eCH-0219 IAM Glossar

Name	IAM Glossar
eCH-Nummer	eCH-0219
Kategorie	Standard
Reifegrad	Definiert
Version	1.0
Status	Genehmigt
Beschluss am	2018-11-28
Ausgabedatum	2019-01-16
Ersetzt Version	-
Voraussetzungen	-
Beilagen	eCH-0219-IAM-Glossar_Hilfsmittel.xlsx
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Autoren	Fachgruppe IAM Annett Laube-Rosenpflanzer, BFH TI, annett.laube@bfh.ch Andreas Spichiger, BFH FBW, andreas.spichiger@bfh.ch Marc Kunz, BFH TI, marc.kunz@bfh.ch Thomas Kessler, Temet, thomas.kessler@temet.ch Adrian Müller, ID Cyber-Identity Ltd, adrian.mueller@cyber-identity.com
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

source: https://doi.org/10.24451/arbor.9061 | downloaded: 27.4.2024

Zusammenfassung

Der vorliegende Standard definiert die wichtigsten Begriffe für IAM-Lösungen im föderalen E-Government 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.

Inhaltsverzeichnis

1 Einleitung 7

1.1 Status 7
1.2 Anwendungsgebiet 7
1.3 Vorteile 7
1.4 Schwerpunkt 7
1.5 Normativer Charakter der Kapitel 7

2 Terminologie 9

2.1 Anbieterin von Zertifizierungsdiensten 9
2.2 Artefakt 9
2.3 Attribut / Attribute 9
2.4 Attributaggregation 9
2.5 Attribut-Autorität (AA) 10
2.6 Attributanfrage 10
2.7 Attributbestätigung 10
2.8 Attribute Assertion Service 10
2.9 Attribute Provider (AP) 10
2.10 Attribute Service 10
2.11 Attribute-Based Access Control (ABAC) 10
2.12 Auditing 11
2.13 Ausgabewert eines Authentifikators 11
2.14 Authentication Proxy 11
2.15 Authentication Service 11
2.16 Authentifikation-Autorität (AuthnA) 11
2.17 Authentifikator 11
2.18 Authentifizierung 12
2.19 Authentifizierungsanfrage 12
2.20 Authentifizierungsbestätigung 12
2.21 Authentifizierungsfaktor 12
2.22 Authentifizierungsmittel 13
2.23 Autorisation Service 14
2.24 Autorisierung 14
2.25 Backend Attribute Exchange (BAE) 15
2.26 Behörde 15
2.27 Benutzer 15
2.28 Benutzerzentriertes Identitätsmanagement 15
2.29 Berechtigung 15
2.30 Bereich STIAM-Domäne 15
2.31 Beweismittel 15
2.32 Biometrisches Merkmal 16
2.33 Broker Service 17
2.34 Certificate Policy (CP) 17
2.35 Certificate Revocation List (CRL) 17
2.36 Certification Authority (CA) 17
2.37 Certification Practice Statement (CPS) 17
2.38 Client Plattform 17
2.39 Community Metadaten 18
2.40 Credential 18
2.41 Credential Service 18
2.42 Credential Service Provider (CSP) 18
2.43 Definitionszeit 18

2.44 Dienstanbieter 19
2.45 Digitales Zertifikat 19
2.46 Ding 19
2.47 Discovery Service (WAYF - Where Are You From) 19
2.48 Domäne 19
2.49 E-Identity 19
2.50 E-Identity Service 20
2.51 Eigenschaften 20
2.52 Elektronische Signatur 20
2.53 Elektronisches Identifizierungsmittel 20
2.54 Elektronisches Identifizierungssystem 20
2.55 Elektronisches Siegel 21
2.56 Empfängerbaustein 21
2.57 Entität 21
2.58 Entitätsmetadaten 21
2.59 E-Ressource 21
2.60 E-Ressource Service 21
2.61 Feinautorisierung 21
2.62 Föderiertes IAM-System 21
2.63 Führung 22
2.64 Funktion 23
2.65 Geregeltes Zertifikat 23
2.66 Globally Unique Identifier (GUID) 23
2.67 Grobautorisierung 23
2.68 IAM-Architektur 23
2.69 IAM-Dienstanbieter 24
2.70 IAM-Führung 24
2.71 IAM-Policy 25
2.72 IAM-Regulator 25
2.73 IAM-Service 25
2.74 IAM-Support 25
2.75 IAM-System 25
2.76 Identifikator 25
2.77 Identifizierung 26
2.78 Identität 26
2.79 Identitäts- und Zugriffsverwaltung / Identity und Access Management (IAM) 26
2.80 Identitätsdokument 26
2.81 Identitäts-Föderierung 26
2.82 Identity and Attribute Provider (IdP/AP) 27
2.83 Identity Linking 27
2.84 Identity Mapping 27
2.85 Identity Provider (IdP) 27
2.86 Juristische Person 27
2.87 Körperliches Merkmal 27
2.88 Kryptographischer Token 27
2.89 Laufzeit 28
2.90 Leistungsbezüger (LB) 28
2.91 Leistungserbringer (LE) 28
2.92 LinkedID 28
2.93 Linking Protokoll 29
2.94 Logging Service 29
2.95 Look-Up Secrets 29
2.96 Memorized Secrets 29
2.97 Meta-Attribut 29

2.98 Metadaten 29
2.99 Meta-Domäne 30
2.100 Multi-Factor Cryptographic Devices 30
2.101 Multi-Factor Cryptographic Software 30
2.102 Namensraum 30
2.103 Natürliche Person 30
2.104 Netzwerk 31
2.105 Nichtabstreitbarkeit 31
2.106 Online Certificate Status Protocol (OCSP) 31
2.107 OpenID Connect 31
2.108 Organisation 31
2.109 OTP Devices 31
2.110 Out of Band Authenticators 32
2.111 Policy 32
2.112 Qualifizierte elektronischen Signatur 32
2.113 Qualifiziertes Zertifikat 32
2.114 Quality Authentication Assurance (QAA) 32
2.115 Rechte 33
2.116 Register 33
2.117 Registrierung 33
2.118 Registrierungsstelle / Registration Authority (RA) 33
2.119 Regulator 33
2.120 Relying Party (RP) 34
2.121 Replizierendes IAM-System 34
2.122 Ressource 34
2.123 Ressourcen-Verantwortlicher 35
2.124 Role based Access Control (RBAC) 35
2.125 Rolle 35
2.126 SAML 2.0 Web Browser SSO Profile 35
2.127 SAML Protokoll 35
2.128 SAML Token 35
2.129 Security Assertion Markup Language (SAML) 36
2.130 Security Token 36
2.131 Security Token Service (STS) 36
2.132 Senderbaustein 36
2.133 Service Level Agreement (SLA) 36
2.134 Service Provider (SP) 36
2.135 Single Factor Cryptographic Devices 36
2.136 Staatlich anerkannte elektronische Identität (E-ID) 37
2.137 STIAM - SuisseTrust Identity and Access Management 37
2.138 STIAM Certificate Authority (STIAM-CA) 37
2.139 STIAM Identity und Attribute Bus 37
2.140 STIAM-Community 37
2.141 STIAM-Empfänger 37
2.142 STIAM-Hub 38
2.143 STIAM-IdP 38
2.144 STIAM-Komponente 38
2.145 STIAM-Metadata Repository (STIAM-MDR) 39
2.146 STIAM-Plattform 39
2.147 STIAM-RLM (Reporting-Logging-Monitoring) 39
2.148 STIAM-Sender 39
2.149 Subjekt 39
2.150 Topologie 40
2.151 Trust Service 40

2.152 Trusted Third Party 40
2.153 UID-Einheit 40
2.154 Verifier 41
2.155 Verlässliche Quelle 41
2.156 Vermittler 41
2.157 Vertrauen 41
2.158 Vertrauensstufe 41
2.159 Verwaltung 42
2.160 Verzeichnis 42
2.161 Widerruf 42
2.162 WS-Federation 42
2.163 WS-Trust 42
2.164 Zugang Service 42
2.165 Zugangsregel 42
2.166 Zugangsregel Service 43
2.167 Zugriff 43
2.168 Zugriffskontrolle 43
2.169 Zugriffsrecht 43
2.170 Zugriffsrecht Service 43
3 Haftungsausschluss/Hinweise auf Rechte Dritter 44
4 Urheberrechte 44
Anhang A – Referenzen & Bibliographie 45
Anhang B – Mitarbeit & Überprüfung 46
Anhang C – Abkürzungen 47
Anhang D – Abbildungsverzeichnis 48
Anhang E - Tabellenverzeichnis 48

Hinweis

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im vorliegenden Dokument bei der Bezeichnung von Personen ausschliesslich die maskuline Form verwendet. Diese Formulierung schliesst Frauen in ihrer jeweiligen Funktion ausdrücklich mit ein.

1 Einleitung

Internetbasierte Geschäftsprozesse setzen vertrauenswürdige Subjekte und damit verbundenes Wissen um die Handlungspartner voraus. Entsprechende Dienste werden durch die Identitäts- und Zugriffsverwaltung (Identity and Access Management, IAM) gewährleistet. Sie sind beim Bereitstellen von Lösungen im E-Government Schweiz zu berücksichtigen, damit lokale Anwendungen und Dienste sowohl organisationsintern wie auch organisationsübergreifend genutzt werden können. Dieser Standard definiert die grundlegenden Begriffe und Konzepte im Bereich IAM und dient damit als Grundlage für alle, welche im E-Government-Umfeld 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 der bereits bestehenden eCH-Standards im Bereich IAM zusammen und konsolidieren diese. Die aufgenommenen Begriffe umfassen Stakeholder, Prozesse, Services bis zu Implementationsdetails in föderierten und nicht föderierten IAM-Lösungen. Begriffe aus internationalen Standards werden zu den definierten Begriffen in Beziehung gesetzt und damit verständlicher gemacht.

1.3 Vorteile

Mit der Schaffung eines Glossars für den Bereich IAM, dass mit jedem neuen oder aktualisierten eCH-Standard auf den letzten Stand gebracht wird, wird die Qualität und Konsistenz aller Standards in diesem Bereich erheblich verbessert.

1.4 Schwerpunkt

Kapitel 2 beschreibt die wichtigsten Konzepte und Begriffe im Bereich IAM mit der Einschränkung auf E-Government und E-Health.

1.5 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 Anbieterin von Zertifizierungsdiensten

Gemäss ZertES [2]: *„Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck digitale Zertifikate ausstellt.“*

Synonyme: Certification Service Provider, Zertifizierungsdienstleister, Zertifizierungsstelle für digitale Zertifikate,

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

2.2 Artefakt

Artefakte sind kleine, strukturierte Datenobjekte, die von einem IAM-Dienstanbieter (Service Provider, IdP) ausgestellt werden und an eine Authentifizierung des Subjektes gekoppelt sind.

Beispiele:

- SAML artifacts [1]
- Elektronische Signatur eines Dokumentes (im Fall eines Remote Signing Service)

2.3 Attribut / Attribute

Semantisches Abbild einer einem Subjekt zugeordneten Eigenschaft, die das Subjekt näher beschreibt. Der Identifikator ist ebenfalls ein speziell verwendetes Attribut.

Ein Attribut setzt sich zusammen aus den Meta-Attributen; Attributname (z.B. „Schuhgrösse“), Attributtyp (z.B. „Integer“) und Attributwert (z.B. „39“).

Im Stellvertretungsfall besitzt die E-Identity des Stellvertreters für eine gewisse Zeit eine Menge von Attributen der E-Identity des vertretenen Subjekts.

Persönliche Attribute: Attribute die einer natürlichen Person gehören. Diese alleine muss über die Weitergabe von diesen Attributen entscheiden können.

Enterprise Attribute: Attribute die einer Organisation gehören. Diese entscheidet im Rahmen geltender Gesetze und Verträge über die Weitergabe der Attribute. Der einzelne Benutzer innerhalb der Organisation spielt im Rahmen dieser Entscheidung eine sekundäre Rolle. Das Subjekt stimmt üblicherweise implizit der Freigabe dieser Attribute zu (z.B. Unterschrift Arbeitsvertrag), weil er sonst von Amtes wegen seine Aufgabe nicht wahrnehmen könnte.

