eCH-0168 SuisseTrustIAM technische Architektur und Prozesse

Name	SuisseTrustIAM technische Architektur und Prozesse
Standard-Nummer	eCH-0168
Kategorie	Standard
Reifegrad	Experimental
Version	1.0
Status	Genehmigt
Genehmigt am	2014-11-26
Ausgabedatum	2014-11-27
Ersetzt Standard	--
Beilagen	keine
Abhänigkeiten	eCH-0107, eCH-0167 und eCH-0169
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Autoren	Fachgruppe IAM Annett Laube-Rosenpflanzer, BFH annett.laube@bfh.ch Gerhard Hassenstein, BFH, gerhard.hassenstein@bfh.ch Stefan Agosti, BFH, stefan.agosti@bfh.ch Hans Häni, BFH, hans.haeni@bfh.ch Marcel Vinzens, Adnovum, marcel.vinzens@adnovum.ch Urs Pfenninger, Zürich, urs.pfenninger@zuerich.ch Daniel Leiser, Atos AG, daniel.leiser@atos.net
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

Zusammenfassung

SuisseTrustIAM ermöglicht es, digitale Identitäten auf einfache Weise über Unternehmensgrenzen hinweg auszutauschen, um dadurch Geschäftsprozesse zu vereinfachen. Basis von SuisseTrustIAM ist eine generische Vermittlerinfrastruktur, auf welcher Identity Federations und IAM-Lösungen abgebildet werden können.

In diesem Dokument wird die Architektur der SuisseTrustIAM-Plattform aus technischer, aber technologieneutraler Sicht beschrieben. Konkret werden die Kommunikationsprotokolle, das Datenmodell und die administrativen Prozesse der SuisseTrustIAM-Vermittlerinfrastruktur modelliert und erläutert.

Im Rahmen der Spezifizierung von SuisseTrustIAM wurden eine Reihe weiterer Dokumente erarbeitet. Dieses Dokument ergänzt einerseits eCH-0167 ‚SuisseTrustIAM Rahmenkonzept' und wird andererseits durch eCH-0169 ‚SuisseTrustIAM Geschäftsarchitektur' referenziert.

Inhaltsverzeichnis

1 Einleitung 8
1.1 Einordnung 8
1.2 Ziel des Dokuments 8
1.3 Aufbau des Dokuments 8
1.4 Abgrenzung 9
2 Begriffsdefinitionen 10
2.1 Attribute Assertion 10
2.2 Attributaggregation 10
2.3 Bereich STIAM-Domäne 10
2.4 Discovery Service (WAYF - Where Are You From) 10
2.5 Empfängerbaustein 10
2.6 GUID 10
2.7 Identity Linking 10
2.8 Identity Provider/ Attribut-Autorität (IdP/AA) 11
2.9 Linking Protokoll 11
2.10 Metadaten (Metadata) 11
2.11 OpenID Connect 11
2.12 RP (Relying Party, Lösungsanbieter, Informationsbezüger) 11
2.13 SAML 2.0 11
2.14 SAML 2.0 Web Browser SSO Profile 11
2.15 SAML Protokoll 12
2.16 SAML Token 12
2.17 Senderbaustein 12
2.18 Security Token 12
2.19 STIAM Certificate Service Provider (STIAM-CSP) 12
2.20 STIAM-Empfänger 12
2.21 STIAM-Hub (Vermittler, Intermediär) 12
2.22 STIAM-IdP 13
2.23 STIAM-Komponente 13
2.24 STIAM-Sender 14
2.25 WS-Federation 14

2.26 WS-Trust 14
3 SuisseTrustIAM Identity Federation Modell 15
3.1 Konzept SuisseTrustIAM 15
3.2 STIAM-Hub-Modell 16
3.3 Verfahren zur Identitäts- und Attributvermittlung 17
3.3.1 Proxying 18
3.3.2 Identitätsübergabe an die AA 19
3.4 Validierung von Identitäts- und Attributinformationen 20
3.4.1 Identity Proxying Modus (IP-Mode) 21
3.4.2 Identity Relaying Modus (IR-Mode) 21
3.5 Security Token und STIAM-Protokolle 21
3.6 Vertrauensbeziehung zwischen den Komponenten 22
3.7 Session Handling 23
3.8 Vertraulichkeit von Attributinhalten 23
3.9 Anonymisierung der Identitäten 23
3.10 Nachvollziehbarkeit von Prozessen 25
3.11 Kategorisierung von Attributen 25
3.12 Attributmanagement 27
4 Anforderungen 28
4.1 SuisseTrustIAM Vermittlerinfrastruktur 28
4.2 STIAM-Empfänger 30
4.3 STIAM-IdP 31
4.4 STIAM-Sender 31
4.5 STIAM-Hub 33
5 Protokolle zur Laufzeit 36
5.1 Authentisierung und Attributaggregation 36
5.2 Service-to-Service basierte Kommunikation 40
5.3 Validierung von Identitäts- und Attributinformationen 41
5.4 Vertraulichkeit von Attributen 41
5.5 Single Logout (SLO) 41
5.6 Reporting, Logging und Monitoring 42
6 Protokolle zur Definitionszeit 44
6.1 Linking Protokolle 44

6.2 Metadaten Aggregation und Verteilung 46
7 Administrative Prozesse und Datenmodell 48
7.1 Übersicht Prozesslandkarte 49
7.2 Datenmodell 50
7.3 Account Management 52
7.3.1 Accountdatenverwaltung 52
7.3.1.1 Account verwalten 52
7.3.1.2 User importieren 53
7.3.1.3 User Identifier Repository (UIR) 53
7.3.2 Verwaltung der IdP/AA-Links 54
7.4 Organisation Management 54
7.4.1 Organisation verwalten 55
7.4.2 Organisationsinformationen und Rollen verwalten 55
7.4.3 Organisation im Datenmodell 56
7.5 Komponenten Management 58
7.5.1 Komponenten verwalten 58
7.5.2 Ressourcen verwalten 59
7.5.3 Attribute verwalten 59
7.5.4 Komponenten, Ressourcen und Attribute im Datenmodell 61
7.5.4.1 Definition von QAA-Level und Attribut-Qualität 61
7.5.4.2 Identity Provider Definition 62
7.5.4.3 Attribute Authority Definition 62
7.5.4.4 Angebotenes Attribut 63
7.5.4.5 Relying Party Definition 64
7.5.4.6 Ressource Definition 65
7.6 Attribut Management 66
8 Sicherheitsüberlegungen 67
9 Verwandte Themen 68
10 Haftungsausschluss/Hinweise auf Rechte Dritter 69
11 Urheberrechte 69
Anhang A – Referenzen und Bibliographie 70
Anhang B – Mitarbeit & Überprüfung 72
Anhang C – Abkürzungen 73

