergibt und dabei kryptographisch nachweist, dass es im Besitz eines zugehörigen privaten Schlüssels ist, im Gegensatz zu einem *Überbringer* oder einer Überbringerin (Bearer), der keinen solchen Nachweis erbringt.

2.59 IAM-Architektur

Die **IAM-Architektur** besteht aus Konzepten, *Prozessen* und *Topologien*, sowie deren Beziehungen innerhalb des *IAM-Systems*.

2.60 IAM-Dienstanbieter

Ein **IAM-Dienstanbieter** [2] ist ein *Akteur* in einem *IAM-System* und verantwortlich für den Betrieb eines oder mehrerer *IAM-Services*.

IAM-Dienstanbieter sind u.a.:

- *IdP*
- *Vermittler*
- *Attribute Provider*
- *Registrierungsstelle*.

2.61 IAM-Führung

Die **IAM-Führung** [2] ist ein *Akteur* in einem *IAM-System*. Sie führt die teilnehmenden *IAM-Dienstanbieter* und *Relying Parties*.

2.62 IAM-Policy

Die **IAM-Policy** definiert die Ziele, Prinzipien und die Systemgrenzen eines *IAM-Systems*.

2.63 IAM-Regulator

Der **IAM-Regulator** [2] ist ein *Akteur* in einem *IAM-System*. Er definiert die rechtlichen, prozeduralen, organisatorischen/architektonischen und technischen Rahmenbedingungen, innerhalb derer das *IAM* abgewickelt werden muss. Er berücksichtigt dabei die Interessen aller *Stakeholder* und beteiligt alle anderen in geeigneter Weise an der Definition.

IAM-Regulatoren existieren in verschiedenen Formen und können sowohl innerhalb einer einzigen *Organisation*, aber auch organisationsübergreifend agieren.

- Die IAM-Steuerung definiert die *IAM-Policy* für ein organisationsinternes oder -externes IAM-System bzw. von *IAM-Services*.
- Der Gesetzgeber definiert die rechtlichen Rahmenbedingungen innerhalb derer sich das Gesamtsystem bewegen und entwickeln muss.
- Das Standardisierungsgremium erstellt Normen und Richtlinien für die prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen.

2.64 IAM-Service

Ein **IAM-Service** [2] ist ein *Service*, der von einem *IAM-Dienstanbieter* angeboten wird. IAM-Services sind keine technischen Komponenten, d.h. bei einer Realisierung können ein oder auch mehrere IAM-Services von einer technischen Komponente implementiert oder auch ein IAM-Service auf mehrere technischen Komponenten verteilt werden.

IAM-Services sind u.a.:

- *Attribute Assertion Service*
- *Attribute Service*
- *Authentication Service*
- *Autorisation Service*
- *Broker Service*
- *Credential Service*
- *Digitale-Identity Service*
- *Digital-Ressource Service*
- *Discovery Service*
- *Logging Service*
- *Trust Service*
- *Zugriffsrecht Service*

Synonym: IAM-Dienst

2.65 IAM-Support

Der **IAM-Support** [2] ist ein *Akteur* in einem *IAM-System*. Er ist verantwortlich für alle Aktivitäten zum Auffinden und Lösen von Problemen im IAM-System.

2.66 IAM-System

Ein **IAM-System** ist eine Implementierung eines *IAM*s innerhalb eines festgelegten Geltungsbereichs, das von einer *Organisation* eingesetzt wird.

Ein IAM-System umfasst technische *Entitäten* wie *Identity Provider (IdP)* und *Relying Parties (RP)*, die beteiligten Personen der Organisation, wie *Subjekte* und IAM-Verantwortliche, sowie die zugrunde liegenden *Prozesse*, wie z. B. *Registrierung* und Benutzerverwaltung.

Synonym: Identitätssystem

2.67 Identifikator

Ein **Identifikator** ist eine Kennung (z. B. eine Zeichenkette), welche eine *Digitale Identität* oder eine *Digitale Ressource* innerhalb eines *Namensraumes* (*Domäne*) eindeutig bezeichnet. Der *Identifikator* einer *Ressource* ist oft eine URL/URI.

Synonym:

- Engl. Identifier

2.68 Identifizierung

Eine **Identifizierung** ist der Prozess, der zum Erkennen eines *Subjektes* dient und somit eine Prüfung der *Identität* des Subjekts oder einzelner *Eigenschaften* erlaubt. Zur Identifizierung werden *Beweismittel* verwendet. Die Identifizierung wird meist durch eine *Registrierungsstelle* als Teil der *Registrierung* durchgeführt.

Synonym: Identitätsfeststellung, Identifikation, Identitätsabklärungsprozess

2.69 Identität

Identität umfasst *Eigenschaften* eines *Subjektes* oder *Objektes*. Die Identität ist ein Datensatz, der das *Subjekt* bzw. das *Objekt* eindeutig in einem *Namensraum* repräsentiert.

Eine Identität hat einen *Identifikator* (eindeutige Kennung), meist zusammen mit einer Menge von zusätzlichen *Attributen*, welcher innerhalb eines *Namensraumes* (und damit einer *Domäne*) eindeutig einem *Objekt bzw. Subjekt* zugewiesen werden kann.

Die Identität eines *Subjektes* entsteht bei der *Registrierung*, dies kann eine *Identifizierung* beinhalten.

Synonym: Identity (engl.)

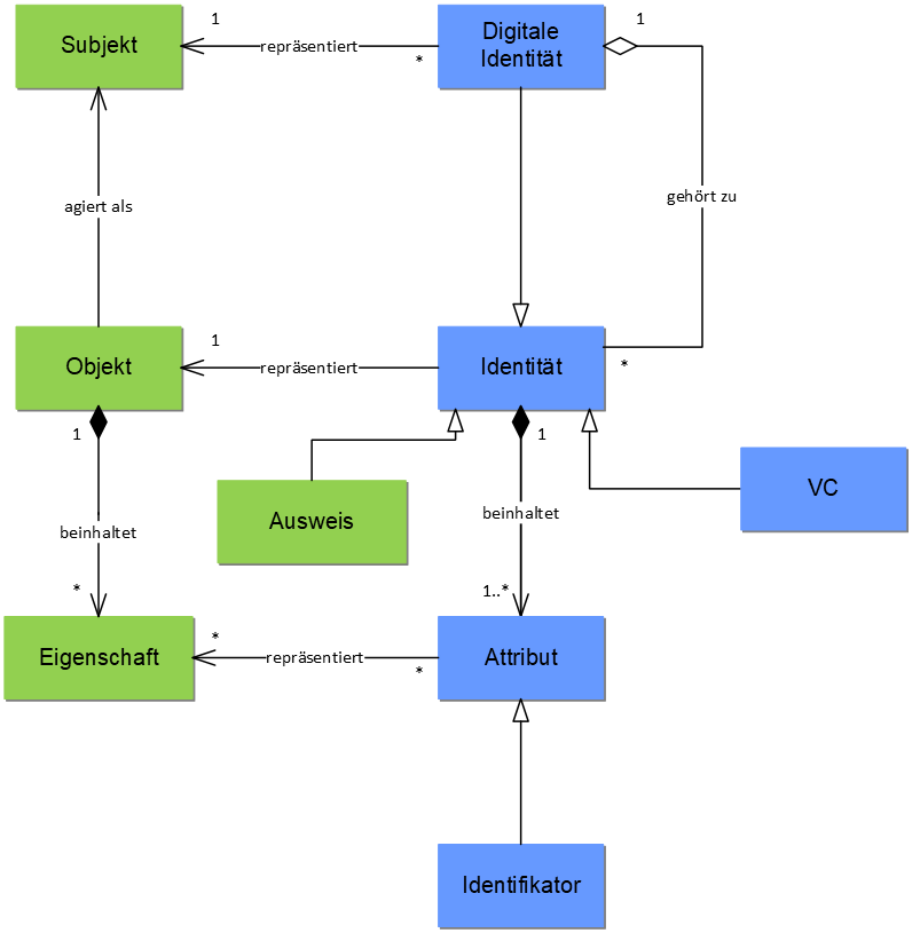


Abbildung 4 - Identität

Beispiele:

- Ein Beispiel für eine Identität ist ein Eintrag in einer Excel- oder einer Datenbank-Tabelle.

2.70 Identitätsdokument

In der Schweiz gelten die folgenden Dokumente als Identitätsdokumente:

- Reisepass,
- Schweizer Identitätskarte,
- eine für die Einreise in die Schweiz anerkanntes Ausweisdokument.

2.71 Identitätsföderierung

Eine **Identitätsföderierung** bezeichnet die Verknüpfung von Identitätssystemen verschiedener *Organisationen* oder *Domänen*, um *Subjekten* eine *Authentifizierung* und *Autorisierung* über System- oder Organisationsgrenzen hinweg zu ermöglichen.