2.4 Attributaggregation

Der Begriff der Attributaggregation wird von N. Klingenstein in „Attribute Aggregation and Federated Identity“ [3] genau beschrieben. Man versteht darunter den Prozess, Attribute zu einer bekannten digitalen Identität von verschiedenen Quellen abzufragen und zusammenzustellen.

2.5 Attribut-Autorität (AA)

Der Begriff Attribut-Autorität wird vor allem im SAML-Umfeld als Synonym für Attribute Provider (AP) (siehe 2.9) verwendet.

eCH-0167: Informationslieferant, der über eine definierte Schnittstelle (STIAM-Sender) Attribute für die STIAM-Community bereitstellt.

Synonyme: attribute authority (engl.), Attribute Provider (AP)

2.6 Attributanfrage

Mit einer Attributanfrage können Attribute für ein Subjekt angefragt werden. Das Resultat einer Attributanfrage ist eine Attributbestätigung (siehe 2.7).

Die Attributanfrage kann mit der Authentifizierungsanfrage (siehe 2.19) kombiniert werden.

2.7 Attributbestätigung

Bestätigung des Wertes eines Attributs durch eine Attribut-Autorität.

Beispiele:

SAML 2.0 Attribute Assertion [1], Aggregated Claim [4]

Synonym: Attribute Assertion (engl.), Attributwertbestätigung

2.8 Attribute Assertion Service

Attribute Assertion Service stellt die *Attributbestätigungen* über eine definierte Schnittstelle aus.

Synonym: Attributbestätigungs Service

2.9 Attribute Provider (AP)

Ein Attribute Provider ist 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

2.10 Attribute Service

Der Attribute Service pflegt zeitnah ein oder mehrere Attribute für definierte Subjekte.

2.11 Attribute-Based Access Control (ABAC)

Konzept dynamischer Zuteilung von Zugriffsrechten basierend auf Attributen des Subjekts.

2.12 Auditing

a) Überprüfung der Policy-Konformität

b) Aufzeichnung aller Aktionen und Entscheide zur Gewährleistung der Nachvollziehbarkeit

2.13 Ausgabewert eines Authentifikators

Als Ausgabewert wird eine mathematische Funktion (Authentifikator oder Authentifizierungsfunktion) aus einem geheimen Wert (z.B. privater Schlüssel), einem oder mehreren optionalen Aktivierungswerten (z.B. PIN oder biometrischer Informationen), und einem oder mehreren optionalen Eingabewerten (z.B. Zufallswerten oder Challenges) generiert.

Die Qualität des Ausgabewertes wird vom gewählten Authentisierungsverfahren bestimmt bzw. dessen Implementation.

Synonym: Ausgabewert eines Authentifizierungsmittels

2.14 Authentication Proxy

Ein Authentication Proxy verbindet zwei Protokollabschnitte und bildet damit ein Protokollendpunkt. Er kann eine Authentifizierungsanfrage transformieren und/oder anpassen und diese an einen IdP/AP (siehe 2.82) weiterleiten. Der Benutzer wird vom IdP/AP authentifiziert. Der Authentication Proxy kann ein Teil eines Vermittlers (siehe 2.156) sein.

Beispiel in STIAM: Ist AuthnA(1) nicht in der Lage, einen Nutzer zu authentifizieren, kann er unter bestimmten Umständen als Authentication Proxy agieren, indem er selber einen eigenen Authentication Request an einen weiteren AuthnA(2) sendet. Die Antwort vom AuthnA(2) kann der AuthnA(1) dann dazu verwenden, eine eigene Response zu generieren.

2.15 Authentication Service

Der Authentication Service überprüft mittels der Authentifizierungsmittel, ob der Zugreifende (Subjekt) der ist, der er behauptet zu sein.

2.16 Authentifikation-Autorität (AuthnA)

Eine AuthnA stellt einen Authentication Service zur Verfügung, gegen den sich das Subjekt authentifizieren kann. Der Authentication Service überprüft mittels der Authentifizierungsmittel, die von einem Credential Service ausgestellt werden. Der Credential Service kann ein Bestandteil der AuthnA sein. Beispiele für Authentifikation-Autoritäten sind IdPs (nach SAML), OpenID Provider und MobileID Provider.

Synonym: Authentication Authority (engl.)

2.17 Authentifikator

Der Authentifikator ist das funktionale Abbild des Authentifizierungsmittels der Realwelt. Mit der Funktion eines Authentifikators wird in der Regel aus einem Eingabewert (Challenge) und einem geheimen Wert ein Ausgabewert erzeugt. Je nach Ausprägung muss der geheime Wert durch einen zweiten Faktor (PIN) aktiviert werden.

Synonyme: Authentifizierungsfunktion, Authentificator (engl.)

2.18 Authentifizierung

Authentifizierung ist der Vorgang der Überprüfung einer behaupteten E-Identity eines Subjekts nach bestimmten Vorgaben. Die angestrebte Vertrauensstufe der Authentifizierung bestimmt diese Vorgaben.

Spezialfall eIDAS: dynamische Authentifizierung (kein SSO)

Synonyme: Authentifikation, Authentisierung[1]

2.19 Authentifizierungsanfrage

Eine Authentifizierungsanfrage ist der Beginn einer Authentifizierung des Subjekts.

Eine Authentifizierungsanfrage wird vom Subjekt an den Authentication Service gesendet. Dieser initialisiert die Überprüfung der behaupteten E-Identity.

Synonym: Authentication Request (engl.)

2.20 Authentifizierungsbestätigung

Die Authentifizierungsbestätigung ist der Nachweis, welchen der Identity Provider (IdP) nach einer erfolgreichen Authentifizierung des Subjektes, ausstellt. Die Authentifizierungsbestätigung ist für einen bestimmten Zeitraum gültig und kann eine Vertrauensstufe enthalten.

Beispiele:

Bei Security Assertion Markup Language (SAML) [5] ist die Authentifizierungsbestätigung die „Authentication Assertion“ und wird vom (SAML) Identity Provider ausgestellt.

Bei OIDC [4] ist die Authentifizierungsbestätigung das sogenannte „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.

2.21 Authentifizierungsfaktor

Authentifizierungsfaktoren sind Informationen und/oder Prozesse, die zur Authentifizierung eines Subjektes verwendet werden können. Authentifizierungsfaktoren können auf vier verschiedenen Merkmalen (besitzabhängig, kenntnisabhängig, inhärent oder verhaltensbasiert) oder auch Kombinationen davon beruhen:

- besitzabhängiger Authentifizierungsfaktor: beruht auf Besitz (etwas, das das Subjekt besitzt, z. B. Soft-Token/Hardware-Token mit privatem Schlüssel, elektronischer Pass oder ID-Karte),

- kenntnisabhängiger Authentifizierungsfaktor: beruht auf Wissen (etwas, das das Subjekt

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

weiss, z.B. Passwort, PIN),

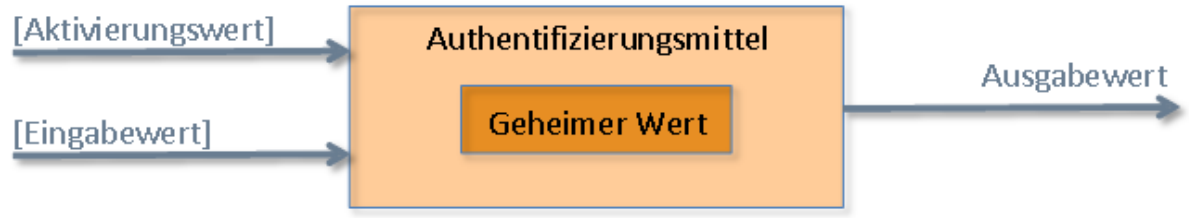
- inhärenter Authentifizierungsfaktor: beruht auf einem biometrischen Merkmal (etwas, das das Subjekt ist, wie Iris, Netzhaut, Fingerabdruck),

- verhaltensbasierter Authentifizierungsfaktor: beruht auf Verhalten (etwas, was das Subjekt typischerweise macht, z.B. dynamisches Unterschriftsmuster).

Synonym: Authentifizierungsmerkmal

2.22 Authentifizierungsmittel

Ein Authentifizierungsmittel ist etwas, das ein Subjekt besitzt und das es unter seiner Kontrolle hat (typischerweise ein kryptographischer Schlüssel, ein Geheimnis, ein biometrisches Merkmal oder ein spezifisches Verhalten). Ein Authentifizierungsmittel muss nicht unbedingt in Hardware Form vorliegen, sondern kann auch ein Soft-Token oder eine Software-Komponente sein. Ein Authentifizierungsmittel kann einen SFA (*single-factor authenticator*) oder auch mehrere unabhängige Authentifizierungsfaktoren MFA (*multi-factor authenticator*) benutzen. Der vom Authentifizierungsmittel generierte Ausgabewert (engl. Authenticator output oder authenticator response) wird durch eine mathematische Funktion (Authentifikator oder Authentifizierungsfunktion) aus einem geheimen Wert (z.B. privater Schlüssel), einem oder mehreren optionalen Aktivierungswerten (z.B. PIN oder biometrischer Informationen), und einem oder mehreren optionalen Eingabewerten (z.B. Zufallswerten oder Challenges) generiert. Im Trivialfall kann das Authentifizierungsmittel der geheime Wert selbst sein (z.B. im Fall eines Passwortes). Siehe Tabelle 1 für weitere Beispiele.




```
Ausgabewert =
       Authentifizierungsfunktion (geheimer Wert,
                                   [Aktivierungswerte],
                                   [Eingabewerte])
```

Abbildung 1: Schematische Funktionsweise eines Authentifizierungsmittels

	Passwort	Strichliste	SMS	OTP	Mobile-ID	SuisseID
Typ	SFA	SFA	SFA	(HW-)MFA	HW-MFA	HW-MFA
Eingabewert	-	Index	gesendeter Code	Seed	gesendeter Code	Nonce
Geheimer Wert	Passwort	(alpha-) numerischen Wert	-	Device Key	Private Key	Private Key

	Pass-wort	Strichliste	SMS	OTP	Mobile-ID	SuisseID
Aktivierungswert	-	-	-	-	PIN	PIN
Authentifikator	-	Liste der (alpha-) numerischen Werte	Handy	Device	SIM-Karte	Crypto-Device
Authentifizierungs-funktion	Keine oder Hash-Fkt.	Selektion	Lesen und Schreiben des gesendeten Codes	HMAC	Signatur	Signatur
Ausgabewert	Passwort, Hash des Passworts	(alpha-) numerischen Wert	gesendeter Code	Code	Sign (gesendeter Code)	Sign (Nonce)
Credential[2]	Passwort, Hash des Passworts	Liste der (alpha-) numerischen Werte	Mobile-Nr.	Device-Nr./ Seed	SIM-Karte mit Mobile-Nr./ Public Key	Certificate

Tabelle 1: Beispiele für Authentifizierungsmittel und zugehörigem Credential

Synonyme:

- Authenticator (siehe NIST 800-63-3 [6]), früher bei NIST 800-63-2 [7] als Token bezeichnet.
- Bei STORK[3] als identity token bzw. authentication token bezeichnet

2.23 Autorisation Service

Der Service überprüft zur Ausführungszeit die Einhaltung der Rechte für die Nutzung der E-Ressource und erlaubt dem Subjekt die Nutzung der Ressource, wenn es die entsprechenden Rechte besitzt.

2.24 Autorisierung

Die Autorisierung ist der Obergriff von Grob- und Feinautorisierung (siehe 2.66 und 2.61).

Synonym: Authorization (engl.)

2 Zum Credential gehört immer auch der Identifier, z.B. der Name des Benutzers.

3 Siehe: https://www.eid-stork2.eu

2.25 Backend Attribute Exchange (BAE)

Attributabfrage im Hintergrund, üblicherweise durch eine Maschine. Ein Benutzer ist bei der Attributabfrage nicht direkt involviert, diese erfolgt ohne seine explizite Zustimmung.

2.26 Behörde

Eine rechtlich begründete Organisation, welche hoheitliche Staatsaufgaben der Schweiz wahrnimmt. Behörden können auf Ebene von Gemeinde, Kanton oder Bund existieren und zur Legislative, Exekutive oder Judikative gehören. (siehe auch eCH-0122[4])

2.27 Benutzer

Ein Benutzer ist eine technische Repräsentation eines Subjekts. Der Begriff «Benutzer» wird normalerweise als die technische Repräsentation einer natürlichen Person verwendet. Die technische Repräsentation eines Services wird «technischer Benutzer» bezeichnet.