Anhang D – Glossar 74
Anhang E – Änderungskontrolle 74
Anhang F – Abbildungsverzeichnis 75
Anhang G – Tabellenverzeichnis 76

Status des Dokuments

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

Notation

Die Schlüsselworte *MUSS*, *DARF NICHT, ERFORDERLICH*, *SOLLTE*, *SOLLTE NICHT*, *EMPFOHLEN*, *KANN* und *OPTIONAL* in diesem Dokument sind zu interpretieren wie in IETF RFC 2119 beschrieben [1].

1 Einleitung

Sprachlicher Hinweis: Aus Gründen der besseren Lesbarkeit werden Personenbezeichnungen lediglich in der männlichen oder weiblichen Form verwendet. Diese Formulierungen schliessen das andere Geschlecht jeweils automatisch mit ein.

1.1 Einordnung

Unter dem Standard eCH-0107 [2] positionieren sich die Konzepte für föderierte IAM-Lösungen und ergänzende Hilfsmittel. Die Konzepte sind konkrete Beschreibungen, wie ein IAM-Lösungsvorschlag aussieht, und beinhalten Teilkonzepte und Architekturen, die für die Umsetzung berücksichtigt werden müssen. Daneben werden den Konzepten Hilfsmittel zur Seite gestellt, die ergänzende Informationen zur Verfügung stellen und die für mehr als ein Konzept relevant sind. Die dargestellten Qualitäts- und Maturitätsmodelle sind Beispiele für Hilfsmittel und nicht abschliessend.

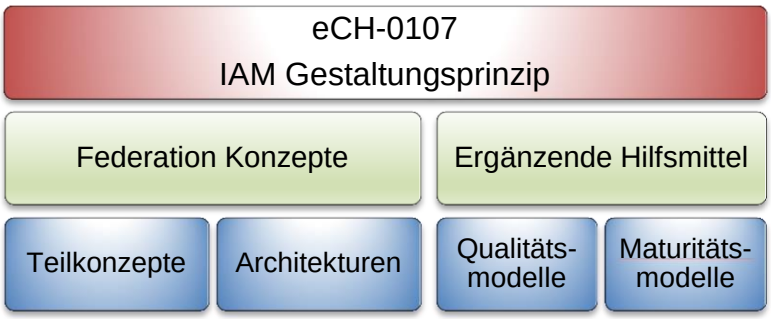


Abbildung 1: Einordnung des eCH-0168 Standards

Der vorliegende Standard eCH-0168 reiht sich in die Dokumentenhierarchie der föderierten IAM-Lösungen als Vorschlag einer IAM-Architektur ein und basiert damit auf den bereits veröffentlichten Dokumenten eCH-0107 [2] und dem SuisseTrustIAM Rahmenkonzept eCH-0167 [3]. Zusätzlich wird auf die Dokumente eCH-0170 [4] und eCH-0171 [5] verwiesen, welche die Qualitätsmodelle für elektronische Identitäten und zur Attributwertbestätigung definieren.

1.2 Ziel des Dokuments

Die in diesem Dokument modellierten Datenstrukturen und Prozesse sowie die verwendeten Protokolle sollen notwendige Informationen liefern, um die Funktionen eines STIAM-Hubs und dessen Interaktionen mit den peripheren Komponenten Relying Party (STIAM-Empfänger), Identity Provider und Attribut-Autorität (STIAM-Sender) umsetzen zu können.

1.3 Aufbau des Dokuments

Das vorliegende Dokument beschreibt die Architektur der SuisseTrustIAM-Plattform aus technischer Sicht. Nach den Begriffsdefinitionen in Kapitel 2 wird in einem ersten Hauptteil [Kapitel 3] das Identity Federation Modell von SuisseTrustIAM im Grundaufbau erklärt. In diesem Kapitel werden auch bestimmte Eigenschaften des Modells ausführlicher behandelt und spezielle Funktionen erklärt. Kapitel 4 beinhaltet die aus dem Identity Federation Modell resultierenden Anforderungen und die zusammengefassten Funktionsbeschreibungen für die

einzelnen Komponenten (STIAM-Hub, STIAM-Sender, STIAM-IdP und STIAM-Empfänger). Anschliessend [Kapitel 5 und 6] werden die im SuisseTrustIAM System zur Laufzeit und zur Definitionszeit zur Anwendung kommenden Protokolle in detaillierter Form illustriert und beschrieben. In einem dritten Teil [Kapitel 7] werden die administrativen Prozesse und das Datenmodell des STIAM-Hubs veranschaulicht.

1.4 Abgrenzung

Der Hauptfokus dieses Dokuments liegt auf der Beschreibung der Architektur der zentralen Vermittlerinfrastruktur und deren Schnittstellen: Das Dokument definiert die Anforderungen an das Gesamtsystem und die einzelnen Komponenten (STIAM-Hub, STIAM-Sender, STIAM-IdP und STIAM-Empfänger). Zudem werden die Protokolle zur Definitions- und Laufzeit in detaillierter, aber technologieunabhängiger Weise beschrieben.

Eine Umsetzung der beschriebenen Konzepte, sowie die konkreten, technologiebezogenen Spezifikationen der Schnittstellen und die Funktionen von STIAM-Sender und –Empfänger werden in separaten Dokumenten (Best Practice)[1] behandelt.

Dieses Dokument stellt eine Ergänzung zum SuisseTrustIAM Rahmenkonzept eCH-0167 [3] dar. Es konkretisiert die dort vorgestellten Konzepte, um eine Grundlage für eine Realisierung zu schaffen.

Der Grundgedanke von STIAM ist die Bereitstellung einer organisationsübergreifenden Vermittlerstruktur. Die Konzepte können auch für den Aufbau einer organisationsinternen Identity Federation verwendet werden, müssen dann aber an die speziellen Anforderungen dieser Organisation angepasst und entsprechend ergänzt werden.