Damit eine Identitätsföderierung etabliert werden kann, müssen sich die verschiedenen Domänen in Bezug auf bestimmte Aspekte gegenseitig vertrauen. Dieses stützt sich auf explizite und implizite Vereinbarungen (*SLA*) ab.

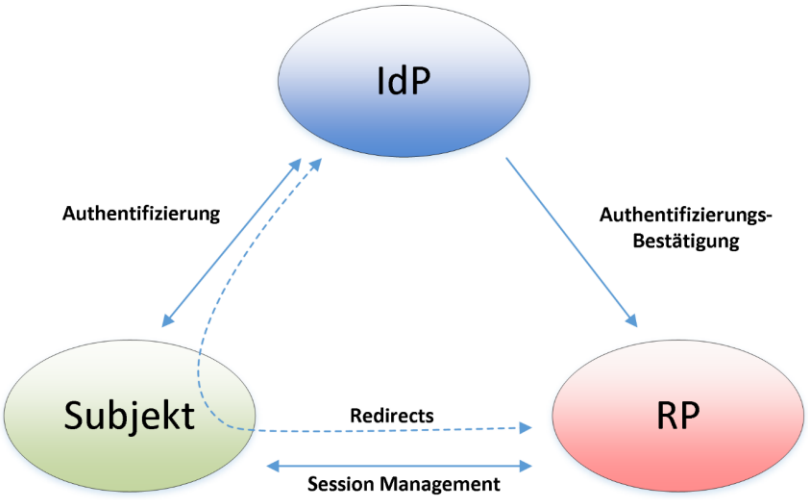


Abbildung 5 - Modell einer Identitäts-Föderierung

Wie in Abbildung 5 dargestellt besteht eine Identitätsföderierung aus den drei *Entitäten* *Subjekt*, *Relying Party* (RP) und einem *Identity Provider* (IdP). Je nach Ausprägung des verwendeten Protokolls ist die Abfolge der Informationen anders. Das Subjekt kommuniziert dabei aber immer mit dem IdP, wie auch mit der RP. Das Subjekt authentisiert sich gegenüber dem IdP. Dieses Ereignis wird dann in Form einer *Authentifizierungsbestätigung* an die RP weitergegeben.

In einer Identitätsföderierung werden Föderierungsprotokolle wie *SAML*, *OAuth 2.0* oder *OpenID Connect* genutzt.

Föderiertes IAM-System im E-Government:
Im E-Government ermöglicht eine *Identitätsföderierung* *Behörden*, *Ressourcen* sowohl für interne Partner (z. B. andere Schweizer Behörden) als auch für externe Partner (z. B. *Personen*, Unternehmen, *Organisationen* oder ausländische Behörden) bereitzustellen. Diese Ressourcen werden genutzt, um definierte Leistungen aus dem Zuständigkeitsbereich der Behörde online verfügbar zu machen. Subjekte aus der eigenen *Domäne* und solche mit *digitalen Identitäten* aus anderen Domänen sollen gleichermassen auf diese Ressourcen zugreifen können. Eine Behörde kann dabei gleichzeitig als *Relying Party* und gegebenenfalls als *IAM-Dienstanbieter* agieren.

Synonyme: föderiertes Identitätssystem, föderiertes IAM, Identity Federation System (engl.) Identity Federation (engl.)

2.72 Identity and Access Management (IAM)

IAM umfasst alles, was die folgenden Fragen bezüglich aller Teilnehmer/-innen in einem System beantwortet:

- Wer bist du?
- Woran erkennt man dich?
- Was darfst du und wozu bist du autorisiert?
- Wie werden die Grenzen deiner Autorisation durchgesetzt?

"*Identity and Access Management (IAM) is a security and business discipline that includes multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons, while keeping unauthorized access and fraud at bay.*"[4]

Synonyme: (dt.) Identitäts- und Zugriffsmanagement

2.73 Identity Linking

Identity Linking erlaubt im organisationsübergreifenden Kontext *digitale Identitäten* aus verschiedenen Domänen miteinander in Beziehung zu setzen und zu verketten.

Identity Linking ist ein Vorgang zur *Definitionszeit*, bei dem zwei digitale Identitäten miteinander verknüpft und diese Verlinkungsinformationen abgelegt werden.

2.74 Identity Mapping

Identity Mapping ist ein Vorgang zur *Laufzeit*, bei welchem Verknüpfungen zwischen digitale Identitäten aufgelöst werden. Eine lokale digitale Identität kann so mit der föderierten digitale Identität verbunden werden.

2.75 Identity Provider (IdP)

Ein **Identity Provider** (IdP) ist eine *Entität*, die *digitale Identitäten* herausgibt und verwaltet. Ein IdP stellt einen *Authentication Service* und optional einen *Attribute Assertion Service* zur Ausstellung von *Attributbestätigungen* zur Verfügung. Ein IdP hat typischerweise eine *Registrierungsstelle*.

Synonym: Authorization Provider, Datenlieferant, Identitätsprovider, Informationslieferant, Authentifikation-Autorität (AuthnA), Authentication Authority (engl.)

[4] Gartner Glossary, https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam, Zugriff: 16.11.2023)

2.76 Inhaberbindung

Inhaberbindung ist ein Konzept der *dezentralen Identitäten*, das sicherstellt, dass eine *digitale Identität* eindeutig einem bestimmten *Subjekt* zugeordnet werden kann.

Da der *Issuer* (Aussteller) der *digitalen Identität* nicht in den Prozess ihrer Nutzung eingebunden ist und dabei keine direkte *Authentifizierung* des Subjekts erfolgt, muss anderweitig sichergestellt werden, dass die präsentierte digitale Identität tatsächlich für das Subjekt ausgestellt wurde, das sie verwendet.

Dies wird üblicherweise durch die Verknüpfung mit einem kryptografischen Schlüssel oder einem Geheimnis des rechtmässigen Subjekts erreicht.

In der Praxis wird die Inhaberbindung häufig mit einer *Gerätebindung* kombiniert.

Synonyme: Holder Binding (engl.), User Binding (engl.)

2.77 Institution

Eine **Institution** ist eine strukturiert agierende *Organisation* mit geregelten Zuständigkeiten, Organisationsstrukturen und definierten Aufgaben definiert.

Dazu gehören:

- *Behörden*
- Unternehmen.

2.78 Issuer

Ein **Issuer** ist eine *Entität*, welche eine bestimmte *Rolle* im SSI-Kontext übernimmt. Der Issuer verifiziert *Claims* über ein oder mehrere *Subjekte* und/oder *Objekte* und stellt dafür *Verifiable Credentials* aus, welche vom *Wallet* des *Holders* übernommen werden können (Freiwilligkeit des Holders).

Synonym: Aussteller

2.79 Juristische Person

Juristische Personen sind Organisationen nach Art. 52 ff ZGB sowie gemäss den einschlägigen Bestimmungen des Gesellschaftsrechtes des OR definiert.
Juristische Personen können nur durch *natürliche Personen* handeln und sind daher immer an mindestens eine *natürliche Person* gebunden.

2.80 Kerberos

Kerberos [11] ist ein netzwerkbasiertes Authentifizierungsprotokoll, das eine gegenseitige *Authentifizierung* zwischen Clients und Diensten (*RP*) ermöglicht. Es verwendet ein Ticket-basiertes System und basiert auf einer zentralen, vertrauenswürdigen Instanz, dem Key Distribution Center (KDC). Das KDC übernimmt die Vergabe von Tickets, wodurch *Single Sign-On (SSO)* ermöglicht wird.

2.81 Körperliches Merkmal

Ein **körperliches Merkmal** ist eine *Eigenschaft* eines Menschen, wie Körpergrösse und Augenfarbe. Spezielle körperliche Merkmale sind die *biometrischen Merkmale*.

2.82 Kryptographischer Token

Ein **kryptographischer Token** ist ein physisches oder virtuelles Sicherheitsgerät (Hardware- oder Softwaremedium), das kryptographische Schlüssel speichert und kryptographische Operationen wie *Authentifizierung*, digitale Signaturen oder Verschlüsselung ausführt, ohne dass die Schlüssel direkt ausgelesen werden können.

Beispiele:

- Software: Microsoft Certificate Manager im Windows OS
- Hardware: SmartCard, USB-Token, Hardware Security Module (HSM)

Synonyme: Zertifikatstoken, Cryptographic Token, Kryptografischer Token

2.83 Laufzeit

Zur **Laufzeit** finden die *digitalen Prozesse* statt, mit denen ein *Subjekt* – im Erfolgsfall – Zugriff auf die *Ressourcen* einer *RP* erhält.

Synonym: Ausführungszeit

Siehe auch: *Definitionszeit*

2.84 Linking Protokoll

Ein **Linking-Protokoll** wird zur Verknüpfung von zwei *digitalen Identitäten* verwendet. (siehe *Identity Linking*)

2.85 Leistungsbezüger (LB)

Der **Leistungsbezüger** [2] ist ein *Stakeholder* in einem *IAM-System*, der eine fachliche Leistung einer *Relying Party* (Bsp. Bestellung einer Parkkarte) online in Anspruch nehmen will.