Synonym: User (engl.)

2.28 Benutzerzentriertes Identitätsmanagement

Ermöglicht dem Benutzer die Auswahl spezifischer Authentifizierungsmittel und Attribute zur Bearbeitung in Authentifizierungs- und Attribut-Anfragen und überlässt ihm so die Kontrolle über die eigene, digitale Identität. Das bedeutet nicht, dass der Benutzer jede Transaktion nochmals explizit genehmigen muss, aber dass die Daten immer durch die Identitätsverwaltung des Benutzers fliessen und direkt an seine digitale Identität gebunden sind.

2.29 Berechtigung

Die Berechtigung ist die Summe aller Zugangs- und Zugriffsrechte.

2.30 Bereich STIAM-Domäne

Als Bereich kann eine begrenzte Gruppe von Informationsbezügern und -lieferanten angesehen werden, welche ein bestimmte Menge an Attributen und eine gemeinsame Policy teilen. Die Semantik und Syntax dieser Attribute werden durch die Teilnehmer der Gruppe bestimmt. Beispielsweise soll es möglich sein, dass sich innerhalb von SuisseTrustIAM eine Teilföderation bilden kann, welche nur ihre intern bekannten Identitäten und Attribute über die Plattform austauscht.

2.31 Beweismittel

Ein Beweismittel (innerhalb von IAM) ist ein Dokument oder Objekt aus einer verlässlichen

[4] https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0122&documentVersion=1.0

Quelle, das Angaben zum Antragsteller enthält. Es kann zur Überprüfen einer Identität verwendet werden.

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

Beispiele:

- Beglaubigte Urkunde
- Kreditkarten
- Fahrausweis
- Identitätsdokumente

2.32 Biometrisches Merkmal

Ein biometrisches Merkmal ist ein körperliches Merkmal eines Menschen, das es erlaubt, diesen hinreichend von anderen zu unterscheiden, welches also zu dessen Identifizierung verwendet werden kann. Ein biometrisches Merkmal sollte sich im Laufe der Zeit wenig ändern. Kombinationen mehrere Merkmale sind dabei möglich, z.B. Erfassung des Gesichtes kombiniert mit Stimmerkennung. Ein entscheidender Nachteil bei der Verwendung von biometrischen Merkmalen bei der Authentifizierung ist, dass sie im Fall einer Kompromittierung nicht für ungültig erklärt bzw. neu erzeugt werden können.

Zu den wichtigsten biometrischen Merkmalen gehören:

- Fingerprint
- (dynamische) Unterschrift
- Gesichtsgeometrie
- Gesichtsbild (Foto)
- Irismuster
- Retina (Netzhaut)
- Handgeometrie
- Fingergeometrie
- Ohrform
- Stimme (Klangfarbe)
- DNA
- Tastenanschlag
- Venenmuster

Zur Identifizierung von natürlichen Personen werden zurzeit meist nur

- Fingerprint
- Iris

- Retina
- Gesichtsgeometrie
- Gesichtsbild (Foto)

verwendet.

Biometrische Merkmale können bezüglich Funktion, Sicherheit, Fälschbarkeit und Anwendungsfreundlichkeit ebenfalls klassifiziert werden. Das NIST hat mit ihrer Online-Dokumentation „Strength of Function for Authenticators – Biometrics“ [8] kurz SOFA-B dazu einen ersten Beitrag geleistet.

2.33 Broker Service

Dieser Service vermittelt zwischen dem Subjekt, Ressourcen und den Services der Ausführungszeit, föderiert Authentifizierungs- und Attributbestätigung.

2.34 Certificate Policy (CP)

Eine Certifcate Policy enthält die Anwendungsregeln für einen bestimmten Zertifikatstyp. Siehe auch 2.111 Policy und 2.37 Certification Practice Statement (CPS).

2.35 Certificate Revocation List (CRL)

Liste, welche die von einer (oder mehreren) CA(s) ausgestellten *digitalen Zertifikate* enthält, welche widerrufen wurden. Ein Eintrag in der Liste besteht mindestens aus der Seriennummer des widerrufenen Zertifikats und dem Widerrufsdatum.

2.36 Certification Authority (CA)

Eine Certification Authority ist ein spezieller Credential Service Provider (CSP) als technische Instanz, welche digitale Zertifikate (Public Key Zertifikate, z.B. X.509) als Authentifizierungsmittel ausgibt, erneuert und revoziert. Siehe auch 2.1 Anbieterin von Zertifizierungsdiensten und 2.42 Credential Service Provider (CSP).

Synonyme: Certificate Authority, Certification Service Provider, Trust Service Provider (TSP)

Synonyme deutsch: Zertifizierungsstelle für digitale Zertifikate, Vertrauensdiensteanbieter

2.37 Certification Practice Statement (CPS)

Policy, welche eine Anbieterin von Zertifizierungsdiensten anwendet, um Zertifikate auszustellen. Siehe auch 2.111 Policy und 2.34 Certificate Policy (CP).

2.38 Client Plattform

Die Client Plattform ist das System oder Gerät, von welchem das Subjekt einen Authentisie-

rungsprozess anstösst. Dies kann beispielsweise ein Browser auf einem PC oder eine Applikation auf einem mobilen Gerät sein.

Synonym: Client, user agent (engl.)

2.39 Community Metadaten

Signierter Zusammenzug von Entitätsmetadaten der Mitglieder einer STIAM-Community.

2.40 Credential

Ein Credential stellt eine Menge von Daten (keine Hardware oder andere physische Container) dar, mit der eine elektronische Identität (E-Identity) an ein Authentifizierungsmittel gebunden wird, welches von Subjekt besitzt und kontrolliert wird.

Das Credential wird zusammen mit dem Ausgabewert des Authentifizierungsmittels zum Nachweis der behaupteten E-Identity verwendet. Je nach verwendeten Authentifizierungsfaktoren ist das Credential z.B. der Hash eines Passwortes, ein Abbild eines biometrischen Merkmals oder ein Zertifikat (siehe auch Tabelle 1), das zur Definitionszeit von einem CSP an eine E-Identity gebunden wurde.

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 [10], Kap 3).

Synonym: Identitätsnachweis

2.41 Credential Service

Der Credential Service gibt Authentifizierungsmittel aus und verwaltet sie. Er ermöglicht eine benutzerfreundliche Erneuerung bzw. den Ersatz von Authentifizierungsmitteln. Ein Authentifizierungsmittel bezieht sich auf eine E-Identity und ist für ein bestimmtes Subjekt ausgestellt.

2.42 Credential Service Provider (CSP)

Ein Credential Service Provider ist eine Entität, die als vertrauenswürdiger Herausgeber von digitalen Zertifikaten und anderer Sicherheits-Tokens (Authentifizierungsmitteln) agiert.

Der CSP enthält eine Registrierungsstelle und Dienste zur Verifizierung der Credentials (IdP). Ein CSP kann als öffentliche Instanz auftreten, oder als Dienst in eine abgeschlossene Domäne integriert sein.

2.43 Definitionszeit

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

2.44 Dienstanbieter

Der Dienstanbieter ist ein Stakeholder in einem IAM-System und möchte, dass seine angebotenen IAM-Leistungen von möglichst vielen verwendet werden. Zudem strebt er eine Zusammenstellung von möglichst komplementär ausgerichteten Diensten an, um das IAM-System effizient und wirtschaftlich zu halten.

Abbildung 2: Dienstanbieter

Abbildung 2 zeigt die Sicht des Dienstanbieters auf das Gesamtsystem. Der Dienstanbieter stellt seine IAM-Leistung der Relying Party zur Verfügung. Mit Hilfe dieser IAM-Leistung kann das Subjekt die fachliche Leistung der Relying Party nutzen.

2.45 Digitales Zertifikat

Strukturierte Daten, die den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels bestätigen.

Synonyme: Digital Certificate (engl.), Zertifikat, Public-Key-Zertifikat

2.46 Ding

Ein Ding ist ein physischer Gegenstand, welcher über ein Netzwerk (siehe 2.104) erreichbar ist. Innerhalb des Netzwerkes ist das Ding mit einem Identifikator eindeutig identifizierbar. Mehrere Dinge, welche im selben Netzwerk verknüpft sind, bilden ein Internet der Dinge (Internet of Things, IoT). Dinge können weitere Dinge enthalten. Ein Ding kann zu einer Organisation (siehe 2.108) oder zu einer natürlichen Person (siehe 2.103) gehören.

Synonyme: Objekt, Thing (IoT)

2.47 Discovery Service (WAYF - Where Are You From)

Der Discovery Service ist dafür zuständig, den Benutzer zu einem IdP seiner Wahl – zwecks Authentifizierung – zu leiten.

2.48 Domäne

Administrative / technische Gemeinschaft oder Organisation mit einer gemeinsamen Policy (unter anderem der Namensraum).

2.49 E-Identity

Eine E-Identity ist die Repräsentation eines Subjekts. Eine E-Identity (digitale Identität) hat einen Identifikator (eindeutiger Name), meist zusammen mit einer Menge von zusätzlichen

Attributen, welche innerhalb eines Namensraumes (und damit einer Domäne) eindeutig einem Subjekt zugewiesen werden können. Ein Subjekt kann mehrere E-Identities haben.

Eine notifizierte E-Identity ist eine E-Identity, die alle in eIDAS 910/2014 [11] Artikel 7 aufgeführten Voraussetzungen erfüllen muss, z.B. die zur Zeit geplante E-ID (siehe 2.136) der Schweiz.

Synonyme: Digitale Identität, Digital Identity, Elektronische Identität, Electronic Identity

2.50 E-Identity Service

Der E-Identity Service stellt zu Subjekten (siehe 2.149) E-Identities aus und verwaltet sie.

2.51 Eigenschaften

Eigenschaften sind charakteristische Merkmale oder charakteristisches Verhalten eines Subjekts, die in ihrer Summe spezifisch für das Subjekt sind.

2.52 Elektronische Signatur

Gemäss ZertES [2]: *„Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder die logisch mit ihnen verknüpft sind und zu deren Authentifizierung dienen.“*

2.53 Elektronisches Identifizierungsmittel

Begriff aus eIDAS 910/2014 [11]: „Elektronisches Identifizierungsmittel“ ist eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird.

Ein elektronisches Identifizierungsmittel enthält Authentifizierungsfaktoren, Attribute für Personen und hat eine Gültigkeit. Bei einer (dynamischen) Authentifizierung wird der gesamte Prozess Subjekt authentifizieren vom elektronischen Identifizierungsmittel abgewickelt. Es umschliesst daher sowohl Authentifizierungsmittel, Credential und IdP. Das Ergebnis einer Authentifizierung mit einem elektronischen Identifizierungsmittel ist eine Authentifizierungsbestätigung, mit der die Identität des Subjekts und die erfolgreiche Authentifizierung bestätigt werden.

Beispiele für elektronische Identifizierungsmittel sind der neue deutsche Personalausweis (nPA) inkl. Middleware (AusweisApp) oder die gesamte SuisseID Infrastruktur bestehend aus SuisseID Token, Middleware (Gerätetreiber) und SuisseID IdP.

2.54 Elektronisches Identifizierungssystem

Begriff aus eIDAS 910/2014 [11]: „Elektronisches Identifizierungssystem“ ist ein System für die elektronische Identifizierung, in dessen Rahmen natürlichen oder juristischen Personen oder natürlichen Personen, die juristische Personen vertreten, elektronische Identifizierungsmittel ausgestellt werden.

Ein notifiziertes elektronisches Identifizierungssystem muss alle in eIDAS 910/2014 [11] Artikel 7 aufgeführten Voraussetzungen erfüllen.

2.55 Elektronisches Siegel

Eine *elektronische Signatur*, welche im Namen einer *UID-Einheit* angebracht wird. Elektronische Siegel können im Rahmen automatisierter Prozesse erstellt werden.

2.56 Empfängerbaustein

Der Empfängerbaustein realisiert eine standardisierte STIAM-Schnittstelle für eine RP, welche die STIAM-Protokolle nicht direkt unterstützt (vgl. 2.144 STIAM-Komponente Abbildung 9).