[1] Die genauen Bezeichnungen der geplanten eCH Best Practice Dokumente liegen noch nicht vor.

2 Begriffsdefinitionen

Viele der in diesem Dokument verwendeten Begriffe werden bereits in den Dokumenten eCH-0107 [2] und eCH-0167 [3] beschrieben. Deshalb wird hier auf eine umfassende Begriffsdefinition verzichtet. Es werden in diesem Kapitel dennoch einige Begriffe erklärt, welche in den beiden erwähnten Dokumenten nicht oder nur am Rand behandelt werden.

2.1 Attribute Assertion

Eine Attribute Assertion ist die Bestätigung eines Attributes durch eine Attribut-Autorität (siehe eCH-0107 [2]). Die Attribute Assertion kann eine SAML 2.0 Attribute Assertion sein, aber auch auf einer anderen Technologie basieren.

2.2 Attributaggregation

Der Begriff der Attributaggregation wird von N. Klingenstein in „Attribute Aggregation and Federated Identity“ [6] genau beschrieben. Man versteht darunter den Prozess, Attribute zu einer bekannten digitalen Identität von verschiedenen Quellen abzufragen und zusammenzustellen.

2.3 Bereich STIAM-Domäne

Als Bereich kann eine begrenzte Gruppe von Informationsbezügern und -lieferanten angesehen werden, welche ein bestimmtes Set 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.

2.4 Discovery Service (WAYF - Where Are You From)

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

2.5 Empfängerbaustein

Der Empfängerbaustein realisiert eine standardisierte STIAM-Schnittstelle für eine Relying Party, welche die STIAM-Protokolle nicht direkt unterstützt (vgl. Abbildung 2).

2.6 GUID

Eine GUID ist die auf dem STIAM-Hub abgelegte, eindeutige Identität eines Subjekts, an welche die LinkedID in dessen Link Table geknüpft werden.

2.7 Identity Linking

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

2.8 Identity Provider/ Attribut-Autorität (IdP/AA)

Im SuisseTrustIAM-Kontext können Unternehmen und Organisationen als Informationslieferanten eine IdP/AA-Komponente bereitstellen, welche als IdP agiert, aber auch zu einer ihr bekannten Identität Informationen in Form von Attributen ausstellen kann. Die Anforderungen an einen solchen IdP/AA und dessen Funktionen werden in den SuisseTrustIAM Dokumenten genauer beschrieben (vgl. auch STIAM-IdP, STIAM-Sender und Abbildung 2).

2.9 Linking Protokoll

Der Benutzer kann IdPs oder AAs 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 Authentisierungsservice authentifizieren. Dadurch kann ein eindeutiger Identifikator zwischen STIAM-Hub und dem IdP oder der AA ausgetauscht werden.

2.10 Metadaten (Metadata)

In SuisseTrustIAM werden die Metadaten innerhalb des Organisations- und Komponentenmanagements für die jeweils registrierten STIAM-Komponenten zentral in der STIAM-Hub Datenbasis abgelegt. Die Metadaten beschreiben die Komponenten der registrierten Organisationen und Provider mit ihren Federation-Service-Endpunkten, Zertifikaten und den angeforderten bzw. zur Verfügung gestellten Attributen.

2.11 OpenID Connect

OpenID Connect 1.0 (OIDC) [7] definiert eine einfache Identitätsschicht auf der Basis von OAuth 2.0 (RFC 6749), die auch von Mobilgeräten verwendet werden kann. OIDC verwendet das Basisprotokoll OAuth sowohl für die Authentisierung als auch für die Zugangskontrolle. Als Security-Tokens werden JSON Web Tokens [8] verwendet.

2.12 RP (Relying Party, Lösungsanbieter, Informationsbezüger)

Unternehmen und Organisationen können als Informationsbezüger (Webportal mit kontrolliertem Zugang auf eine Ressource) auftreten. In dieser Rolle benötigen sie Informationen über einen zugreifenden Benutzer, um die Nutzung der Ressource zu gewähren oder abzulehnen.

2.13 SAML 2.0

SAML (Security Assertion Markup Language) erlaubt es, Informationen über Authentifizierungs- und Attributinformationen zwecks Autorisierung standardisiert zwischen mehreren Teilnehmern auszutauschen. Der SAML-Standard [9] beschreibt die Syntax und Regeln zum Anfordern, Erstellen und Austauschen von SAML-Assertions.

2.14 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 [10] beschreibt webbasierte Authentisierungsszenarien, inkl. Identity Federation, für Browser.

2.15 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 (vgl. Kapitel 2.25 und 2.26).

2.16 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.

2.17 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. Abbildung 2).

2.18 Security Token

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

2.19 STIAM Certificate Service Provider (STIAM-CSP)

Ein STIAM-CSP ist ein CSP, der von der STIAM-Community akzeptiert wird.

2.20 STIAM-Empfänger

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 eines Security Tokens. Der STIAM-Empfänger ist eine Relying Party, beispielsweise ein Portal.

2.21 STIAM-Hub (Vermittler, Intermediär)

Der STIAM-Hub als Kernstück der SuisseTrustIAM-Plattform hat zwei Funktionen. Erstens bietet er zur Definitionszeit die Trust- und eIdentity-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.

Die administrativen Aufgaben auf dem STIAM-Hub können grob in folgende Prozesse und Funktionen aufgeteilt werden (vgl. dazu die administrativen Prozesse in Kapitel 7):

- *User Management:* Benutzer können auf dem STIAM-Hub einen User-Account eröffnen und diesen verwalten. Alternativ ist es auch möglich, dass ein System Administrator einer Organisation User-Accounts für einen (oder mehrere) Benutzer bzw. Maschinen erstellen kann.
- *Organisation Management:* Eine Organisation wird vom SuisseTrustIAM Betreiber initial in der Datenbasis eröffnet. Ein Mitarbeitender der Organisation (in der Rolle eines Organisationsverantwortlichen) wird dabei ermächtigt, bestimmte Eigenschaften der Organisation zu administrieren und zusätzliche Systemadministratoren zu erstellen und zu ermächtigen. Damit können administrative Aufgaben der Organisation aufgetrennt und delegiert werden (vgl. dazu die Definition der Rollen und Prozesse in der eCH-0169 SuisseTrustIAM-Geschäftsarchitektur [11]).
- *Komponenten Management:* Ziel der zentralen Administration auf dem STIAM-Hub ist die einfache und selbstständige Verwaltung der STIAM-Komponenten durch deren Systemverantwortlichen. Dieser kann selbstständig einzelne Komponenten zu SuisseTrustIAM hinzufügen bzw. verwalten. Für diese Komponenten müssen bestimmte Parameter, welche für ihre Rolle innerhalb der STIAM-Plattform notwendig sind, erfasst und konfiguriert werden.
- *Attribut Management:* Der SuisseTrustIAM Betreiber unterhält eine Liste von Attributen, welche in der SuisseTrustIAM-Community verwendet werden können.