2.86 Leistungserbringer (LE)

Der **Leistungserbringer** [2] ist ein *Stakeholder* in einem *IAM-System* und möchte fachliche Leistungen online anbieten. Den Zugriff und den Schutz der Ressourcen möchte er gemäss seinen Bedürfnissen (z. B. Risikobereitschaft, Wirtschaftlichkeit) an die *IAM-Dienstanbieter* übertragen.

2.87 Logging Service

Der **Logging Service** [2] ist ein *IAM-Service*, der zur *Laufzeit* die Verwendung eines *IAM-Services* dokumentiert. Er stellt der Support-Organisation die notwendigen Informationen bereit, um Nutzungsprobleme oder Fehler aufzuklären.

2.88 Look-Up Secret

Look-Up Secrets enthalten eine Liste von (alpha-)numerischen Werten, die zuvor zwischen *Subjekt* und *IdP* ausgetauscht wurden. Die ausgetauschten Werte müssen zufällig generiert werden. Sie dürfen nur einmal benutzt werden und müssen eine genügend hohe Entropie besitzen. Look-Up Secrets müssen sicher aufbewahrt werden, um zu verhindern, dass sie in die falschen Hände geraten.

Look-Up Secrets können als 2. Faktor bei einer MFA oder auch als Notfall- oder Backup-Code verwendet werden.

Beispiele: Strichlisten (engl. tally sheet), TAN-Blöcke, Recovery-Codes

Synonym: Nachschlagbares Geheimnis

2.89 Magic Link

Bei **Magic Links** erhält das *Subjekt* einen einzigartigen, einmal verwendbaren Link per E-Mail oder SMS. Wenn das Subjekt auf diesen Link klickt, wird es direkt authentifiziert. Der Link hat oft eine kurze Gültigkeitsdauer. Magic Links gehören zu den Verfahren der *Passwortlosen Authentifizierung*.

2.90 Memorized Secret

Memorized Secrets sind wissensbasierten *Authentifizierungsmittel*, bei denen das *Subjekt* durch das Eingeben eines nur ihm bekannten Geheimnisses authentifiziert wird. Typische Beispiele sind *Passwörter*, PINs (Persönliche Identifikationsnummern) aber auch Sicherheitsfragen.

Memorized Secrets müssen über eine genügend hohe Komplexität und Zufälligkeit verfügen, um von einem Angreifer nicht erraten oder auf sonstige Art und Weise berechnet werden können. Einfache Passwörter oder PINs sind potenziell anfällig für Angriffe wie Phishing oder Brute-Force-Methoden. So legen z. B. Passwort Policies die Regeln zur Länge, Komplexität, Zeichenmix, Ablaufdauer und Wiederverwendung fest und bestimmen somit die Stärke des Memorized Secrets.

Synonym: gespeichertes Geheimnis

2.91 Meta-Attribut

Ein **Meta-Attribut** wird zur Beschreibung und Spezifizierung von *Attributen* verwende, um die Struktur, Bedeutung oder den Zweck von Attributen im Rahmen eines Attribut-Schemas festzulegen oder zu standardisieren. Es liefert also „Daten über Daten“ und unterstützt die Konsistenz und Verwaltung von Informationen über verschiedene Systeme hinweg.

Beispiele für Meta-Attribute sind:

- Attributname (z. B. „Schuhgrösse“),
- Attributdatentyp (z. B. „Integer“) und
- Attributwert (z. B. „39“).

2.92 Metadaten

Metadaten sind strukturierte, ergänzende Informationen. Sie werden für die Durchführung von (IAM)-*Prozessen* benötigt und beschreiben u.a. Daten, Datenstrukturen, verwendete Protokolle oder Auditinformationen (Zeitstempel).

Synonym: Metadata (engl.)

2.93 Namensraum

Anwendungsbereich (z. B. ein Unternehmen, ein Staat, eine Fachgemeinschaft, eine Sprachgemeinschaft), für welchen die Bedeutung einer Kennung oder Zeichenkette (z. B. *Identifikator*) definiert ist.

Innerhalb eines Namensraumes werden *Subjekte* und *Ressourcen* eindeutig bezeichnet, d.h. ihnen ist mindestens ein eindeutiger *Identifikator* (als Teil ihrer digitalen Repräsentation, d.h. der *Digitale Identität* bzw. *Digitalen Ressource*) zugeordnet.

Synonym: Namespace (engl.)

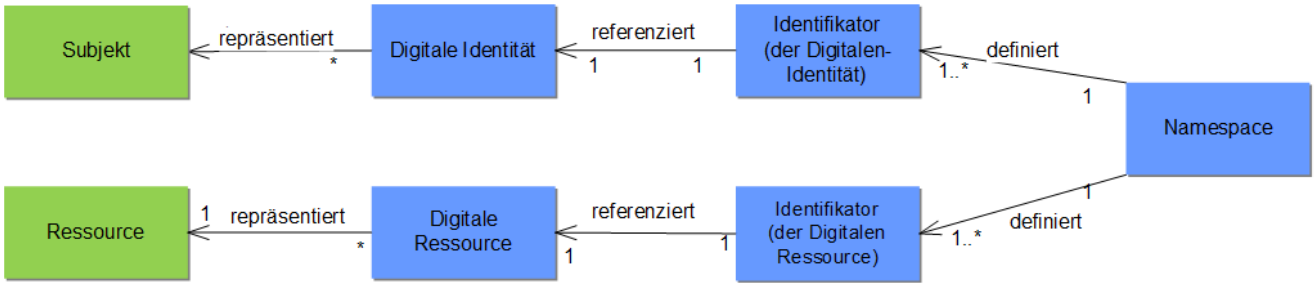


Abbildung 6 - Namespaces & Identifikatoren

2.94 Natürliche Person

Eine **natürliche Person** ist ein Mensch als Rechtssubjekt. Natürliche Personen können zu einer oder mehreren *Organisationen* gehören.

2.95 Netzwerk

Ein **Netzwerk** ist eine Gruppe miteinander verbundener Geräte oder Systeme, die miteinander kommunizieren und Daten austauschen können.

2.96 Nichtabstreitbarkeit

Nichtabstreitbarkeit gewährleistet, dass Daten oder Nachrichten eindeutig einem bestimmten *Subjekt* zugeordnet werden können, wodurch das Subjekt die Urheberschaft nicht bestreiten kann.

In der Praxis wird Nichtabstreitbarkeit mit *digitalen Signaturen* erreicht. Man geht davon aus, dass, wenn eine Signatur mit einem öffentlichen Schlüssel verifiziert wurde, damit auch bewiesen ist, dass die Signatur mit dem zugehörigen privaten Schlüssel erzeugt wurde.

Synonym: Verbindlichkeit, (engl.) Non-repudiation

2.97 OAuth 2.0

OAuth 2.0 [12] ist ein offenes Autorisierungsprotokoll, das Drittanbieteranwendungen ermöglicht, im Namen eines *Benutzers* oder einer Benutzerin auf *Ressourcen* zuzugreifen, ohne dessen Authentifizierungsdaten offenzulegen. Stattdessen basiert es auf Access Tokens, die vom Authorization Server ausgestellt werden.

2.98 Objekt

Ein **Objekt** ist eine *natürliche Person*, eine handelnde *Organisation* oder eine *Entität*, welche an einem *digitalen Prozess* beteiligt ist oder in diesem referenziert wird. Ein Objekt wird zu einem *Subjekt,* wenn es sich in diesem digitalen Prozess authentifiziert.

Eine Übersicht ist in Abbildung 7 dargestellt.

2.99 Online Certificate Status Protocol (OCSP)

OCSP [13] ist ein Protokoll zur Abfrage des Gültigkeitsstatus eines *digitalen Zertifikats*.
Siehe auch *Widerruf* und *Certificate Revocation List* (CRL).

2.100 OpenID Connect (OIDC)

OpenID Connect (OIDC) [14] ist ein offener Standard zur *Authentifizierung*, der auf *OAuth 2.0* aufbaut.

2.101 Organisation

Eine **Organisation** (Unternehmen, Verein, Amtsstelle, Gruppe von Personen) ist eine Gruppe aus mehreren *natürlichen Personen* oder *Dingen*. Eine Organisation kann (Unter-)Organisationen enthalten. Siehe auch Abbildung 7.

Bei Organisationen wird zwischen handelnden und nicht handelnden Organisationen unterschieden. **Handelnde Organisationen** (z. B. Gruppen-Identitäten) können sich authentifizieren und Zugriff zu Ressourcen erhalten. **Nicht handelnde Organisationen** (z. B. *juristische Personen*) können sich nicht selbst authentifizieren, sondern nur über das dazugehörige *Subjekt* (meist eine *natürliche Person*), an das sie ihre Rechte delegieren.