2.57 Entität

Ein aktives Element eines IT Systems, z.B. ein automatisierter Prozess oder eine Menge von Prozessen, ein Teilsystem, eine Person oder eine Gruppe von Personen mit definierten Funktionalitäten [1].

Organisation mit definierter Rolle innerhalb einer STIAM-Community.

Synonym: Entity

2.58 Entitätsmetadaten

Metadaten einer Attribut-Autorität, IdP oder RP zur Definition der Rolle einer Entität innerhalb der STIAM-Community.

2.59 E-Ressource

Digitale Repräsentation einer Ressource (siehe 2.122). Eine E-Ressource hat einen Identifikator (eindeutiger Name, oft URL/URI), welcher innerhalb eines Namensraumes eindeutig einer Ressource zugewiesen werden kann. Eine Ressource kann mehrere E-Ressourcen haben.

2.60 E-Ressource Service

Der E-Ressource Service stellt zu Ressourcen E-Ressourcen aus und verwaltet sie.

2.61 Feinautorisierung

Gewährung bzw. Verweigerung des Zugriffs auf einzelne von einer Ressource bereitgestellten Funktionen oder Daten.

2.62 Föderiertes IAM-System

Ein föderiertes IAM-System ist eine Implementation einer Identitäts-Föderierung (siehe Kapitel 2.81). Damit ein föderiertes IAM-System etabliert werden kann, müssen sich die verschiedenen Domänen in Bezug auf bestimmte Aspekte gegenseitig vertrauen. Dieses Vertrauen

stützt sich auf explizite und implizite Vereinbarungen ab.

Wie in Abbildung 3 dargestellt besteht ein föderiertes Identitätssystem 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 in einem primären Authentisierungsverfahren mit einem bestimmten Authentifizierungsmittel (Authenticator). Dieses Ereignis wird dann in Form einer Authentifizierungsbestätigung an die vertrauende Partei über das Netzwerk weitergegeben. Der IdP kann zu dieser Authentifizierungsbestätigung noch weitere (Personen-)Attribute zum authentisierten Subjekt beifügen.

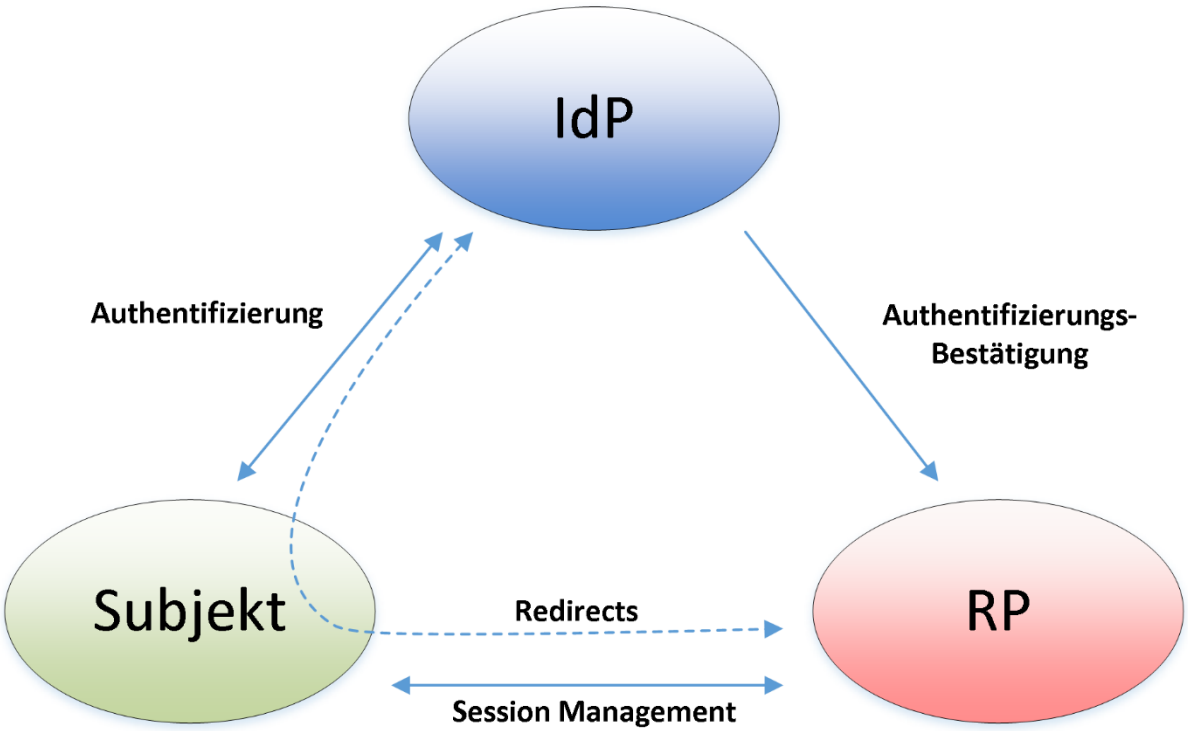


Abbildung 3: Modell einer Identitäts-Föderierung

Föderiertes IAM-System im E-Government: Beim föderierten IAM-System im E-Government stellen Behörden (siehe 2.26) Ressourcen den Subjekten ihren internen (andere Behörden der Schweiz) oder externen Partnern (Personen, Unternehmen, Organisationen oder Behörden anderer Staaten) zur Verfügung, mit denen definierte Leistungen aus dem Bereich ihrer Zuständigkeit online verfügbar gemacht werden. Diese Ressourcen sollen für Subjekte der eigenen Domäne(n) und für Subjekte mit E-Identities anderer Domänen zugreifbar sein. Eine Behörde kann somit Relying Party (siehe 2.120) aber auch u.U. gleichzeitig IAM-Dienstanbieter (siehe 2.69) sein.

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

2.63 Führung

Die Führung ist ein Stakeholder in einem IAM-System und möchte ein funktionierendes und stabiles IAM-System, das allen Stakeholdern gerecht wird. Sie führt die daran beteiligten IAM-Dienstanbieter und Relying Parties und garantiert den zuverlässigen Betrieb des IAM-Systems.

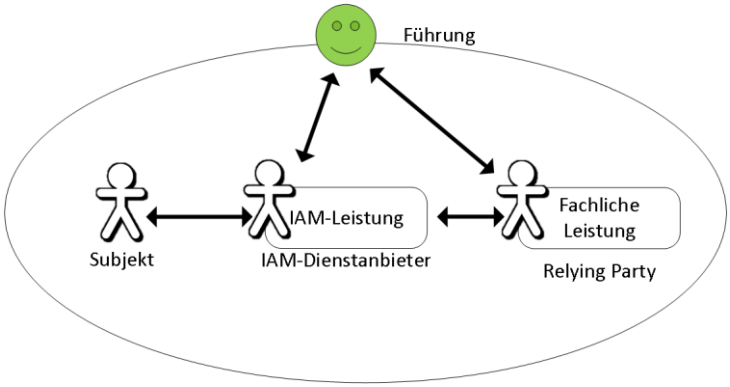


Abbildung 4: Führung

Abbildung 4 zeigt die Sicht der Führung des gesamten IAM-Systems. Die Führung möchte das IAM-System und die daran beteiligen Relying Parties und IAM-Dienstanbietern effizient führen, um die Implementierung zu erleichtern und den zuverlässigen Betrieb zu garantieren. Die Führung koordiniert dabei die Anforderungen aller Stakeholder im IAM-System, auch die des Regulators und des Leistungsbezügers.

2.64 Funktion

Eigenschaft, die einem Subjekt bestimmte Aufgaben, Kompetenzen und Verantwortung innerhalb einer Organisation zuweist. Ein Subjekt kann mehrere Funktionen haben (vgl. Rolle).

2.65 Geregeltes Zertifikat

Ein auf eine *natürliche Person* oder eine *UID-Einheit* ausgestelltes *digitales Zertifikat*, welches die entsprechenden Formvorschriften des ZertES [2] erfüllt. Geregelte Zertifikate können z.B. für elektronische Siegel oder zur Website-Authentisierung eingesetzt werden.

2.66 Globally Unique Identifier (GUID)

Ein Globally Unique Identifier ist eine eindeutige Nummerierung und kann einem Subjekt zugeordnet werden.

2.67 Grobautorisierung

Gewährung bzw. Verweigerung des Zugangs zu einer Ressource anhand der Zugangsregeln (siehe 2.165).

2.68 IAM-Architektur

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

2.69 IAM-Dienstanbieter

Der IAM-Dienstanbieter ist verantwortlich für den Betrieb von einem oder mehreren IAM-Geschäftsservices gemäss der IAM-Policy (siehe 2.71). Es können die folgenden Spezialisierungen unterschieden werden, die aber oft gemeinsam implementiert werden. Der Betrieb kann vom IAM-Dienstanbieter selbst gewährleistet oder auch an einem Betreiber ausgelagert werden (Outsourcing). Im Outsourcing-Fall überträgt der IAM-Dienstanbieter die an ihn gestellten Anforderungen an den Betreiber.

- 2.118 Registrierungsstelle / Registration Authority (RA)
- 2.42 Credential Service Provider (CSP)
- 2.85 Identity Provider (IdP)
- 2.9 Attribute Provider (AP)
- 2.156 Vermittler

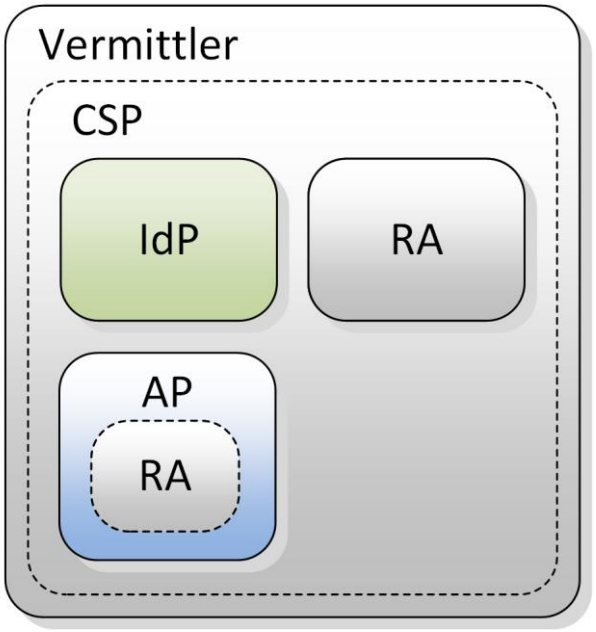


Abbildung 5: IAM-Dienstanbieter

Die Abbildung 5 stellt alle IAM-Dienstanbieter dar, falls sie gemeinsam implementiert werden.

2.70 IAM-Führung

Die IAM-Führung ist verantwortlich für das Managen eines IAM- Systems oder von Teilen davon (IAM-Dienstanbieter (siehe 2.69) und Relying Party (siehe 2.120)).

Die **IAM-Führung des Gesamtsystems** managt die teilnehmenden IAM-Dienstanbieter und Relying Parties (z. B. analog zu ITIL [12]) in allen Fachbereichen wie z.B. Release-Management, Qualitätsmanagement, IAM-Lieferanten- und -Konsumentenmanagement, Service-Request-Management. Dies kann sowohl im internen Kontext als auch über Verträge/SLA mit externen IAM-Dienstanbietern und Relying Parties geschehen.

2.71 IAM-Policy

Die IAM-Policy definiert die Ziele, Prinzipien und die Systemgrenzen des angestrebten IAM-Systems.

2.72 IAM-Regulator

Der IAM-Regulator (oder die IAM-Steuerung) definiert die rechtlichen, prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen, innerhalb derer das IAM abgewickelt werden muss. Er berücksichtigt dabei die Interessen aller Stakeholder und beteiligt alle anderen Rollen 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-Geschäftsservices.

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.

2.73 IAM-Service

Die IAM-Services erbringen ihre Aufgaben mit Hilfe von IT. Dabei arbeiten sie über standardisierte Schnittstellen zusammen, welche offene Standards (z.B. SAML, OIDC, …) benutzen. Jeder IAM-Service wird von einem IAM-Dienstanbieter erbracht. Die Nutzung ist vertraglich geregelt. IAM-Service sind keine technische Service-Komponenten, d.h. bei einer Realisierung können ein oder auch mehrere IAM-Services von einer technischen Service-Komponente implementiert oder auch ein IAM-Service auf mehrere technischen Service-Komponenten verteilt werden.