2.22 STIAM-IdP

Ein Identity Provider hat in STIAM die Funktion, ein Subjekt zu authentifizieren. Ein STIAM-IdP implementiert eine standardisierte STIAM-Schnittstelle zum STIAM-Hub (vgl. Abbildung 2).

2.23 STIAM-Komponente

Zu den STIAM-Komponenten gehören STIAM-Sender (Attribut-Autorität), STIAM-Empfänger (Relying Party), 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.

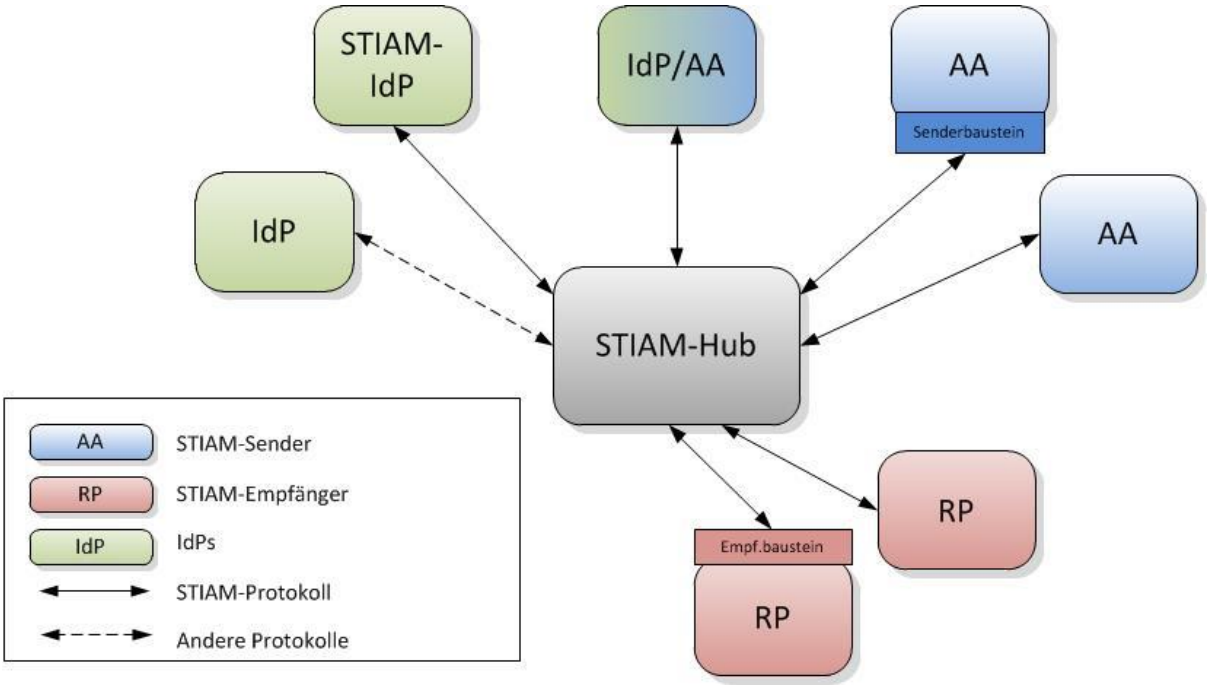


Abbildung 2: STIAM-Komponenten

2.24 STIAM-Sender

Der STIAM-Sender ist eine Attribut-Autorität (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. Abbildung 2).

2.25 WS-Federation

WS-Federation in der aktuellen Version 1.2 [12] [13] 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. Sowohl bei WS-Trust wie auch bei WS-Federation kann das SAML-Tokenformat als Security Tokens verwendet werden.

2.26 WS-Trust

Der von OASIS spezifizierte Web Service Trust (WS-Trust) [14] in der aktuellen 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. Dieses Protokoll ermöglicht einem Consumer (z.B. ein Web-Service-Client), den Austausch eines bestimmten Sicherheitstokens von einem anerkannten Aussteller, dem Security Token Service (STS), anzufordern und einer Relying Party zu übergeben.

3 SuisseTrustIAM Identity Federation Modell

3.1 Konzept SuisseTrustIAM

Ziel eines STIAM-Hubs ist es, die Informationslieferanten und -konsumenten auf einfache Weise zu verbinden und gleichzeitig gegenseitig zu abstrahieren. In einer klassischen Identity Federation Umgebung stehen Identity Provider als Informationslieferanten und Relying Parties als -konsumenten in einer direkten Beziehung zueinander. In diesem Modell agiert der STIAM-Hub gegenüber den Informationskonsumenten als Vermittler von gesicherten Informationen zu einer digitalen Identität. Er abstrahiert zudem gegenüber den Teilnehmern beider Ebenen die gesprochenen Protokolle, den Austausch notwendiger Informationen zwischen den Teilnehmern und den unumgänglichen Aufbau der Vertrauensbeziehungen. Damit kann die Interoperabilität der einzelnen Teilnehmer vereinfacht werden, insbesondere wenn die Anzahl der Teilnehmer gross ist.