2.102 OTP-Device

Ein OTP-Device ist eine Software oder ein physisches Gerät, das nach einem bestimmten Algorithmus (ereignisbasiert oder zeitbasiert) ein *Einmal-Passwort* generiert. Im OTP-Device ist ein geheimes, eingebettetes Geheimnis (Schlüssel) hinterlegt, das zusammen mit einem Eingabewert (z. B. der aktuellen Zeit oder einem sich inkrementierenden Zähler) zur Generierung des Einmal-Passworts dient.

Ein **Single-Factor OTP Device** benötigt keinen zusätzlichen Authentifizierungsfaktor. Typische Beispiele sind der SafeNet MobilePass oder ein SecureID-Token.

Ein **Multi-Factor OTP Device** erfordert zur Aktivierung des OTP-Algorithmus einen zweiten Authentifizierungsfaktor, beispielsweise in Form eines Wissensfaktors (z. B. eine PIN) oder eines biometrischen Faktors (z. B. Fingerabdruck). Solche Geräte sind häufig mit einem integrierten Keypad, biometrischen Sensoren oder einer Schnittstelle wie USB ausgestattet. Beispiele hierfür sind SecureID-Token mit Keypad oder HID ActivID Token.

Synonym: Einmal-Passwort-Generator

2.103 Out-of-Band Authenticator

Ein **Out-of-Band Authenticator** ist ein *Authentifizierungsmittel*, bei dem ein separater Kommunikationskanal als unabhängiger, zusätzlicher Kanal zur primären Authentifizierungsanfrage dient.

Ein Out of Band Authenticator ist ein physisches Gerät im Besitz des *Subjekts*, welches eindeutig adressierbar sein muss und welches Geheimnisse zur einmaligen Verwendung empfangen kann.

Out of Band Authenticatoren können auf zwei verschiedene Arten funktionieren:

1. Das Subjekt präsentiert das Geheimnis, welches es über den zweiten Kanal erhalten hat, dem authentifizierenden Dienst über den primären Kommunikationskanal.

2. Das Subjekt sendet dem authentifizierenden Dienst eine Antwort direkt über den zweiten Kommunikationskanal zurück.

Beispiele für Out-of-Band-Authentifizierung sind:

- Smartphone mit Mobilnummer und SMS-Code
- Eine *Push-Nachricht*, die an das Mobiltelefon des *Benutzers* oder der Benutzerin gesendet wird, wenn dieser oder diese versucht, sich zu authentifizieren.
- Ein Anruf auf eine zuvor registrierte Telefonnummer zur Verifizierung.

Synonym: Externer Kanal

2.104 Passkey

Ein **Passkey** ist eine *passwortlose Authentifizierungsmethode*, die von FIDO (Fast Identity Online) und Google entwickelt wurde. Sie ermöglicht eine sichere und einfache Möglichkeit, sich auf Websites oder bei Diensten anzumelden, ohne ein herkömmliches Passwort zu verwenden. Stattdessen nutzt ein Passkey biometrische Daten, Sicherheitsschlüssel oder Geräte wie Smartphones.

Wenn ein *Subjekt* sich bei einem Dienst anmeldet, wird der öffentliche Schlüssel, der auf dem Server gespeichert ist, mit dem privaten Schlüssel auf dem Gerät des Subjekts abgeglichen. Das Subjekt bestätigt dann seine Identität entweder mit biometrischen Merkmalen, einem Passwort oder PIN, oder durch die Verwendung eines physischen Geräts.

2.105 Passwort

Ein **Passwort** ist eine vertrauliche Zeichenfolge, die ein *Subjekt* und ein *Verifier* während der *Registrierung* festlegen. Das Passwort kann das Subjekt anschliessend verwenden, um sich gegenüber dem *Verifier* zu authentifizieren.

2.106 Passwortlose Authentifizierung

Passwortlose Authentifizierung ist eine moderne Methode zur Authentifizierung, bei der auf den Einsatz von Passwörtern verzichtet wird.

Gängige Methoden für passwortlose Authentifizierung sind:

- *Biometrische Merkmale* (z. B. Fingerprints oder Gesichtserkennung),
- *Einmal-Passwörter* (z. B. Google Authenticator),
- *Magic Links* (z. B. Slack),
- Hardware-Token (z. B. Yubikey oder Smartcards),
- *Push-Nachrichten*.

Eine passwortlose Authentifizierung ist nicht zu verwechseln mit einer Multi-Faktor-Authentifizierung (MFA), bei welcher als Faktor durchaus ein *Passwort* als *Authentifizierungsmittel* verwendet werden kann.

2.107 Physischer Ausweis

Ein **Ausweis** ist ein physisches Dokument, das *Attribute* zu einer *natürlichen Person* enthält und als Bestätigung oder Legitimation für etwas ausgestellt worden ist (siehe Abbildung 4).

Beispiele: Pass, Kreditkarte, Führerausweis

2.108 Policy

Eine **Policy** umfasst schriftlich festgehaltene Regelungen und Vorschriften, die das gewünschte Verhalten oder die zulässigen Aktionen innerhalb eines Systems, einer *Organisation* oder eines *Prozesses* definiert und steuert.

Beispiel: Eine Policy für ein *IAM-System* ist eine *IAM-Policy*.

2.109 Provisionierung

Provisionierung ist der *Prozess* des Einrichtens, Verwaltens und Entfernens von *Digitalen Identitäten* oder *Benutzer-Accounts* bei *Entitäten* im *IAM-System* (z. B. *IdP*, *RP*). Dabei werden Identitätsdaten meist aus einem zentralen Quell-System an ein oder mehrere Zielsysteme übertragen. Provisionierung kann manuell, automatisiert (einmalig, oder periodisch) oder in hybrider Form erfolgen und umfasst typischerweise die Initialisierung, Aktualisierung, Deaktivierung und Löschung von Digitalen Identitäten bzw. Benutzer-Accounts.

Siehe auch *Identitäts-Föderierung*.

Synonym: Provisioning (engl.)

2.110 Prozess

Ein **Prozess** ist eine strukturierte Reihe von Aktivitäten, die durch bestimmte Eingaben gesteuert, zu einem definierten Ergebnis führen.

2.111 Push-Nachrichten

Eine **Push-Nachricht** ist eine kurze Mitteilung, die direkt von einer App oder einem Dienst an das mobile Gerät des *Subjekts* gesendet wird. Push-Nachrichten werden über spezielle Dienste wie Apple Push Notification Service (APNs) für iOS oder Firebase Cloud Messaging (FCM) für Android versendet.

Eine Push-Nachricht kann zur *Authentifizierung* genutzt werden (Push-Authentifizierung). Ohne einen Code einzugeben, kann das Subjekt die Authentifizierungsanfrage durch Antippen oder Wischen bestätigen.

Eine Push-Nachricht kann auch als *Out-of-Band Authenticator* als 2. Faktor bei einer MFA verwendet werden.

2.112 Qualifizierte elektronischen Signatur (QES)

Eine **qualifizierte elektronische Signatur** kann nach OR Artikel 14 Absatz 2bis rechtlich einer handschriftlichen Unterschrift gleichgestellt werden. Grundsätzlich regelt das Bundesamt für Kommunikation (BAKOM) im Bundesgesetz über die elektronischen Signaturen ZertES [7] anerkannte Signaturen und Siegel.

Die qualifizierte elektronische Signatur (QES) ist eine unverzichtbare Lösung für die rechtskonforme, sichere elektronische Kommunikation und Vertragsabwicklung.

2.113 Qualifiziertes Zertifikat

Ein **qualifiziertes Zertifikat** ist ein auf eine *natürliche Person* ausgestelltes *digitales Zertifikat*, welches die entsprechenden Vorschriften des ZertES [7] erfüllt. Eine qualifizierte elektronische Signatur muss auf einem qualifizierten Zertifikat beruhen.

(Anmerkung: In der EU-Verordnung eIDAS 2024/1183 [8] ist die Definition des qualifizierten Zertifikats weiter gefasst. Dort umfasst dieser Begriff neben dem Zertifikat für qualifizierte elektronische Signatur auch Zertifikate für *elektronische Siegel* und für Website-Authentifizierung.)

2.114 Rechte

Die **Rechte** sind spezifische abstrakte *Eigenschaften*, welche das *Subjekt* besitzen muss, um auf eine *Ressource* zugreifen zu dürfen. Diese können z. B. in Gesetzen oder Verträgen festgelegt sein.

2.115 Register

Ein **Register** ist ein Datenbestand, der von offiziellen Stellen (*Behörden*) geführt wird und für dessen Führung eine explizite gesetzliche Vorschrift besteht. (siehe auch eCH-0177 [5] – Beilage 1)

Beispiele sind Einwohnerregister, Anwaltsregister, Zivilstandsregister, Handelsregister

2.116 Registrierung

Eine **Registrierung** ist ein *Prozess*, bei dem eine *Digitale Identität* für ein *Subjekt* erstellt oder mit einem *Benutzer-Account* verknüpft wird. Die Registrierung beinhaltet meist eine *Identifizierung*.

Synonym: Registration (engl.), Onboarding (engl.)