Synonym: IAM-Dienst

2.74 IAM-Support

Der IAM-Support ist verantwortlich für alle Aktivitäten zum Auffinden und Lösen von Problemen.

2.75 IAM-System

Ein IAM-System ist eine Implementierung eines IAMs (siehe 2.79), welches in einer Organisation eingesetzt wird. Grundsätzlich kann ein IAM-System unabhängig sein. Registrierungsprozesse und Benutzerverwaltung sind integrierte Bestandteile eines IAM-Systems.

2.76 Identifikator

Eine Zeichenkette, welche eine E-Identity oder eine E-Ressource innerhalb eines Namensraumes (Domäne) eindeutig bezeichnet. Der Identifikator einer Ressource ist oft eine

URL/URI.

2.77 Identifizierung

Identifizierung ist ein Vorgang zur Definitionszeit, bei welchem die Identität des Subjekts meist mit Hilfe von Beweismitteln überprüft wird. Die Identifizierung wird meist durch eine Registrierungsstelle als Teil der Registrierung durchgeführt.

Synonym: Identitätsfeststellung

2.78 Identität

Identität ist die Gesamtheit der Eigenschaften eines Subjektes, die es kennzeichnen und als Individuum von allen anderen unterscheiden. Im IAM-Kontext wird hauptsächlich die E-Identity eines Subjekts verwendet (siehe 2.49).

Synonym: Identity (engl.)

2.79 Identitäts- und Zugriffsverwaltung / Identity und Access Management (IAM)

Alle Prozesse und Systeme, um Subjekten den Zugriff auf die Ressourcen zu ermöglichen, die diese auf Grund ihrer Funktion in der Organisation benötigen.

Synonym: Identitätsmanagement

2.80 Identitätsdokument

In der Schweiz gelten die folgenden Dokumente als Identitätsdokumente:

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

2.81 Identitäts-Föderierung

Eine Identitäts-Föderierung ist eine Zusammenarbeit verschiedener Entitäten eines IAM-Systems über Organisations- und Systemgrenzen hinweg, ohne Duplikation oder Replikation der dazu notwendigen Benutzerdaten (E-Identities und Attribute) im Gegensatz zum replizierenden IAM-System (siehe 2.121).

Eine Föderierung von Identitäten erlaubt es, Informationen über eine Authentifizierung eines Subjektes und optional Identitätsinformationen zu diesem Subjekt über ein Netzwerk zu übermitteln.

Synonyme: Identity Federation, Föderiertes IAM

2.82 Identity and Attribute Provider (IdP/AP)

Ein Identity and Attribute Provider (IdP/AP) ist eine Komponente, die ein IdP (siehe 2.85) und ein AP (siehe 2.9) kombiniert. Sie stellt Authentifizierungs-, sowie Attributbestätigungen aus. (vgl. auch 2.144 STIAM-Komponente Abbildung 9).

Synonyme: Identity Provider/Attribut-Autorität (IdP/AA), Identitätslieferant

2.83 Identity Linking

Identity Linking ist der Vorgang zur Definitionszeit, bei welchem eine LinkedID an eine eindeutige, digitale Identität eines Subjekts geknüpft wird. Die dazu notwendigen Informationen werden in einer Link Table abgelegt.

2.84 Identity Mapping

Identity Mapping ist der Vorgang zur Laufzeit, bei welchem mit Hilfe der Link Table LinkedID Verknüpfungen aufgelöst werden. Eine lokale E-Identity kann so mit der föderierten E-Identity verbunden werden.

2.85 Identity Provider (IdP)

Entität, die E-Identities verwaltet und herausgibt. Ein IdP stellt einen Authentication Service (siehe 2.15) zur Verfügung.

Synonym: Authorization Provider, Issuer (U-Prove)

2.86 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 (vgl. 2.149).

2.87 Körperliches Merkmal

Ein körperliches Merkmal ist ein Merkmal eines Menschen, wie Körpergrösse und Augenfarbe. Spezielle körperliche Merkmale sind die biometrischen Merkmale (siehe 2.32).

2.88 Kryptographischer Token

Software- oder Hardwaremedium zur Speicherung des/der privaten Schlüssel eines Zertifikates (Bsp. f. Software: Microsoft Certificate Manager im Windows OS; Bsp. f. Hardware: SmartCard, USB-Token, Hardware Security Module)

Synonyme: Zertifikatstoken, Cryptographic Token, Kryptografischer Token

2.89 Laufzeit

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

Synonym: Ausführungszeit

2.90 Leistungsbezüger (LB)

Der Leistungsbezüger ist ein Stakeholder in einem IAM-System und möchte jederzeit, kostengünstig und einfach eine fachliche Leistung (Bsp. Bestellung einer Funklizenz oder einer Parkkarte) online in Anspruch nehmen. Er fordert Unterstützung bei Problemen (z. B. bei Identitätsdiebstahl) und erwartet Konformität mit gesetzlichen Regelungen.

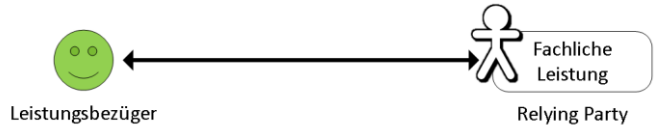


Abbildung 6: Leistungsbezüger (LB)

Abbildung 6 zeigt die Sicht des Leistungsbezügers auf das Gesamtsystem. Der Leistungsbezüger möchte vorrangig eine fachliche Leistung einer Relying Party in Anspruch nehmen. Das verwendete IAM-System ist für ihn zweitrangig und nur Mittel, um sein Ziel zu erreichen.

2.91 Leistungserbringer (LE)

Der Leistungserbringer ist ein Stakeholder in einem IAM-System und möchte fachliche Leistungen online anbieten. Dies soll kostengünstig, stabil, einfach und konform mit den gesetzlichen Regelungen sein und von möglichst vielen genutzt werden. Den Zugriff und den Schutz der Ressourcen möchte er gemäss seinen Bedürfnissen (z. B. Risikobereitschaft, Wirtschaftlichkeit) an die IAM-Dienstanbieter übertragen.

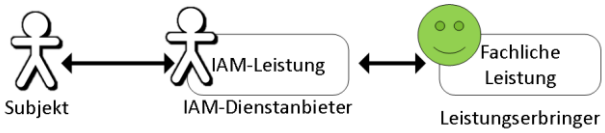


Abbildung 7: Leistungserbringer (LE)

Abbildung 7 zeigt die Sicht des Leistungserbringers auf das Gesamtsystem. Der Leistungserbringer möchte seine fachliche Leistung dem Subjekt zur Verfügung stellen. Die dazu notwendigen IAM-Leistungen möchte er zumeist nicht selbst erbringen, sondern diese an IAM-Dienstanbieter auslagern.

2.92 LinkedID

Im organisationsübergreifenden Kontext erlaubt linkedID, E-Identities aus verschiedenen Domänen miteinander in Beziehung zu setzen. E-Identities können mit linkedIDs zu einem beliebigen gerichteten Graphen verkettet werden.

2.93 Linking Protokoll

Der Benutzer kann IdPs oder APs in der Link Table seines Accounts verbinden. Um den korrekten Identifikator als Eintrag in der Link Table zu erhalten, muss sich der Benutzer gegenüber dem jeweiligen Authentication Service authentisieren. Dadurch kann ein eindeutiger Identifikator zwischen Vermittler und dem IdP oder der AP ausgetauscht werden.

2.94 Logging Service

Der Service dokumentiert zur Laufzeit die Verwendung eines Services und stellt der Support-Organisation die notwendigen Informationen bereit, um Nutzungsprobleme oder Fehler aufzuklären.

2.95 Look-Up Secrets

Look-Up Secrets enthalten eine Liste von (alpha-)numerischen Werten, die zuvor zwischen dem Subjekt und dem CSP ausgetauscht wurden. Zur Authentifizierung muss der Benutzer einen bestimmten Wert aus dieser Liste angegeben.

Die ausgetauschten Werte müssen zufällig generiert werden. Sie dürfen nur einmal benutzt werden und eine genügend hohe Entropie besitzen.

Beispiele: Strichlisten (engl. tally sheet) oder TAN-Blöcke

Synonym: Nachschlagbares Geheimnis

2.96 Memorized Secrets

Memorized Secrets, im Allgemeinen als Passwort oder PIN bezeichnen, sind geheim gehaltene Werte, die meist vom Benutzer gewählt und in seinem Gedächtnis oder an einem anderen sicheren Aufbewahrungsort gespeichert werden. Sie müssen über eine genügend hohe Komplexität und Zufälligkeit verfügen, um von einem Angreifer nicht erraten oder auf sonstige Art und Weise berechnet werden können. Passwort Policies legen die Regeln zur Länge, Komplexität, Zeichenmix, Ablaufdauer und Wiederverwendung fest und bestimmen somit die Stärke des Memorized Secrets.

Beispiele: Passwort oder PIN

Synonym: gespeichertes Geheimnis

2.97 Meta-Attribut

Bestandteil des Attribut-Schemas, Spezifizierung des Attributs.

2.98 Metadaten

Ein Mittel, um Vertrauen und technische Interoperabilität zwischen SAML Komponenten (Entitäten) zu ermöglichen. Können auch verwendet werden, um Attributinformationen auszutauschen.

Die Metadaten beschreiben die Komponenten der registrierten Organisationen und Provider

mit ihren Federation-Service-Endpunkten, Zertifikaten und den angeforderten bzw. zur Verfügung gestellten Attributen.

Synonym: Metadata

2.99 Meta-Domäne

Domäne, welche die Zusammenarbeit zwischen zwei oder mehreren Domänen regelt.

Synonym: Gemeinschaft

2.100 Multi-Factor Cryptographic Devices

Ein multi-factor cryptographic device ist ein physisches Gerät, welches einen geschützten kryptographischen Schlüssel enthält. Es muss mit einem zweiten Authentifizierungsfaktor (Wissen oder Eigenschaft) aktiviert werden. Die Authentifizierung wird durch den Besitznachweis und Kontrolle des kryptographischen Schlüssels vollbracht.

Beispiele: SmartCard, SuisseID

Synonym: Multifaktor Verschlüsselungs-Geräte

2.101 Multi-Factor Cryptographic Software

Ein multi-factor software cryptographic authenticator ist ein kryptographischer Schlüssel, welcher auf einer Festplatte oder ähnlichem Medium gespeichert ist. Ein solcher Authenticator muss mit einem zweiten Authentifizierungsfaktor aktiviert werden. Die Authentifizierung wird durch den Besitznachweis und Kontrolle des kryptographischen Schlüssels vollbracht. Dieser Authenticator kombiniert zwei Authentifizierungsfaktoren: Besitz (kryptographischer Schlüssel) mit einem weiteren Geheimnis (Besitz oder Eigenschaft), das zur Aktivierung verwendet wird.

Beispiel: Soft-Token (PKCS#12 Datei)

Detaillierte Anforderungen sind in den folgenden Quellen beschrieben:
Siehe auch NIST SP 800-63B [10], Kapitel 5.1.7.

Synonym: Multifaktor Verschlüsselungs-Software

2.102 Namensraum

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

Synonym: Namespace (engl.)

2.103 Natürliche Person

Eine natürliche Person ist ein Mensch als Rechtssubjekt. Natürliche Personen können zu einer Organisation (siehe 2.108) gehören.

2.104 Netzwerk

Informationssystem welches in der Lage ist, Informationen mit verschiedenen verbundenen Komponenten auszutauschen.

2.105 Nichtabstreitbarkeit

Die Garantie bzw. der Beweis, dass sich ein Subjekt auf die Korrektheit der Daten bzw. den Inhalt eines elektronischen Dokuments verpflichtet hat. Nichtabstreitbarkeit ist ein wichtiger Bestandteil der qualifizierten elektronischen Signatur.

Synonyme: Non-Repudiation, Content-Commitment

2.106 Online Certificate Status Protocol (OCSP)

Bei OCSP handelt es sich um ein Protokoll zur Abfrage des Gültigkeitsstatus eines digitalen Zertifikats. Siehe auch 2.161 Widerruf und 2.35 Certificate Revocation List (CRL).