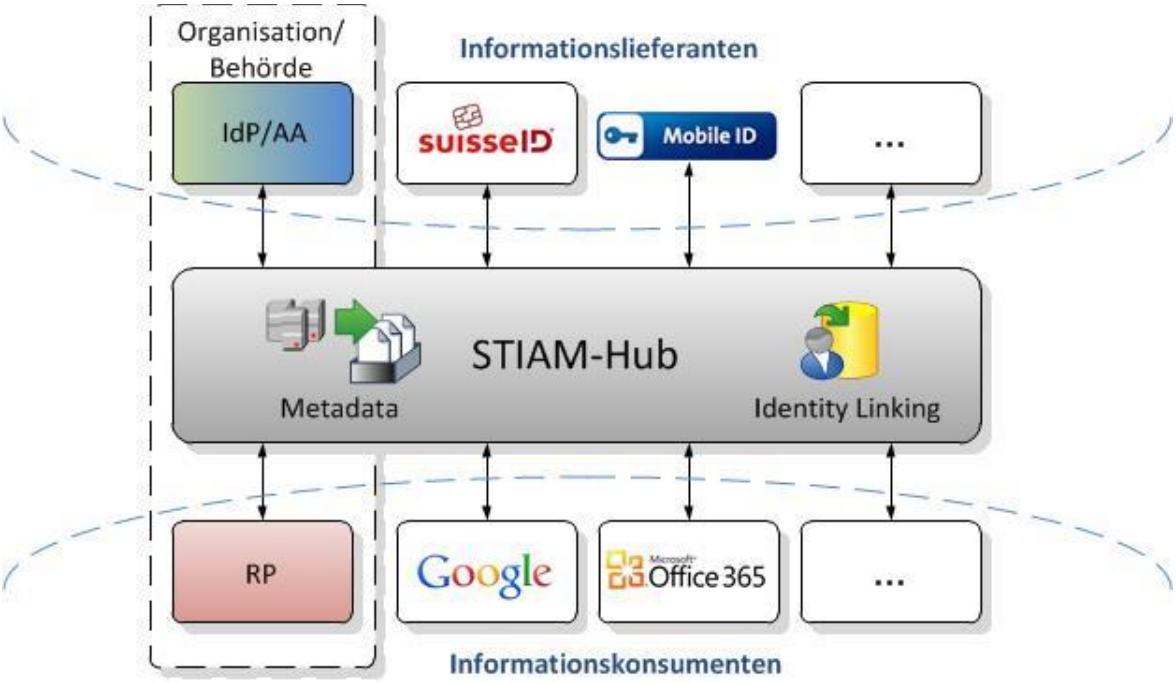


Abbildung 3: STIAM-Hub und Dienste

Eine Organisation (Behörde, Unternehmen) kann als Kunde dieser Infrastruktur selbst eigene Applikationen als Relying Parties (RP) einbinden, um zugreifende Benutzer durch einen der angeschlossenen Informationslieferanten authentifizieren zu lassen. Umgekehrt kann diese Organisation aber auch selbst Lieferant (IdP/AA) von digitalen Identitäten und Attributinformationen für die eigenen oder für andere Konsumenten sein. Es können aber auch bereits existierende Cloud-Lösungen, wie Google-Mail oder MS-Office 365, als Informationskonsumenten eingebunden werden. Um die Dienste der angeschlossenen Teilnehmer verwalten zu können und gegenseitig bekannt zu machen, unterhält der STIAM-Hub eine Metadatenbasis (Metadata) der angegliederten Systeme. Damit der STIAM-Hub die gewünschten Informationen eines Subjekts zusammentragen kann, benötigt er pro Subjekt eine Art *Link*

Table (Identity Linking), um die bei den Informationslieferanten dezentral vorhandenen digitalen Identitäten zuordnen zu können.

3.2 STIAM-Hub-Modell

In den eCH-0107 Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung wurden bereits verschiedene Identity Federation Konzepte vorgestellt. In diesem Kapitel sollen die für SuisseTrustIAM relevanten Modelle vertieft behandelt und veranschaulicht werden. Bei der SuisseTrustIAM Plattform handelt es sich um ein *Hub-,n'-Spoke* Modell[2] (STIAM-Hub-Modell). Dieses Modell basiert auf einem zentralen STIAM-Hub, welchem alle beteiligten Parteien vertrauen.

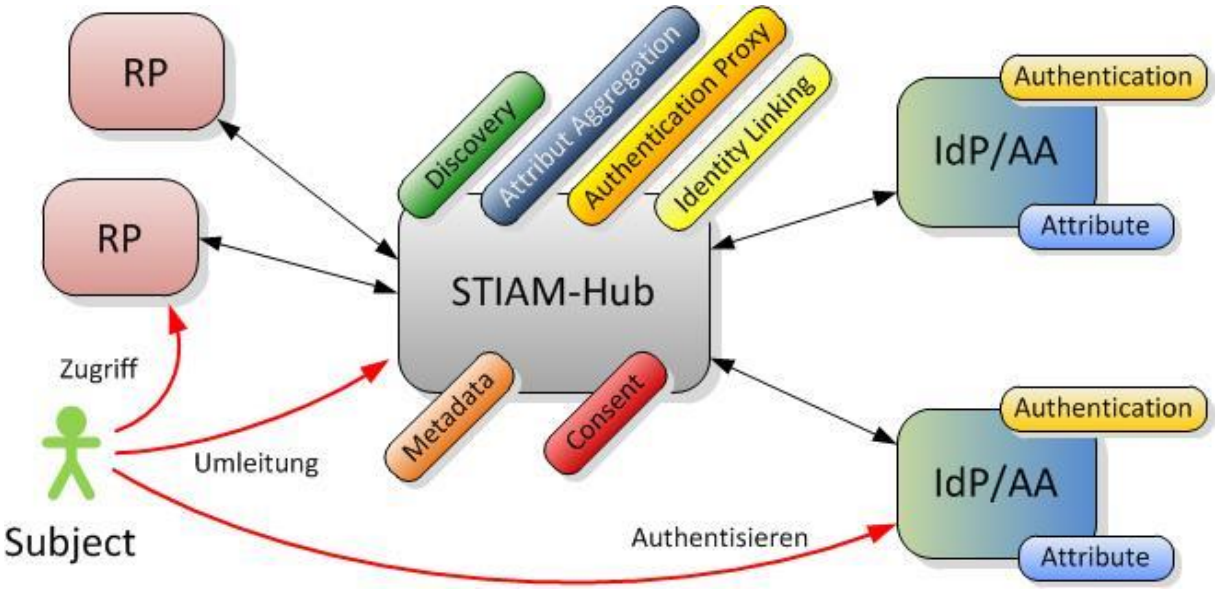


Abbildung 4: STIAM-Hub-Modell

In Abbildung 4 markieren die schwarzen Pfeile die Kommunikationsbeziehungen zwischen den einzelnen Komponenten.