2.117 Registrierungsstelle / Registration Authority (RA)

Eine **Registrierungsstelle** ist eine *Entität*, die die Ausstellung einer *Digitalen Identität* für ein zuvor überprüftes *Subjekt* autorisiert. Dazu überprüft die Registrierungsstelle die vom Subjekt vorgewiesenen oder anderweitig erhobenen *Beweismittel*.

Die RA kann ein integraler Bestandteil eines *IdPs* sein oder als eigener Dienst im Auftrag des IdPs handeln.

2.118 Regulator

Der **Regulator** [2] ist ein *Stakeholder* in einem *IAM-System* und möchte die Interoperabilität (insbesondere bei selbstständig geführten Teilsystemen), Robustheit und Sicherheit des IAM-Gesamtsystems sicherstellen.

2.119 Relying Party (RP)

Die **Relying Party** [2] ist ein *Akteur* in einem *IAM-System*. Sie ist zuständig für die *Zugriffskontrolle* auf ihre *Ressourcen*. Sie nutzt IAM-Geschäftsservices [2] und verarbeitet Informationen von *IAM-Dienstanbietern* zu deren Schutz. Sie braucht zur Beurteilung der Berechtigung eines Ressourcenzugriffs Informationen zu einem *Subjekt*, d.h. dessen *digitale Identität* mit den berechtigungsrelevanten Attributen, und den Kontext des Zugriffs (Lokation, Zeitpunkt, Sicherheitsniveau etc.).

Synonyme: Informationsbezüger, Informationskonsument, Identitätskonsument, Lösungsanbieter, SAML Service Provider, Verifier

2.120 Ressource

Ressourcen sind Services oder Daten, auf welche ein *Subjekt* zugreifen kann. Dies schliesst physische Ressourcen wie Gebäude und Anlagen, deren Benutzung über IT-Systeme gesteuert wird, ein.

Es wird zwischen drei Arten von Ressourcen unterschieden:

- **öffentliche** (nicht schützenswerte) Ressourcen: Diese Ressourcen sind freizugänglich und benötigen zum Zugriff keinerlei Authentisierung oder Autorisierung. Beispiele sind informative Webseiten (Lesezugriff) und öffentliche Daten.
- **versteckte** Ressourcen: Diese Ressourcen erfordern ebenfalls keine Authentifizierung/Autorisierung vor dem Zugriff, aber die Ressource ist nicht allgemein verfügbar, sondern nur einer Menge von Benutzer/-innen bekannt. Jeder der die entsprechende URL kennt, kann auch auf die Ressource zugreifen. Beispiele sind Zugriffe auf Google-Docs oder Doodle-Links.
- **schützenswerte** (nicht öffentliche) Ressourcen: Diese Ressourcen erfordern eine erfolgreiche Authentifizierung und Autorisierung des zugreifenden Subjektes.

2.121 Ressourcen-Verantwortlicher

Der Ressourcen-Verantwortliche ist die verantwortliche Stelle für die von der *Relying Party* verwalteten *Ressourcen* (z. B.: Anwendungsverantwortlicher, Serviceverantwortlicher, Dateninhaber).

2.122 Rolle

Eine **Rolle** ist eine Sammlung von *Berechtigungen* für Gruppen von *Subjekten*, die mit einer bestimmten Funktion oder Aufgabe in der *Organisation* verknüpft sind.

Synonym: Role (engl.)

2.123 Rollenbasierte Zugriffskontrolle (RBAC)

Die **Rollenbasierte Zugriffskontrolle (RBAC)** [15] bezeichnet eine Art der *Zugriffskontrolle*, mit welcher eine *Relying Party* den Zugang zu einer *Ressource* aufgrund der *Rollen* eines *Subjekts* in einer *Organisation* autorisiert.

Synonym: Role based Access Control (engl.)

2.124 Security Assertion Markup Language (SAML)

SAML [16] ist ein Standard, der den sicheren und standardisierten Austausch von *Authentifizierungs-* und *Attributinformationen* ermöglicht. Es definiert dabei sowohl die Struktur von SAML-Assertions, als auch die zugehörigen Protokolle und Bindings zur Übertragung der Assertions [17]. SAML findet häufig Anwendung in *Single Sign-On (SSO)*-Szenarien (siehe SAML 2.0 Web Browser SSO Profil [18])

SAML ist die Grundlage für weitere Sicherheitsprotokolle, wie WS-Federation [19], WS-Trust [20] und WS-Security [21].

2.125 Security Token

Ein **Security Token**[5] [21] ist Datenpaket, dass *Claims* über ein *Subjekt* enthält und das verwendet werden kann, um den Zugriff auf eine *Ressource* zu autorisieren.

Synonym: Sicherheits-Token

2.126 Security Token Service

Ein **Security Token Service** (STS) ist ein Dienst, der Security Token gemäss WS-Security Spezifikation [21] ausstellt, um *Subjekte* zu authentifizieren und ihnen den Zugriff auf geschützte *Ressourcen* zu ermöglichen.

2.127 Selektive Offenlegung

Selektive Offenlegung bezeichnet die gezielte und kontrollierte Weitergabe spezifischer Informationen aus einer grösseren Menge signierter Daten. Dies ermöglicht es, nur die für einen bestimmten Zweck erforderlichen Daten zu teilen, ohne zusätzlich unnötige Daten offenzulegen und trotzdem die Integrität und Authentizität der Daten zu gewährleisten.

Synonym: Selective Disclosure (engl.)

[5] Der Begriff wird mit einer abweichenden Bedeutung auch im Kontext von Kryptowährungen und Blockchain-Technologie verwendet.

2.128 Self-Sovereign Identity (SSI)

Self-Sovereign Identity (SSI) ist ein Konzept zur dezentralen und sicheren Verwaltung von *Verifiable Credentials*. *Issuer* stellen *Verifiable Credentials (VCs)* mit *Claims* über *Subjekte* oder *Objekte* aus. Die *Holder* speichern diese Credentials dezentral (z. B. auf einem Mobiltelefon) und können sie einem *Verifier* präsentieren.

SSI ermöglicht die räumliche und zeitliche Trennung zwischen der Ausstellung eines *Verifiable Credentials* und seiner Präsentation. Dies ermöglicht einem *Holder*, ein Credential zu präsentieren, ohne dass der *Issuer* (im Gegensatz zu *Attribute Providern* oder *Identity Providern*) involviert wird. Dies erhöht die Privatsphäre der *Holder*.
Des Weiteren können *Holder* entscheiden, welche *Verifiable Credentials* oder Teile davon sie präsentieren, optional als *Verifiable Presentation*.

2.129 Service

Ein **Service** ist eine digitale Dienstleistung, die über ein *Netzwerk* bereitgestellt. Services können Anwendungen, Datenbanken, APIs, Server o.ä. umfassen, die bestimmte Funktionen oder Informationen zur Verfügung stellen.

Synonym: Dienst

2.130 Service Level Agreement (SLA)

Ein **Service Level Agreement (SLA)** ist eine vertragliche Vereinbarung zwischen Auftraggeber und Auftragnehmer, welche die erwarteten Leistungen, Qualitätsstandards und Verantwortlichkeiten für einen Service klar definiert und messbar macht.

2.131 Single Sign-On (SSO)

Single Sign-On (SSO) ist ein Authentifizierungsverfahren, bei dem sich ein *Subjekt* einmalig authentifiziert, um Zugriff auf mehrere *Ressourcen* zu erhalten, ohne sich jedes Mal erneut *authentifizieren* zu müssen.

SSO wird häufig durch zentrale Authentifizierungsdienste wie *Identity Provider (IdP)* und Protokolle wie *Kerberos*, *SAML* oder *OIDC* ermöglicht.

2.132 Staatlich anerkannte elektronische Identität (E-ID)

Eine **staatlich anerkannte elektronische Identität (E-ID)** ist eine von einer staatlichen oder staatlich anerkannten Stelle ausgestellte *digitale Identität*, die zur sicheren und rechtlich verbindlichen *Identifizierung* von Personen in Online-Services verwendet werden kann.

2.133 Stakeholder

Die **Stakeholder** [2] im IAM-Kontext sind Realweltobjekte, d.h. Personen, Gruppen von Personen oder *Organisationen*, die gemeinsame Interessen im *IAM* haben. Stakeholder haben Anforderungen an die verschiedenen *Akteure* in einem *IAM-System*.

Es gibt u.a. die folgenden Stakeholder in einem IAM-System:

- *Leistungsbezüger*,
- *Leistungserbringer*,
- *Dienstanbieter*,
- *Führung*,
- *Regulator*.

2.134 Subjekt

Ein **Subjekt** [2] ist ein *Akteur* in einem *IAM-System* und möchte in einem *digitalen Prozess* auf eine *Ressource* zugreifen.

Ein Subjekt kann mehrere digitale Repräsentationen, sog. *digitale Identitäten,* in einer *Domäne* haben.