2.107 OpenID Connect

OpenID Connect 1.0 (OIDC) [4]definiert eine einfache Identitätsschicht auf der Basis von OAuth 2.0 (RFC 6749) [13], die auch von Mobilgeräten verwendet werden kann. OIDC verwendet das Basisprotokoll OAuth sowohl für die Authentifizierung als auch für die Zugangskontrolle. Als Security-Tokens werden JSON Web Tokens [14] verwendet.

2.108 Organisation

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

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.

2.109 OTP Devices

Ein Single-Factor OTP (One-time Password) Device ist eine Software oder ein Gerät, welches nach einem bestimmten Algorithmus (pro Ereignis, Zeitbasiert) spontan ein Einmal-Passwort generiert.

Auf dem Gerät oder in der Applikation befindet sich ein eingebettetes Geheimnis (Schlüssel), welches für die Generierung des einmal verwendbaren Passwortes genutzt wird. Als Eingabewert kann die aktuelle Zeit oder ein sich inkrementierender Zähler dienen.

Beispiele: SecureID-Token, Google Authenticator, SafeNet mobilePass

Ein Multi-Factor OTP Device erfordert zur Aktivierung des Algorithmus einen zweiten Faktor (Wissen oder Eigenschaft) auf dem Gerät. Dieser zweite Authentifizierungsfaktor kann ein

integriertes Keypad, ein biometrischer Sensor (z.B. Fingerabdruck) oder eine direkte Computer Schnittstelle (z.B. USB) sein.

Beispiele: SecureID-Token mit Keypad, HID ActivID Token

Synonym: Einmal-Passwort Generator

2.110 Out of Band Authenticators

Out of Band ist ein physisches Gerät, welches eindeutig adressierbar sein muss und welches Geheimnisse die vom CSP gewählt werden, zur einmaligen Verwendung empfangen kann.

Das Gerät ist im Besitz des Subjekts und sollte über einen eigenen, privaten Kanal angesprochen werden können, welcher unabhängig vom primären Kanal für den zweiten Authentifizierungsfaktor genutzt wird.

Der Out of Band Authenticator kann auf zwei verschiedene Arten funktionieren:

1. Das Subjekt präsentiert das Geheimnis, welches er 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: Handy/Smartphone mit Mobilnummer und SMS-TAN-Verfahren

Synonym: Externer Kanal

2.111 Policy

Schriftlich festgehaltene Regelungen und Vorschriften, welche einzuhalten sind.

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

2.112 Qualifizierte elektronischen Signatur

Eine elektronische Signatur, welche die entsprechenden Formvorschriften des ZertES [2] erfüllt. Eine qualifizierte elektronische Signatur kann als Pendant der eigenhändigen Unterschrift in der elektronischen Welt betrachtet werden.

2.113 Qualifiziertes Zertifikat

Ein auf eine *natürliche Person* ausgestelltes *digitales Zertifikat*, welches die entsprechenden Formvorschriften des ZertES [2] erfüllt. Eine *qualifizierte elektronische Signatur* muss auf einem qualifizierten Zertifikat beruhen.

(Anmerkung: In der EU-Verordnung eIDAS 910/2014 [11] 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. Siehe dazu auch Kapitel 2.65 *geregeltes Zertifikat*.)

2.114 Quality Authentication Assurance (QAA)

Qualität der Authentifikation einer digitalen Identität gemäss ISO 29115:2013 [9].

2.115 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.

2.116 Register

Verzeichnisse in der Verwaltungssprache, wie z.B. die Einwohnerregister, Anwaltsregister, Zivilstandsregister, Handelsregister etc. Sie werden in der Regel von offiziellen Stellen (Verwaltungen, Behörden) geführt.

2.117 Registrierung

Prozess einer Registrierungsstelle, bei dem ein Subjekt eine E-Identity mit dazugehörigem Authentifizierungsmittel und Credential erlangt. Die Registrierung beinhaltet meist eine *Identifizierung*.

Synonym: Registration (engl.)

2.118 Registrierungsstelle / Registration Authority (RA)

Eine Registrierungsstelle ist eine Entität, die genügend Informationen zu einem Subjekt erfasst und überprüft, um dessen Identität überprüfen zu können.

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

2.119 Regulator

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

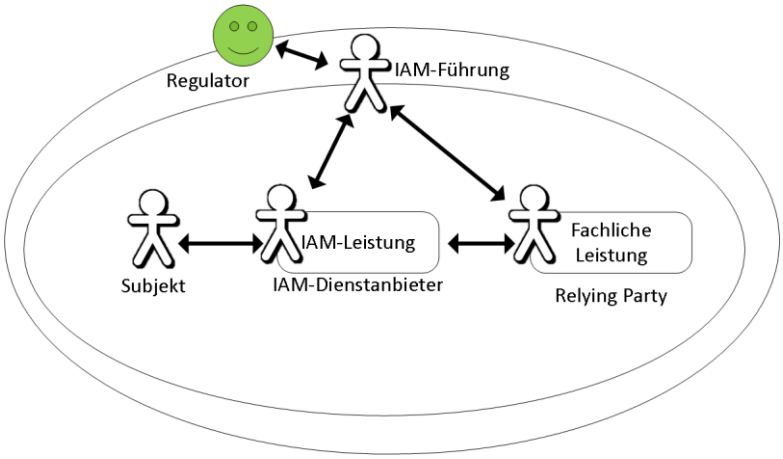


Abbildung 8: Regulator

Abbildung 8 zeigt die Sicht des Regulators. Der Regulator möchte durch die Schaffung entsprechender Rahmenbedingungen (Gesetze, Standards, Strategien, etc.) den Einsatz von

föderierten IAM-Systemen im organisationsübergreifenden Kontext fördern und gleichzeitig eine hohe Qualität nicht funktionaler Merkmale, wie z. B. Interoperabilität, Zuverlässigkeit und Sicherheit, erreichen.

2.120 Relying Party (RP)

Die Relying Party vertritt die Interessen der Ressource im IAM-System. Sie nutzt IAM-Geschäftsservices und verarbeitet Informationen von IAM-Dienstanbietern (siehe 2.69) für den Schutz ihrer Ressourcen. Sie braucht zur Beurteilung der Berechtigung eines Ressourcenzugriffs nähere Informationen (berechtigungsrelevante Eigenschaften) zu einem Subjekt, dessen E-Identity (siehe 2.49) und den Kontext des Zugriffs (Lokation, Zeitpunkt, Sicherheitsniveau etc.).

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

2.121 Replizierendes IAM-System

Ein replizierendes IAM-System verwaltet Benutzerdaten (E-Identities und Attribute) zentral an einem Standort. Während der Etablierung eines replizierenden IAM-Systems werden die Daten, die für die Erstellung einer E-Identity aggregiert (von mehreren Quellen kopiert und persistiert) und harmonisiert. Während des Betriebes des replizierenden IAM-Systems können die Daten von den Quellen periodisch aktualisiert werden.

Die Datenquellen sind im Unterschied zu einem föderierten IAM-System (siehe 2.62) nicht eigenständig.

2.122 Ressource

Service oder Daten, auf welche ein Subjekt zugreifen kann, wenn es sich authentisiert hat und es auf der Basis der benötigten Attribute autorisiert wurde. Dies schliesst physische Ressourcen wie Gebäude und Anlagen, deren Benutzung über IT-Systeme gesteuert wird, ein.

Es wird im IAM zwischen drei Arten von Ressourcen unterschieden:

- **öffentliche** (nicht schützenswerte) Ressourcen: Diese Ressourcen sind freizugänglich und benötigen zum Zugriff keinerlei Authentisierung. Beispiele sind informative Webseiten (Lesezugriff) und öffentliche Daten.
- **versteckte** Ressourcen: Diese Ressourcen erfordern ebenfalls keine Authentifizierung vor dem Zugriff, aber die Ressource ist nicht allgemein verfügbar, sondern nur einer Menge von Benutzern 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 des zugreifenden Subjektes.

2.123 Ressourcen-Verantwortlicher

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

2.124 Role based Access Control (RBAC)

Verfahren zur Zugriffssteuerung und -kontrolle auf Dateien oder Dienste.

Bei der rollenbasierten Zugriffskontrolle werden Benutzern oder Gruppen von Benutzern eine oder mehrere Rollen zugeordnet. Eine Rolle enthält eine Menge von Berechtigungen (Permissions), die die erlaubten Operationen auf einer Ressource beschreiben. vgl. 2.11

Synonym: Rollenbasierte Zugriffskontrolle

2.125 Rolle

a) Organisation, Subjekt: Bestimmte Anzahl von Funktionen, die in einer Organisation ausgeführt werden. Einem Subjekt können eine oder mehrere Rollen zugeteilt werden.

b) E-Identity: Attribute, die die Rolle/Funktionen des Subjekts repräsentieren

c) System, Entität: Aufgabe und Zweck einer Entität in einer Föderation. Einer Entität können eine oder mehrere Rollen zugeteilt werden.

Synonym: Role (engl.)

2.126 SAML 2.0 Web Browser SSO Profile

Profile fassen spezielle Anwendungsfälle von SAML zusammen. Das SAML 2.0 Web Browser SSO (single-sign-on) Profil [15] beschreibt webbasierte Authentisierungsszenarien, inkl. Identity Federation, für Browser.

2.127 SAML Protokoll

OASIS hat mit der Einführung von SAML nicht nur das SAML Token, sondern auch ein Protokoll und Bindings definiert, welche die Übertragung der Token spezifizieren. SAML unterstützt unter anderem HTTP-POST und HTTP-Redirect als Request-Response Schema. Nebst SAML gibt es auch andere Protokolle, welche SAML Token unterstützen. Zwei Beispiele dafür sind WS-Federation und WS-Trust.

2.128 SAML Token

Ein SAML Token enthält bestätigte Identitätsinformationen eines Subjekts in standardisierter Form. Kernpunkt eines SAML Tokens ist die Assertion. Diese beschreibt, zu wem das Token gehört, wie lange es gültig ist, wer es ausgestellt hat und dann die Identitätsinformationen des Subjekts und allfällige Attribute, welche an dieses geknüpft sind.

2.129 Security Assertion Markup Language (SAML)

SAML (Security Assertion Markup Language) erlaubt es, Informationen über Authentifizierungs- und Attributinformationen zwecks Autorisierung standardisiert zwischen mehreren Teilnehmern auszutauschen. Der SAML-Standard [14] beschreibt die Syntax und Regeln zum Anfordern, Erstellen und Austauschen von SAML-Assertions.

2.130 Security Token

Ein Datenpaket, welches verwendet werden kann, um den Zugriff auf eine Ressource zu autorisieren.

Ein Security Token enthält bestätigte Identitätsinformationen eines Subjekts in standardisierter Form (Authentication Statement, Authentication Assertion). Eine RP verifiziert und validiert diese Informationen, um daraus einen Zugangsentscheid abzuleiten.

2.131 Security Token Service (STS)

Security Token Service ist ein Webservice, welcher Security Tokens gemäss WS-Security Spezifikation [16] ausstellt.

2.132 Senderbaustein

Der Sender-Baustein realisiert eine standardisierte STIAM-Schnittstelle zur Anbindung einer Attribut-Autorität, welche die STIAM-Protokolle nicht direkt unterstützt, an den STIAM-Hub (vgl. 2.144 STIAM-Komponente Abbildung 9).

2.133 Service Level Agreement (SLA)

Bezeichnet einen Vertrag zwischen Auftraggeber und Auftragnehmer für wiederkehrende Dienstleistungen.

2.134 Service Provider (SP)

Ein Service Provider ist ein IAM-Dienstanbieter (vgl. siehe 2.69), der für ein authentisiertes Subjekt Artefakte (siehe 2.2), z.B. eine elektronische Signatur für ein Dokument, ausstellt und diese auf Anfrage an eine Relying Party (siehe 2.120) zurücksendet. Der Service Provider ist damit ein Überbegriff für einen Attribut Provider.

Nicht zu verwechseln ist der Service Provider mit dem SAML Service Provider, welcher OASIS in der SAML Spezifikation verwendet und ein Synonym für Relying Party ist.