Die roten Pfeile verdeutlichen die Interaktionen des Subjekts:

- Zugriff: Das Subjekt möchte auf eine geschützte Ressource einer Relying Party zugreifen.
- Umleitung: Die Relying Party veranlasst eine Umleitung des Subjektes zum STIAM-Hub, wo mit Hilfe des Discovery-Dienstes der Identity Provider ausgewählt wird.
- Authentisieren: Der STIAM-Hub leitet das Subjekt zum gewählten Identity Provider weiter, wo sich das Subjekt nun authentifizieren kann.

Wie in Abbildung 4 gezeigt, kann der STIAM-Hub verschiedene Dienste innerhalb der Identity Federation übernehmen und zentral ausüben:

Discovery: Der STIAM-Hub ist dafür zuständig, den Benutzer (Subjekt) zu einem Identity Provider seiner Wahl zur Authentifizierung zu leiten. Er zeigt dem Subjekt eine Auswahl po-

[2] Nabe und Speiche

tenziell möglicher Identity Provider an, oder leitet dieses direkt zum einzig möglichen IdP zur Authentisierung um.

Authentication Proxy: Der STIAM-Hub authentifiziert ein Subjekt in der Regel nicht selbst. Er agiert viel eher als Authentisierungsvermittler (Proxy), indem er sich gegenüber dem authentisierenden IdP wiederum als Relying Party verhält und in seinem eigenen Namen eine entsprechende Anfrage startet.

Attribute Aggregation: Der STIAM-Hub muss in der Lage sein, nach erfolgter Authentifizierung bei einem Identity Provider zusätzliche Informationen (Attribute), welche eine Relying Party angefordert hat, von möglichen Attributlieferanten mit der Identität des Subjekts zu verbinden und an die anfragende RP zurückzuliefern.

Metadata: Der STIAM-Hub verwaltet und vermittelt alle notwendigen Informationen zwischen den Komponenten und stellt damit die Vertrauensbeziehungen zwischen diesen her. Die vom Hub zentral geführten Metadaten enthalten die Informationen aller IdP/AAs und aller RPs. Diese Metadaten werden vom STIAM-Hub digital signiert und stellen damit eine vertrauenswürdige dritte Instanz (Trusted Third Party) dar.

Consent: Bevor die Zusicherung einer Authentifizierung (*Authentication Statement*) oder ein Set an Attributen einer Relying Party übergeben werden kann, muss der Benutzer seine Einwilligung zur Weitergabe geben.

Identity Linking[3]*:* Wenn eine Relying Party - für den Zugriff auf eine von ihr kontrollierten Ressource - Attribute aus verschiedenen Quellen verlangt, so muss sowohl der STIAM-Hub wie auch diese Informationsquelle (Attribut-Autorität) eine Möglichkeit haben, herauszufinden für welchen, ihr lokal bekannten Benutzer sie ein Attribut ausstellen muss. Alle informationsliefernden Dienste und der STIAM-Hub müssen über einen oder mehrere Identifikator(en) verfügen, über welche(n) sie die digitale Identität des Subjekts eindeutig zuordnen können. Der STIAM-Hub muss im Rahmen des User Managements eine Link Table führen, in welcher ein Benutzer seine Identifikatoren zentral hinterlegen kann.

Die Liste der zentralisierten Services ist im STIAM-Hub-Modell nicht im Voraus vorgegeben. Die Ausübung einzelner Services kann auch verteilt bleiben. So ist es absolut denkbar, dass die Zustimmung (Consent) zu einer Authentisierungs- bzw. Attributfreigabe weiterhin durch den IdP/AA erfolgt.

3.3 Verfahren zur Identitäts- und Attributvermittlung

Wichtigster Unterschied zu einem klassischen Identity Federation Modell (Cross Domain oder full-meshed Modell) ist der Umstand, dass RP und IdP/AA nicht mehr direkt kommunizieren, sondern zur Laufzeit die Kommunikation ausschliesslich über den STIAM-Hub leiten.

Dies hat zur Folge, dass dieser in Vertretung der Relying Party die Authentifizierung des Subjekts bei einem IdP anstossen und die Aggregation der angeforderten Informationen übernehmen muss. Verschiedene IdP/AAs können in diesem Szenario zuständige Quellen für die Authentifizierung und für Benutzerattribute sein.

[3] Das System des Identity Linking mittels Link Table basiert auf den Erkenntnissen des Shintau-Projekts der University of Kent [15].

SuisseTrustIAM entspricht diesem Modell, da ein Subjekt von einem Identity Provider seiner Wahl authentifiziert werden kann, Attributinformationen hingegen aus anderen Quellen stammen können.

Je nachdem wie viele Attributlieferanten bei einer Anfrage beteiligt sind und wie diese zum authentisierenden Identity Provider in Beziehung stehen, kann der STIAM-Hub unterschiedliche Verfahren zur Attributaggregation wählen. Es sind grundsätzlich zwei Verfahren mit unterschiedlichem Protokollablauf möglich, welche im Folgenden vorgestellt werden.

3.3.1 Proxying

Beim Proxying setzt die anfragende Komponente (in unserem Fall der STIAM-Hub) eine sequenzielle Anfrage über mehrere Destinationen ab. Die letzte Destination in der Kette ist der authentisierende Identity Provider. Jeder dazwischenliegende IdP/AA (Authentisierungsproxy) wird nach erfolgter Authentifizierung des Subjekts die Attribute hinzufügen, für welche er zuständig ist. Das Verfahren bedingt aber, dass alle beteiligten Informationslieferanten für jedes mögliche Subjekt in Kenntnis des Identifikators (UID) des authentisierenden IDP/AAs sind. Daher eignet sich das Verfahren besonders für folgende Szenarien:

- Der STIAM-Hub agiert selbst als einziger Attributlieferant in der Kette zwischen RP und authentisierendem IdP/AA.
- Authentisierender Identity Provider und involvierte Attributlieferanten teilen einen bereits vereinbarten und zuvor ausgetauschten Identifikator.
- Eine Kette der involvierten Attributlieferanten ist relativ kurz und besteht aus hochverfügbaren, belastbaren Servern.