Ein Subjekt kann die *Rechte* an ein weiteres Subjekt delegieren.

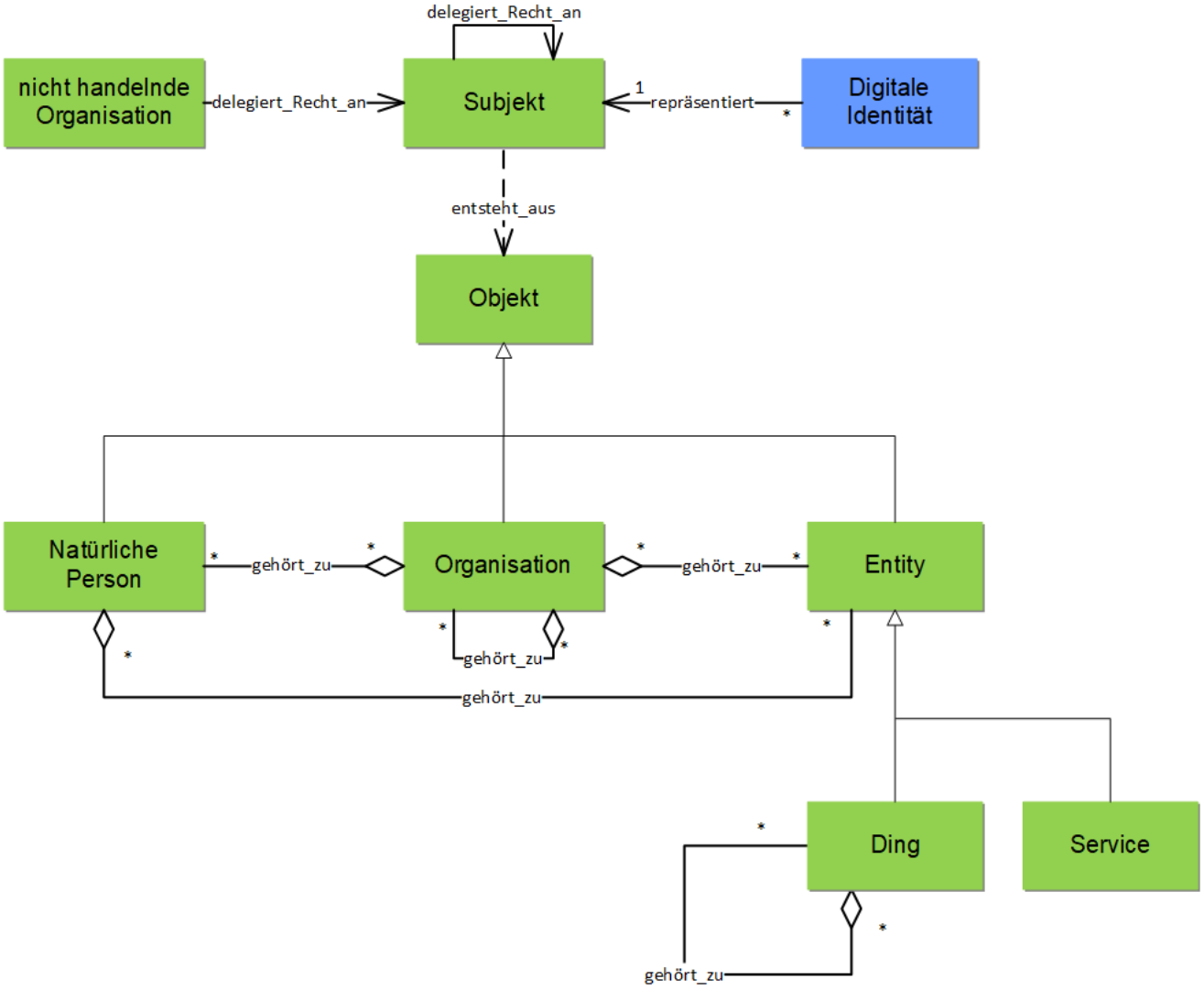


Abbildung 7 - Objekt und Subjekt

Abbildung 7 zeigt welche Objekte in welchen enthalten sein können (z. B. *Organisationen* können mehrere (Unter-)Organisationen enthalten).

Synonyme:

- Eine *natürliche Person*, die als Subjekt agiert, wird häufig als *Benutzer/-in* bezeichnet.
- Im *SSI*-Kontext wird das Subjekt meist als *Holder* bezeichnet.
- *Abonnent/-in*
- *Überbringer/-in*

2.135 Topologie

Die **Topologie** eines *IAM-Systems* beschreibt die Anordnung der verschiedenen *Entitäten*, wie *IdP* oder *RP* und ihre logischen Verbindungen.

2.136 Trust Service

Der **Trust Service** [2] ist ein *IAM-Service*, der die akzeptierten, vertrauenswürdigen *IAM-Dienstanbieter* und *Relying Parties* in einem *IAM-System* pflegt.

2.137 Trusted Third Party

Eine **Trusted Third Party** ist eine unabhängige, vertrauenswürdige *Entität*, die in Sicherheits- und Identitätsmanagementsystemen die Authentizität, Integrität oder Vertraulichkeit von Informationen und Transaktionen sicherstellt.

Beispiele sind:

- *Certification Authority* (CAs) in einer Public Key Infrastructure (PKI)
- *Identity Provider* (IdP) in *Identitätsföderierungen*.

2.138 UID-Einheit

UID-Einheiten sind nach Art. 3.c des Bundesgesetzes über die Unternehmens-Identifikationsnummer (UIDG) [22] festgelegt.

Bei UID-Einheiten handelt es sich um alle Unternehmen und *Institutionen*, die eine UID erhalten. Im UID-System ist der Unternehmensbegriff weit gefasst. Unter UID-Einheit versteht man somit nicht nur alle in der Schweiz tätigen Unternehmen im eigentlichen Sinn, sondern alle «Kundinnen und Kunden der öffentlichen Verwaltung», die Charakteristiken eines Unternehmens aufweisen oder die zu rechtlichen, administrativen oder statistischen Zwecken identifiziert werden.

2.139 Überbringer/-in

Ein **Überbringer** oder eine Überbringerin ist ein *Subjekt*, das eine vom *IdP* ausgestellte *Authentifizierungsbestätigung* an die *RP* übergibt. (siehe *Holder of Key (HoK)*)

Synonym: Bearer (engl.)

2.140 Verifiable Credential (VC)

Ein ***Verifiable Credential*** ist ein signiertes Datenpaket, das *Claims* über ein oder mehrere *Subjekte* und/oder *Objekte* enthält und von einem *Issuer* ausgestellt wird. Ein Verifiable Credential ist ein integritätsgeschützter Nachweis, dessen Urheberschaft idealerweise bewiesen werden kann. Ein Verifiable Credential kann direkt oder als *Verifiable Presentation* einem *Verifier* präsentiert werden.

Verifiable Credentials können Metadaten enthalten, welche die VCs beschreiben, wie z. B. *Issuer* oder Ablaufdatum.

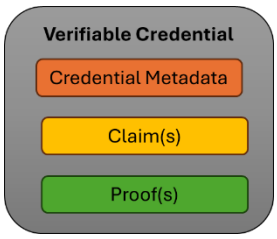


Abbildung 8 - Schematischer Aufbau eines Verifiable Credentials

Synonym: überprüfbarer digitaler Nachweis

2.141 Verifiable Data Registry

Ein **Verifiable Data Registry (VDR)** ist ein Service im *SSI*-Kontext, welcher als vertrauenswürdige und transparente Datenquelle für die dezentrale Verifizierung der Authentizität und Gültigkeit von *Verifiable Credentials (VC)* dient. Das VDR speichert und verwaltet dafür Schemas, Identifikatoren, Revokationslisten sowie öffentliche Schlüssel der *Issuer* und *Verifier*.

2.142 Verifiable Presentation (VP)

Eine **Verifiable Presentation** ist ein signiertes Datenpaket, welches *Verifiable Credentials* verschiedener *Issuer* oder Teile davon enthält und vom *Wallet* des *Holders* erstellt wird. Verifiable Presentations erlauben die selektive Offenlegung von *Claims* aus *Verifiable Credentials*. Der Holder übermittelt die erstellte *Verifiable Presentation* mit Hilfe seines *Wallets* an den *Verifier*.

Eine Verifiable Presentation enthält Metadaten, *Verifiable Credentials* oder Teile davon sowie kryptographische Nachweise (Proofs) (siehe Abbildung 9). Die Metadaten beschreiben die VP, wie z. B. Ablaufdatum. Die Proofs können unterschiedliche Zwecke, z. B. *Inhaber*- oder *Gerätebindung* sowie Integritätsschutz, haben.

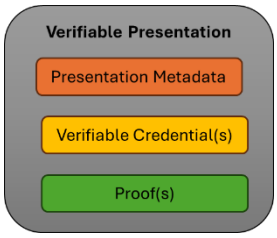


Abbildung 9 - Schematischer Aufbau einer Verifiable Presentation

2.143 Verifier

Der Begriff **Verifier** bezeichnet eine prüfende Instanz. Je nach Kontext wird unterschieden, was verifiziert wird.