2.135 Single Factor Cryptographic Devices

Ein single-factor cryptographic device ist ein physisches Gerät, welches kryptographische Berechnungen anhand einer dem Gerät gegebenen Eingabe durchführt. Das Gerät benötigt dazu keine Aktivierung über einen zweiten Authentifizierungsfaktor. Das Gerät benutzt zur Generierung des Ausgabewerts in ihm gespeicherte symmetrische oder asymmetrische

Schlüssel. Die Authentifizierung wird durch den Besitznachweis des Gerätes vollbracht.

Beispiel: YubiKey U2F

Siehe auch NIST SP 800-63B [10], Kapitel 5.1.6.

Synonym: Einfaktor-Verschlüsselungsgeräte

2.136 Staatlich anerkannte elektronische Identität (E-ID)

Mit E-ID wird die staatlich anerkannte elektronische Identität der Schweiz bezeichnet, deren rechtliche und organisatorische Rahmenbedingungen im Bundesgesetz über elektronische Identifizierungsdienste (E-ID Gesetz, siehe https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/e-id.html) definiert werden.

2.137 STIAM - SuisseTrust Identity and Access Management

SuisseTrust Identity and Access Management bildet ein Modell für ein föderiertes Identity und Access Management System ab und ist als mögliche Lösungsvariante zu verstehen.

2.138 STIAM Certificate Authority (STIAM-CA)

Eine STIAM-CA ist eine CA, die von der STIAM-Community akzeptiert wird.

2.139 STIAM Identity und Attribute Bus

Vermittelt Authentisierungs- und Attributanfragen zwischen Subjekt, RP, AuthnA und AP.

Nimmt die SAML-Requests der STIAM-Empfänger entgegen und leitet sie an die korrekte AuthnA und AP weiter. Danach nimmt er die Responses der STIAM-Sender entgegen und sendet die Informationen als aggregierte SAML-Response an die korrekte RP zurück.

2.140 STIAM-Community

Die STIAM-Community bilden alle Teilnehmer, die mit einer STIAM-Plattform interagieren und die einheitliche Spezifikation (vgl. 2.111) berücksichtigen.

2.141 STIAM-Empfänger

Kommunikationsmodul, das die standardisierte SAML-Kommunikation zwischen der RP und dem STIAM-Hub realisiert.

Der STIAM-Empfänger nutzt die Dienste des STIAM-Hubs, um einen Benutzer authentifizieren zu lassen und weitere Informationen über diesen zu beziehen, die dann zur Zugangssteuerung verwendet werden können. Der STIAM-Empfänger definiert, wie der Benutzer authentifiziert werden soll und welche Attribute in welcher Qualität notwendig sind, um Zugang auf eine seiner geschützten Ressourcen zu erlauben. Der STIAM-Empfänger erhält vom

STIAM-Hub die geforderten Informationen in Form einer Authentifizierungs- und/oder Attributbestätigung.

2.142 STIAM-Hub

Der STIAM-Hub als Kernstück der SuisseTrustIAM-Plattform hat zwei Funktionen. Erstens bietet er zur Definitionszeit die Trust- und E-Identity-Geschäftsservices an, indem sich Benutzer und Organisationen auf dem STIAM-Hub registrieren können und zweitens agiert er als Vermittler (Broker) zwischen den Entitäten zur Laufzeit.

2.143 STIAM-IdP

Interner IdP einer STIAM-Plattform. Dient dem Registrieren und Initialisieren von STIAM Accounts und liefert qualitativ minimale Authentifikation der Subjekte.

Ein Identity Provider hat in STIAM die Funktion, ein Subjekt zu authentifizieren. Ein STIAM-IdP implementiert eine standardisierte STIAM-Schnittstelle zum STIAM-Hub (vgl. 2.144 STIAM-Komponente Abbildung 9).

2.144 STIAM-Komponente

Zu den STIAM-Komponenten gehören STIAM-Sender (AP), STIAM-Empfänger (RP), STIAM-IdPs, der STIAM-Hub und STIAM-CSPs. Die STIAM-Komponenten besitzen eine standardisierte Schnittstelle, die es ihnen erlaubt, miteinander zu kommunizieren und sich gegenseitig zu vertrauen.

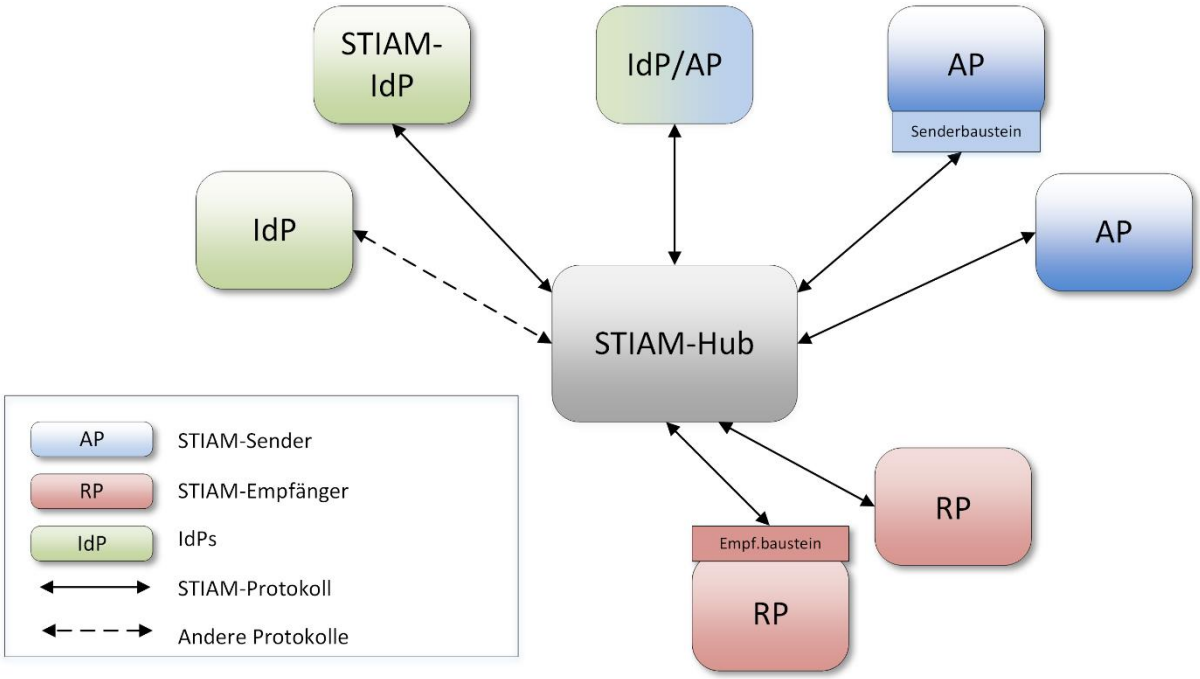


Abbildung 9: STIAM-Komponenten

2.145 STIAM-Metadata Repository (STIAM-MDR)

Zentraler Auskunftsdienst der STIAM-Plattform, verwaltet und publiziert die Metadaten für die STIAM-Community.

2.146 STIAM-Plattform

Die STIAM-Plattform umfasst den STIAM-Hub sowie alle zusätzlichen STIAM-spezifischen Komponenten (STIAM-Sender, STIAM-Empfänger, STIAM-CSP) die den Betrieb der funktionalen Lösung ermöglichen.

2.147 STIAM-RLM (Reporting-Logging-Monitoring)

Zur Gewährleistung der Nachvollziehbarkeit und Nachweisbarkeit werden Zugriffe auf Ressourcen gespeichert. Mit dem STIAM-RLM sollen analog dazu alle Vorgänge, die vom STIAM-Hub vermittelt werden, geloggt und überwacht werden können.

2.148 STIAM-Sender

Kommunikationsmodul, das die standardisierte SAML-Kommunikation zwischen der AP und dem STIAM-Hub realisiert.

Der STIAM-Sender ist eine AP (in der Regel Verzeichnisse oder Register), die Attribute für die STIAM-Community in standardisierter Form bereitstellt. Der STIAM-Sender hat ein standardisiertes Interface zum STIAM-Hub (vgl. 2.144 STIAM-Komponente Abbildung 9).

2.149 Subjekt

Ein Subjekt ist eine natürliche Person, eine handelnde Organisation (juristische Person), ein Service oder ein Ding, das auf eine Ressource zugreift oder zugreifen möchte. Ein Subjekt wird durch E-Identities (siehe 2.49) in der digitalen Welt repräsentiert. Ein Subjekt kann die Rechte an ein weiteres Subjekt delegieren.

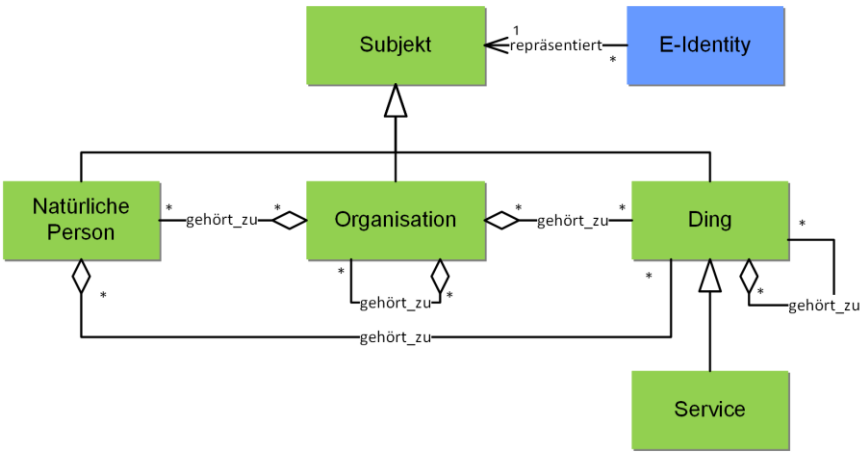


Abbildung 10: Definition Subjekt

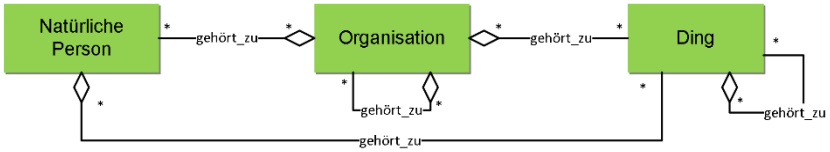


Abbildung 11: Zugehörigkeit der Subjekte

Abbildung 11 zeigt welche Subjekte in welchen enthalten sein können (z. B. Organisationen können mehrere Organisationen enthalten).

Ein **Abonnent** (engl. Subscriber, siehe NIST 800-63-3A [17]) ist ein Subjekt, welches nach erfolgreich abgeschlossenem Registrationsprozess (Prozess Subjekt registrieren) ein Authentifizierungsmittel von einer CSP erhalten hat. Damit wird das Subjekt zu einem autorisierten Teilnehmer in der Identity Federation Community.

Ein **Antragsteller** (engl. Applicant, siehe NIST 800-63-3A [17]), ist ein Subjekt, das in die Identity Federation Community aufgenommen werden möchte und dazu den Prozess Subjekt registrieren durchläuft. Wurde dieser erfolgreich abgeschlossen, wird aus dem Antragsteller ein Abonnent.

Ein **Überbringer** (engl. Bearer) ist ein Subjekt, das eine vom IdP ausgestellte Authentifizierungsbestätigung an die RP übergibt.

2.150 Topologie

Die Topologie eines Identity Federation Systems beschreibt die Anordnung der verschiedenen Komponenten und ihre logischen Verbindungen.

2.151 Trust Service

Der Trust Service pflegt die akzeptierten, vertrauenswürdigen IAM-Dienstanbieter (siehe 2.69) und Relying Parties (siehe 2.120).

2.152 Trusted Third Party

Vertrauenswürdige Instanz, z.B. zur Verwaltung von öffentlichen Schlüsseln oder Zertifikaten.

2.153 UID-Einheit

UID-Einheiten sind nach Art. 3.c des Bundesgesetzes über die Unternehmens-Identifikationsnummer [18] 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.

Weitere Informationen zu der Unternehmens-Identifikationsnummer sind beim Bundesamt für

Statistik vorhanden[5].

2.154 Verifier

Der Verifier ist ein integraler Bestandteil des IdPs. Er gleicht den Ausgabewert des Authentifikators mit dem Credential ab und bestätigt so die behauptete E-Identity des Subjekts.

2.155 Verlässliche Quelle

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

eIDAS 2015/1502: „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, Stellen usw.