Um zu diesem Identifikator zu gelangen, kann der Attributlieferant diesen durch den Benutzer selbst eingeben lassen oder in einem Registrierungsprozess durch den IdP/AA elektronisch bestätigen lassen.

Beispiel für eine Attributaggregation mit Proxying in SuisseTrustIAM könnte die Anbindung eines SuisseID Claim Assertion Services (CAS) sein, wobei der authentifizierende IdP/AA in diesem Fall der SuisseID IdP sein muss.

Abbildung 5 stellt dar, wie alle beteiligten Informationslieferanten dezentral über denselben Identifikator (UID) eines Subjekts verfügen müssen, damit jede der beteiligten Komponenten die digitale Identität des Subjekts eindeutig zuordnen kann. In den lokalen Userdatenbasen (User DB) können jeweils lokale Identifikatoren abgelegt sein. Über eine Mapping-Table können die UIDs des authentisierenden IdP/AAs mit den lokalen Identifikatoren zugeordnet werden.

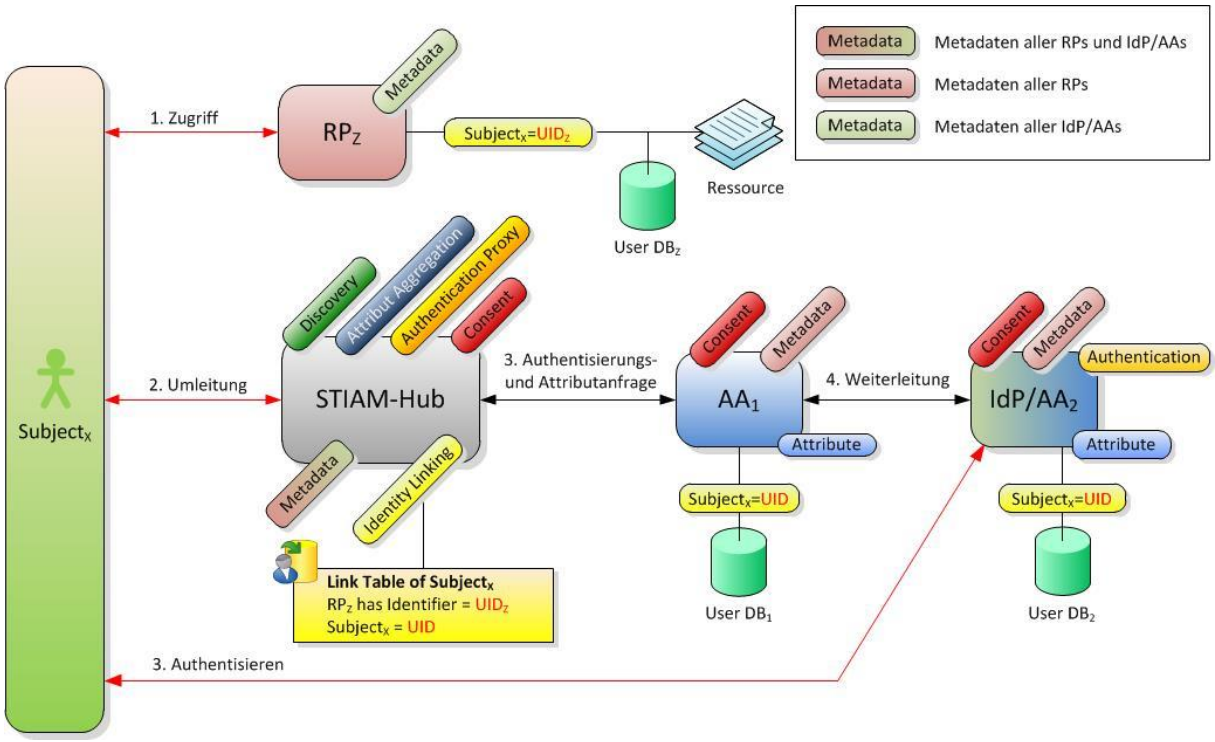


Abbildung 5: Identität- und Attributvermittlung mittels Proxying

Ein Benutzer ($Subject_X$) greift in diesem Szenario auf eine Relying Party (RP_Z) zu. Die Relying Party leitet den Benutzer zum STIAM-Hub weiter. Aus den Metadaten der RP kann der Hub entnehmen, dass Attribute von AA_1 benötigt werden, der Benutzer sich aber bei IdP/AA_2 authentisieren muss. Der Hub erstellt einen Proxypfad mit AA_1 als erste Destination und IdP/AA_2 als authentisierenden Server (2. Destination). Er leitet den Benutzer zusammen mit dieser Pfadinformation an AA_1 um. Dieser erkennt anhand des Proxypfads, dass er den Benutzer zuerst zu IdP/AA_2 weiterleiten muss. IdP/AA_2 authentifiziert den Benutzer, fügt die von ihm selbst bereitgestellten Attribute bei und leitet ihn zurück zum AA_1. In seiner Antwort ist die UID des Benutzers enthalten, so dass AA_1 die Identität des Benutzers nun erkennt und nun ebenfalls seine Attribute hinzufügen kann. Er sendet die nun vollständige Information zurück zum Hub, welcher die erfolgte Authentifizierung und die einzelnen Attribute prüft und in einer eigenen Assertion an die RP als Bestätigung zurücksendet.

3.3.2 Identitätsübergabe an die AA

Wenn mehrere unabhängige Attributlieferanten in einer Abfrage enthalten sind, so verfügen diese in der Regel nicht über einen gemeinsam bekannten Identifikator. Hier kommt die Link Table des STIAM-Hubs zum Zug, in welcher nun pro Subjekt zentral die Identifikatoren der Attributlieferanten gespeichert werden. Dies ermöglicht dem STIAM-Hub nach erfolgter Authentisierung des Benutzers bei einem Identity Provider, die noch fehlenden Attribute durch direkte Anfragen bei den Attributlieferanten einzuholen. Er schickt dazu zuvor eine unsolicited[4] Authentication-Response an den Attributlieferanten (vgl. dazu den Bericht zum Suisse-TrustIAM PoC [15] von ATOS).