1. Klassisches *IAM-System*: Der **Verifier** ist Teil eines *Identity* Providers *(IdP)* oder einer *Relying Party* (RP). Er authentifiziert das *Subjekt* mit Hilfe seines *Authentication Service*, indem er den vom Authentifikator gelieferten Ausgabewert mit den bei ihm gespeicherten *Credentials* abgleicht. Dadurch bestätigt er die behauptete *Digitale Identität* des Subjekts.

2. *SSI*: Ein **Verifier** ist eine Rolle, welche eine *Entität* im SSI-Kontext übernimmt. Ein Verifier verifiziert die Integrität, Gültigkeit und im Idealfall die Urheberschaft von *Verifiable Credentials* bzw. *Verifiable Presentations*, die er vom *Wallet* eines *Holders* erhält.

2.144 Verlässliche Quelle

Eine **verlässliche Quelle** ist eine beliebige Informationsquelle, welche bezogen auf eine konkrete Situation als vertrauenswürdig betrachtet wird.

eIDAS 2015/1502 [23]: «„**Verlässliche Quelle**“ ist eine beliebige Informationsquelle, die auf verlässliche Weise präzise Daten, Informationen und/oder Beweismittel bereitstellt, die zum Identitätsnachweis verwendet werden können.»

Verlässliche Quellen können viele verschiedene Formen haben, z. B. Register, Urkunden usw.

eIDAS 2024/1183 [8] definiert zusätzlich: «„**Authentische Quelle**“ ist ein Datenspeicher oder ein System, der bzw. das unter der Verantwortung einer öffentlichen Stelle oder privaten Einrichtung betrieben wird, Attribute zu einer natürlichen oder juristischen Person oder zu einem Objekt enthält und bereitstellt und als eine primäre Quelle für diese Informationen gilt oder im Einklang mit Unionsrecht oder nationalem Recht — einschliesslich der Verwaltungspraxis — als authentisch anerkannt wird.»

2.145 Vermittler

Ein Vermittler bietet gemeinsame Dienste, wie Metadatenverwaltung, IdP-Discovery (*Discovery Service*), *Identity Linking* oder Transformation der *Authentifizierungs*- und *Attributbestätigung* (*Broker Service*), für alle anderen *IAM-Dienstanbieter* und *Relying Parties* in einer *Identitätsföderierung* nach dem Hub-'n'-Spoke Modell an. Ein integraler Bestandteil eines Vermittlers ist immer ein *Authentication Proxy*.

Synonym: Hub, Broker (engl.)

2.146 Vertrauen

Vertrauen im IAM-Kontext ist die bewusste Entscheidung, die Authentizität und Integrität eines Teilnehmers in einem *Prozess* zu akzeptieren, obwohl ein Risiko besteht, dass diese Erwartungen nicht erfüllt werden.

Vertrauen ist essenziell in *IAM-Systemen*, da es die Interaktion trotz unvermeidbarer Unsicherheiten ermöglicht. IAM-Systeme sind darauf ausgelegt, ein definiertes Mass an Sicherheit und Zuverlässigkeit zu gewährleisten und das Risiko beherrschbar zu machen. Sie schaffen damit das nötige Vertrauen.

Formell wird Vertrauen zwischen zwei *Organisationen*, *Entitäten*, *Domänen* meist in *SLA* festgelegt.

Synonym: Trust (engl.)

2.147 Vertrauensstufe

Die **Vertrauensstufe** besagt mit welcher Qualität ein *Subjekt* authentifiziert wurde, dabei wird zwischen natürlichen und juristischen Personen unterschieden. So kann man z. B. mit dem Modell aus eCH-0170 [24] anhand von 4 Teilmodellen (Vertrauensstufe der Authentifizierung, Vertrauensstufen der Registrierung, Vertrauensstufen der Steuerung und Vertrauensstufen der Föderierung) die Gesamt-Vertrauensstufe bestimmen.

Synonym: Vertrauensniveau

2.148 Wallet

Ein **Wallet** ist eine digitale Anwendung, die es *Subjekten* ermöglicht, ihre kryptographischen Schlüssel, *Verifiable Credentials* o.ä. dezentral abzulegen, zu verwalten und zu nutzen.

Synonym: Identity Wallet (engl.)

2.149 Widerruf

Der **Widerruf** bezeichnet den *Prozess* zur Erklärung der Ungültigkeit von *Berechtigungen*, *Authentifizierungsmitteln*, *digitalen Zertifikaten*, *Verifiable Credentials* o.ä. Durch den Widerruf wird sichergestellt, dass ein bestimmtes Element nicht mehr vertrauenswürdig ist und nicht mehr verwendet werden kann.

Beispiele:

- Ein Issuer kann die von ihm herausgegebenen digitalen Zertifikate oder Verifiable Credentials revozieren. Siehe auch *OCSP* und *CRL*.
- Eine *Relying Party* entzieht einem *Subjekt* die *Berechtigung* auf eine *Ressource*.
- API-Tokens: Ungültigmachen von kompromittierten oder veralteten Tokens.
- *OTP-Devices*: Einmal-Passwort-Generatoren können widerrufen werden.
- Aktive Session-Tokens werden z. B. bei einem Sicherheitsvorfall widerrufen.

Synonyme: Revokation, Revocation (engl.), Sperrung

2.150 Zugriffsrecht Service

Der **Zugriffsrecht Service** [2] ist ein *IAM-Service*, der die Regeln für die Nutzung einer *digitalen Ressource* verwaltet. Die Regeln sind auf der Basis von *Authentisierung*, *Attributen*, Kontext des Zugriffs (Lokation, Zeitpunkt, Vertrauensstufe usw.) oder eigenen Modellen (Gruppen, *Rollen*, Einzelberechtigungen) definiert.

Synonym: Zugangsregel Service

2.151 Zugriffskontrolle

Zugriffskontrolle ist ein Prozess zur Überwachung und Steuerung der Nutzung von *Ressourcen*. Das Ziel ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen. Integrale Bestandteile der Zugriffskontrolle sind *Authentifizierung* und *Autorisierung* der zugreifenden Subjekte.

Zur Gewährleistung der Nachvollziehbarkeit und Nachweisbarkeit werden die Zugriffsentscheide in der Regel protokolliert.

Zugriffsentscheide erfolgen in der Regel automatisch auf der Grundlage der Attribute oder Rollen eines authentifizierten *Subjekts* (*ABAC* bzw. *RBAC*) und ggf. weiteren Informationen (z. B. Kontext des Zugriffs, wie Lokation, Zeitpunkt, Sicherheitsniveau usw.).

Synonym: Access Control (engl.)

2.152 Zero-Knowledge Proof (ZKP)

Bei **Zero Knowledge Proof** unterscheidet man zwischen einem interaktiven und einem nicht interaktiven Verfahren.

Das interaktive Verfahren ist ein spezielles *Challenge Response* Verfahren. Der Prüfer eines Beweises (Verifier) kann bei ZKP einem Dritten nicht darlegen, dass der Prover diesen Beweis erbracht hat. Der Prover kann folglich gegenüber dem Dritten *abstreiten*, den Beweis erbracht zu haben.

Das nicht interaktive Verfahren wird aus dem interaktiven abgeleitet. Beim nicht interaktiven Verfahren wird unterschieden, ob der Prover vermag, den von ihm erbrachten Beweis abzustreiten, oder nicht. Den Beweis eines nicht interaktiven Verfahrens wird des Öfteren auch als Signatur bezeichnet.

3 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** den Benutzenden zur unentgeltlichen Nutzung zur Verfügung stellen oder welche **eCH** referenzieren, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche den Benutzenden auf Grund dieser Dokumente trifft und / oder ergreift. Die Benutzenden sind verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit der Benutzenden, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche den Benutzenden aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

4 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichten sich die Erarbeitenden, ihr betreffendes geistiges Eigentum oder ihre Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen urhebenden Person von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Anhang A – Referenzen & Bibliographie

[1] NIST, «NIST Special Publication 800-63B - Digital Identity Guidelines,» June 2017. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html.

[2] eCH, «eCH-0107 Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM), V3.0,» 14 01 2019. [Online]. Available: https://ech.ch/de/ech/ech-0107/3.0.

[3] NIST, «Attribute Based Access Control ABAC,» 24 Mai 2016. [Online]. Available: https://csrc.nist.gov/Projects/Attribute-Based-Access-Control.

[4] OASIS, «Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0,» 15 March 2005. [Online]. Available: https://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf.

[5] eCH, «eCH-0177 Informationsmodell zur Geschäftsabwicklung in einer Vernetzten Verwaltung Schweiz,» 24 Februar 2016. [Online]. Available: https://ech.ch/de/ech/ech-0177/1.0.