2.156 Vermittler

Ein Vermittler bietet gemeinsame Dienste, wie Metadatenverwaltung, IdP-Discovery, Identity Linking oder Transformation der Authentifizierungs- und Attributbestätigung (2.12), für alle andere IAM-Dienstanbieter und Relying Parties (2.120) in einer Identity Federation nach dem Hub-'n'-Spoke Modell an. Ein integraler Bestandteil eines Vermittlers ist immer ein Authentication Proxy (siehe 2.14). Ein Vermittler kann optional einen CSP (2.42) enthalten. Siehe auch 2.33 Broker Service und 2.142 STIAM-Hub

Synonym: Hub, Broker (engl.)

2.157 Vertrauen

Formell meist im SLA definierte Vertrauensbeziehung zwischen verantwortlichen Stellen.
z.B. die formelle Beschreibung der Kriterien, die erfüllt sein müssen, damit sich zwei Organisationen, Entitäten, Domänen etc. gegenseitig vertrauen.

Synonym: Trust (engl.)

2.158 Vertrauensstufe

Die Vertrauensstufe besagt mit welcher Qualität ein Subjekt authentifiziert wurde. Anhand von 4 Teilmodellen (Vertrauensstufe der Authentifizierung, Vertrauensstufen der Registrierung, Vertrauensstufen der Steuerung und Vertrauensstufen der Föderierung) wird die Gesamt-Vertrauensstufe bestimmt.

Synonym: Vertrauensniveau

---

[5] https://www.bfs.admin.ch/bfs/de/home/register/unternehmensregister/unternehmens-identifikationsnummer/uid-einheiten-unternehmen.html

2.159 Verwaltung

Verwaltung bezeichnet ein Gemeinwesen (Ämter und Behörden, allenfalls mit solchen Aufgaben beauftragte Private), welches gesetzlich übertragene Staatsaufgaben besorgt. Der Begriff Verwaltung ist ein organisatorischer Begriff, der ausserhalb der juristischen Definition von natürlicher und juristischer Person steht.

2.160 Verzeichnis

Systematische Sammlung von Informationen mit gemeinsamen Merkmalen.

2.161 Widerruf

Beim Zertifikatswiderruf handelt es sich um eine Erklärung der Ungültigkeit eines digitalen Zertifikats. Analog können auch elektronische Identifizierungsmittel widerrufen werden.

Synonyme: Revokation, Revocation (engl.), Sperrung

2.162 WS-Federation

WS-Federation in der aktuellen Version 1.2 [16] ist ebenfalls Teil der WS-* Spezifikation und erweitert WS-Trust mit der Möglichkeit, Security Tokens auch über unterschiedliche Domains auszutauschen, indem der Standard mehrere Identity Provider unterstützt. Bei WS-Federation kann das SAML-Tokenformat als Security Token verwendet werden.

2.163 WS-Trust

Der von OASIS spezifizierte Web Service Trust (WS-Trust) [16] in der Version 1.4 ist Teil der WS-* Spezifikation, welche ein Framework für den sicheren Austausch von Web Service Nachrichten bereitstellt. Bei WS-Trust handelt es sich um einen Standard, der die Interoperabilität von Sicherheits-Token durch Definition eines Protokolls für Anforderungen und Antworten unterstützt.

2.164 Zugang Service

Der Service überprüft die Einhaltung der Zugangsregeln und erlaubt dem Subjekt den Zugang, wenn die entsprechenden Regeln erfüllt sind.

Synonym: Access Service (engl.)

2.165 Zugangsregel

Ressourcenverantwortliche definieren die Zugangsregeln für ihre E-Ressourcen. Die Zugangsregeln definieren die Bedingungen, unter denen ein Subjekt Zugang zu einer Ressource (siehe 2.122) oder deren Funktionalitäten erhält (Grobautorisierung), z.B. nach erfolgreicher Authentifizierung und Bestätigung bestimmter Attribute.

2.166 Zugangsregel Service

Der Zugangsregel Service verwaltet die Regeln für den Zugang zu einer E-Ressource (siehe 2.52). Die Regeln sind auf der Basis von Authentisierung oder Attributen definiert.

2.167 Zugriff

Interaktion mit einer Entität um eine oder mehrere ihrer Ressourcen zu manipulieren und oder zu nutzen [1].

Zur Gewährleistung der Nachvollziehbarkeit und Nachweisbarkeit werden Zugriffe gespeichert.

Synonym: Access (engl.)

2.168 Zugriffskontrolle

Überwachung und Steuerung des Zugriffs auf Ressourcen. Das Ziel ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen.

Synonym: Access Control (engl.)

2.169 Zugriffsrecht

Ressourcenverantwortliche definieren die Zugriffsrechte für ihre E-Ressourcen. Die Zugriffsrechte definieren die Bedingungen unter denen ein Subjekt auf die verschiedenen Funktionalitäten einer Ressource nutzen darf (Feinautorisierung), z.B. nach erfolgreicher Authentifizierung und Bestätigung bestimmter Attribute.

2.170 Zugriffsrecht Service

Der Zugriffsrecht Service verwaltet die Rechte für die Nutzung einer E-Ressource. Die Rechte sind auf der Basis von Authentisierung, Attributen, Kontext des Zugriffs (Lokation, Zeitpunkt, Sicherheitsniveau usw.) oder eigenen Modellen (Gruppen, Rollen, Einzel-berechtigungen) definiert.

3 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer 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 der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist 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 des Benutzers, 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 dem Benutzer 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 verpflichtet sich der Erarbeitende, sein betreffendes geistiges Eigentum oder seine 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 Urheber 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] S. Cantor, J. Hodges, F. Hirsch, R. Philpott, R. S. a Security, J. Hughes, A. Origin, H. Lockhart, B. E. a Systems, M. Beach, R. Metz, B. A. Hamilton, R. Randall, T. Wisniewski, I. Reid, P. Austel, R. L. B. Morgan, P. C. Davis, J. Kemp, P. Madsen, A. Anderson, and S. Microsystems, “Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0,” *Oasis Stand.*, 2005 [Online]. Available: https://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf

[2] Schweizerische Eidgenossenschaft, “Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES),” 2016 [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20131913/index.html

[3] N. Klingenstein, “Attribute aggregation and federated identity,” *SAINT - 2007 Int. Symp. Appl. Internet - Work. SAINT-W*, 2007.

[4] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, and C. Mortimore, “OpenID Connect Core 1.0 incorporating errata set 1,” 2014 [Online]. Available: http://openid.net/specs/openid-connect-core-1_0.html

[5] N. Ragouzis, J. Hughes, R. Philpott, E. Maler, P. Madsen, and T. Scavo, “Security Assertion Markup Language (SAML) V2.0 Technical Overview (OASIS),” 2007 [Online]. Available: https://www.oasis-open.org/committees/security/docs/draft-sstc-baker-saml-arch-00.pdf

[6] J. L. F. Paul A. Grassi, “DRAFT NIST Special Publication 800-63-3,” 2017 [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3.html. [Accessed: 22-Jun-2017]

[7] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, W. E. Burr, D. F. Dodson, and R. A. Perlner, “NIST Special Publication 800-63-2 Electronic Authentication Guideline,” 2003 [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[8] NIST, “DRAFT Strength of Function for Authenticators - Biometrics.” [Online]. Available: https://pages.nist.gov/SOFA/SOFA.html. [Accessed: 03-Nov-2016]

[9] P. Editors, W. Fumy, M. De Soete, E. J. Humphreys, K. Naemura, and K. Rannenberg, “ITU-T Recommendation X . 1254 | International Standard ISO / IEC DIS 29115 Information technology — Security techniques — Entity authentication assurance framework,” 2011.

[10] J. P. R. Paul A. Grassi, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, James L. Fenton, “DRAFT NIST Special Publication 800-63B,” 2017 [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html. [Accessed: 22-Jun-2017]

[11] D. A. S. Europ, I. Parlamentder, R. A. T. D. E. R. Europ, and I. Union, “VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, (eIDAS),” 2015.

[12] Wikipedia, “IT Infrastructure Library.” [Online]. Available: https://de.wikipedia.org/wiki/IT_Infrastructure_Library

[13] E. D. Hardt, “The OAuth 2.0 Authorization Framework [RFC 6749],” 2012 [Online]. Available: https://tools.ietf.org/html/rfc6749

[14] M. Jones, J. Bradley, and N. Sakimuar, “JSON Web Token (JWT),” 2015 [Online]. Available: https://tools.ietf.org/pdf/rfc7519.pdf

[15] S. Cantor, J. Hodges, F. Hirsch, R. Philpott, R. S. a Security, J. Hughes, A. Origin, H. Lockhart, B. E. a Systems, M. Beach, R. Metz, B. A. Hamilton, R. Randall, T. Wisniewski, I. Reid, P. Austel, R. L. B. Morgan, P. C. Davis, J. Kemp, P. Madsen, A. Anderson, and S. Microsystems, “Profiles for the OASIS Security Assertion Markup Language (SAML),” *Oasis Stand.*, 2005 [Online]. Available: https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[16] K. Lawrence, C. Kaler, A. Nadalin, M. Goodner, and M. Gudgin, “WS-Trust 1.4,” *Oasis Stand.*, no. April, 2012 [Online]. Available: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html

[17] J. L. F. Paul A. Grassi, Jamie M. Danker, William E. Burr, “DRAFT NIST Special Publication 800-63A,” 2017 [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63a.html. [Accessed: 22-Jun-2017]

[18] D. Bundesversammlung and D. S. Eidgenossenschaft, *Bundesgesetz über die Unternehmens-Identifikationsnummer (UIDG)*. 2011 [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20082601/index.html

Anhang B – Mitarbeit & Überprüfung

Gruoner Torsten	Bundesverwaltung – EFD – ISB
Hassenstein Gerhard	Berner Fachhochschule, TI
Heerkens Marc	Bundesverwaltung – EFD – ISB
Kunz Marc	Berner Fachhochschule, TI
Laube-Rosenpflanzer Annett	Berner Fachhochschule, TI
Leimer Bojan	Berner Fachhochschule, TI
Müller Adrian	ID Cyber-Identity Ltd
Selzam Thomas	Berner Fachhochschule, FBW
Spichiger Andreas	Berner Fachhochschule, FBW
	eCH Fachgruppe IAM

Anhang C – Abkürzungen

AA	Attribut-Autorität
AP	Attribute Provider
CA	Credential Authority
CSP	Credential Service Provider
E-ID	Staatlich anerkannte elektronische Identität
eIDAS	Verordnung (EU) Nr. 910/2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
EU	Europäische Union
FIDO	Fast IDentity Online
HTTP	Hypertext Transfer Protocol
HW-MFA	Hardware Multifactor Authentication
IAM	Identity and Access Management
IdP	Identity Provider
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KDC	Kerberos Distribution Center
MFA	Multi Factor Authentication
NIST	National Institute of Standards and Technology
nPA	neuer Personalausweis
OIDC	OpenID Connect
OTP	One-time Password
PIN	Persönliche Identifikationsnummer
RA	Register Authority / Registrierungsstelle
RP	Relying Party
SAML	Security Assertion Markup Language
SFA	Single Factor Authentication
SMS	Short Message Service
SSO	Single Sign-on
STORK	Secure idenTity acrOss boRders linKed
TGT	Ticket Granting Ticket
TSP	Trust Service Provider
UID	Unique Identifier
URL	Uniform Resource Locator
ZGB	Schweizerisches Zivilgesetzbuch

Anhang D – Abbildungsverzeichnis

Abbildung 1: Schematische Funktionsweise eines Authentifizierungsmittels 13
Abbildung 2: Dienstanbieter 19
Abbildung 3: Modell einer Identitäts-Föderierung 22
Abbildung 4: Führung 23
Abbildung 5: IAM-Dienstanbieter 24
Abbildung 6: Leistungsbezüger (LB) 28
Abbildung 7: Leistungserbringer (LE) 28
Abbildung 8: Regulator 33
Abbildung 9: STIAM-Komponenten 38
Abbildung 10: Definition Subjekt 39
Abbildung 11: Zugehörigkeit der Subjekte 40

Anhang E - Tabellenverzeichnis

Tabelle 1: Beispiele für Authentifizierungsmittel und zugehörigem Credential 14