[6] NIST, «Strength of Function for Authenticators - Biometrics (SOFA-B),» 16 October 2023. [Online]. Available: https://pages.nist.gov/SOFA/. [Zugriff am 2024].

[7] Schweizerische Eidgenossenschaft, «Bundesgesetz über die elektronische Signatur, ZertES,» 01 01 2020. [Online]. Available: https://www.fedlex.admin.ch/eli/cc/2016/752/de.

[8] DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION, «Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität,» 11 4 2024. [Online]. Available: http://data.europa.eu/eli/reg/2024/1183/oj.

[9] ISO/IEC JTC 1, «ISO/IEC 29115:2013,» ISO/IEC, 2013.

[10] Wikipedia, 29 Dezember 2024. [Online]. Available: https://de.wikipedia.org/wiki/Personalausweis_(Deutschland)#Der_elektronische_Personalausweis_(nPA). [Zugriff am 17 Januar 2025].

[11] C. Neumann, T. Yu, S. Hartman und K. Raeburn, «RFC 4120: The Kerberos Network Authentication Service (V5),» Juli 2005. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4120.html. [Zugriff am 24 Januar 2025].

[12] T. Hardt, «RFC 6749: The OAuth 2.0 Authorization Framework,» Oktober 2012. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6749.html. [Zugriff am 24 Januar 2025].

[13] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin und C. Adams, «X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP,» [Online]. Available: https://datatracker.ietf.org/doc/html/rfc6960.

[14] N. Sakimura, NAT.Consulting, J. Bradley, Yubico, M. Jones, Self-Issued Consulting, B. de Medeiros, Google, C. Mortimore und Disney, «OpenID Connect Core 1.0 incorporating errata set

] 2,» 15 Dez. 2023. [Online]. Available: https://openid.net/specs/openid-connect-core-1_0.html.

[15] NIST, «Role Based Access Control RBAC,» 21 November 2016. [Online]. Available: https://csrc.nist.gov/projects/role-based-access-control.

[16] OASIS, «Security Assertion Markup Language (SAML) V2.0 Technical Overview,» 25 March 2008. [Online]. Available: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.

[17] OASIS, «Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard,» 15 March 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[18] OASIS, «Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0,» März 2005. [Online]. Available: https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.

[19] OASIS, «Web Services Federation Language (WS-Federation) Version 1.2,» May 2009. [Online]. Available: https://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.htm.

[20] OASIS, «WS-Trust 1.4,» April 2012. [Online]. Available: https://docs.oasis-open.org/ws-sx/ws-trust/v1.4/errata01/ws-trust-1.4-errata01-complete.html.

[21] OASIS, «Web Services Security: SOAP Message Security Version 1.1.1,» May 2012. [Online]. Available: https://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SOAPMessageSecurity-v1.1.1.html.

[22] Bundesversammlung der Schweizerischen Eidgenossenschaft, «Bundesgesetz über die Unternehmens-Identifikationsnummer (UIDG) vom 18. Juni 2010 (Stand am 1. September 2023),» [Online]. Available: https://lex.weblaw.ch/lex.php?norm_id=431.03&source=SR&lex_id=83199&file=de-pdf_file_a.pdf.

[23] DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION, «VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES,» 28 8 2014. [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32014R0910.

[24] eCH, «eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten, V2.0,» 9 Oktober 2017. [Online]. Available: https://ech.ch/de/ech/ech-0170/2.0.

[25] eCH, «eCH-0219 - IAM Glossar V2.0.0,» 2025. [Online]. Available: https://ech.ch/de/ech/ech-0219/2.0.0.

Anhang B – Mitarbeit & Überprüfung

Dominic Baumann	BFH

Gerhard Hassenstein	BFH
Annett Laube	BFH
Daniel Muster	it-rm IT-Riskmanagement GmbH

Anhang C – Abkürzungen

2FA	Zwei-Faktor-Authentifizierung
ABAC	Attribute Based Access Control (Attributbasierte Zugriffskontrolle)
AD	Active Directory
AP	Attribute Provider
CA	Certification Authority
CRL	Certificate Revocation List
CP	Certificate Policy
EIDAS	Electronic Identification and Trust Services Regulation
FIDO	Fast IDentity Online
HoK	Holder of Key
IAM	Identity and Access Management
IdP	Identity Provider
IoT	Internet of Things
JWT	JSON Web Token
LB	Leistungsbezüger
LE	Leistungserbringer
MFA	Multi-Faktor-Authentifikator / Mehr-Faktoren-Authentifizierung
NIST	National Institute of Standards and Technology
nPA	Neuer Personalausweis
OCSP	Online Certificate Status Protocol
OIDC	OpenID Connect
OTP	One-Time Password / Einmal-Passwort
PIN	Persönliche Identifikationsnummer
PKI	Public Key Infrastructure
RA	Registration Authority
RP	Relying Party
QES	Qualifizierte elektronischen Signatur
RBAC	Role based Access Control (Rollenbasierte Zugriffskontrolle)
RP	Relying Party
SAML	Security Assertion Markup Language

SFA	Single-Faktor-Authentifikator / Single-Faktoren-Authentifizierung
SLA	Service Level Agreement
SSL	Self-Sovereign Identity
SSO	Single Sign On
STS	Security Token Service
TSP	Trust Service Provider
UID	Unique Identifier
VC	Verifiable Credential
VDA	Vertrauensdiensteanbieter
VDR	Verifiable Data Registry
VP	Verifiable Presentation
WAYF	Where Are You From (Discovery Service)
ZKP	Zero Knowledge Proof

Anhang D – Änderungen gegenüber Vorversion

Alle Begriffe des Standards Version 1.0 wurden überarbeitet und angepasst. Nachfolgend werden die neuen, umbenannten und gelöschten Begriffe aufgelistet.

Neue Begriffe:

- Abonnent/-in
- Akteur
- Antragsteller/-in
- Auth 2.0
- Benutzer-Account
- Challenge Response
- Claim
- Dezentrale Identität
- Digitale Identität
- Digitaler Prozess
- Digitale Signatur
- Elektronisches Identifizierungsmittel
- Elektronisches Identifizierungssystem
- Gerätebindung
- Holder
- Holder of Key (HoK)
- IAM
- Inhaberbindung
- Institution
- Issuer
- Kerberos
- Magic Link
- Objekt
- Passkey
- Passwort
- Passwortlose Authentifizierung
- Physischer Ausweis
- Prozess
- Provisionierung
- Push-Nachricht
- Selektive Offenlegung
- Self Soverein Identity (SSI)
- SSO
- Stakeholder
- Verifiable Credential (VC)
- Verifiable Data Registry
- Verifiable Presentation (VP)
- Verifier (2. Bedeutung)

- Wallet
- ZKP

Umbenannte Begriffe:

- E-Ressource -> Digitale Ressource
- E-Ressource Service -> Digitale-Ressource Service

Gelöschte und zusammengeführte Begriffe:

- Anbieterin von Zertifizierungsdiensten
- Artefakt
- Attribut-Autorität (AA)
- Attributaggregation
- Attributanfrage
- Authentifikation-Autorität (AuthnA)
- Authentifizierungsanfrage
- Authentifizierungsfaktor
- Authentifikator
- Ausgabewert eines Authentifikators
- Backend Attribute Exchange (BAE)
- Benutzerzentriertes Identitätsmanagement
- Community Metadaten
- Empfängerbaustein
- Entitätsmetadaten
- Föderiertes IAM-System
- Funktion
- Globally Unique Identifier (GUID)
- Identity and Attribute Provider (IdP/AP)
- LinkedID
- Meta-Domäne
- Qualität Authentication Assurance (QAA)
- Replizierendes IAM-System
- Service Provider (SP)
- STIAM - SuisseTrust Identity and Access Management
- STIAM Certificate Authority (STIAM-CA)
- STIAM Identity und Attribute Bus
- STIAM-Community
- STIAM-Empfänger
- STIAM-Hub
- STIAM-IdP
- STIAM-Komponente
- STIAM-Metadata Repository (STIAM-MDR)

- STIAM-Plattform
- STIAM-RLM (Reporting-Logging-Monitoring)
- STIAM-Sender
- Verzeichnis
- Verwaltung
- WS-Federation
- WS-Trust

Anhang E – Abbildungsverzeichnis

Abbildung 1 - Schematische Funktionsweise eines Authentifizierungsmittels 13

Abbildung 2 - Einzelne und verknüpfte Claims im Kontext SSI 18

Abbildung 3 - Übersicht der verschiedenen digitalen Zertifikate 24

Abbildung 4 - Identität 27

Abbildung 5 - Modell einer Identitäts-Föderierung 28

Abbildung 6 - Namespaces & Identifikatoren 33

Abbildung 7 - Objekt und Subjekt 43

Abbildung 8 - Schematischer Aufbau eines Verifiable Credentials 45

Abbildung 9 - Schematischer Aufbau einer Verifiable Presentation 45

Anhang F – Tabellenverzeichnis

Tabelle 1: Beispiele für Authentifizierungsmittel 14