[4] unsolicited message: unaufgeforderte Nachricht

Wie in Abbildung 6 dargestellt, ermöglicht der Linking Service dem Benutzer in einer Tabelle, Identifikatoren zu autoritativen Quellen zentral zu pflegen. Durch diese Link Table ist es möglich, nach einer erfolgreichen Authentisierung Attributabfragen in einer unbestimmten Reihenfolge direkt bei den autoritativen Quellen zu machen.

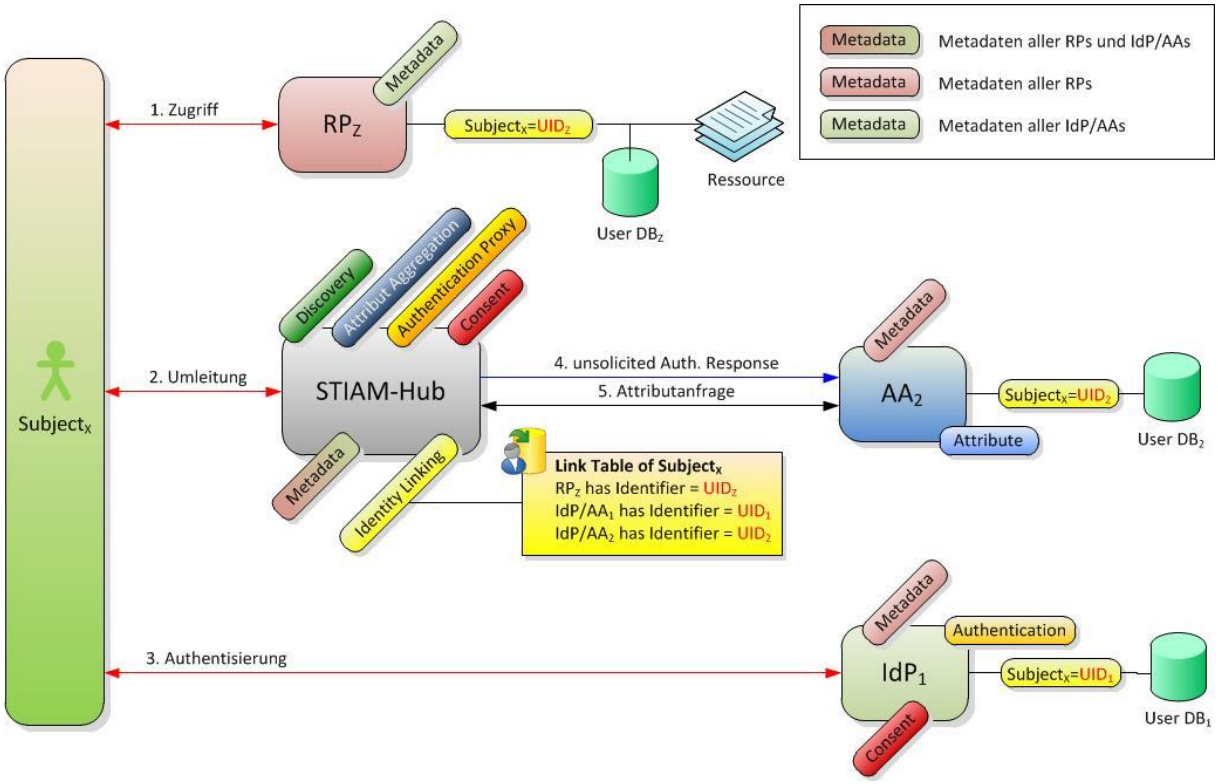


Abbildung 6: Identitäts- und Attributvermittlung mittels solicited Messages

Ein Benutzer greift in diesem Szenario auf eine Relying Party (RP_z) zu. Die Relying Party leitet den Benutzer zum STIAM-Hub weiter. Aus den Metadaten der RP kann der Hub entnehmen, dass Attribute von AA_2 benötigt werden, der Benutzer sich aber bei IdP/AA_1 authentisieren muss. Der Hub leitet den Benutzer zuerst zu IdP_1 um, damit sich dieser hier authentisiert. Nach erfolgter Authentifizierung kennt der STIAM-Hub den Benutzer und kann anhand der Link Table den Identifikator für AA_2 entnehmen. Er schickt zunächst eine ‚unsolicited' Authentication Response mit der UID_2 an den AA_2 (in Abbildung 6 blau markiert). Danach kann er eine direkte Anfrage für ein bestimmtes Set an Attributen bei AA_2 absetzen. AA_2 verifiziert die Anfrage des Hubs und antwortet mit der gewünschten Attributassertion. Der Hub, welcher die erfolgte Authentifizierung und die einzelnen Attribute selbst geprüft hat, erstellt eine eigene Assertion und sendet diese an die RP zurück.

3.4 Validierung von Identitäts- und Attributinformationen

Im SuisseTrustIAM Modell vermittelt der STIAM-Hub Identitäts- und Attributinformationen (Security Tokens, Attribute Assertions), welche von den autoritativen Quellen fälschungssicher ausgestellt werden, gegenüber der Relying Party. Dies kann je nach Anforderung der Relying Party auf zwei verschiedene Arten erfolgen.

3.4.1 Identity Proxying Modus (IP-Mode)

Der STIAM-Hub nimmt zur Laufzeit die vom authentisierenden Identity Provider bzw. die von den Attributlieferanten ausgestellten Security Tokens und Assertions entgegen und validiert sie selbst. Er generiert daraus ein neues, von ihm stammendes digital signiertes Token (oder eine Assertion) und gibt dieses an die Relying Party weiter. In diesem Fall kann die Relying Party nur die Aussagen des STIAM-Hubs validieren. Die Relying Party muss damit den Aussagen des STIAM-Hubs vollumfänglich vertrauen.

3.4.2 Identity Relaying Modus (IR-Mode)

Der STIAM-Hub nimmt zur Laufzeit die vom authentisierenden Identity Provider bzw. die von den Attributlieferanten ausgestellten Security Tokens und Assertions entgegen, validiert sie aber nicht. Er generiert eine Antwort an die Relying Party, worin alle angeforderten Tokens und Assertions im Original enthalten sind, und sendet diese an die Relying Party. Die RP validiert zuerst die Authentizität des STIAM-Hubs und dann die der in der Nachricht integrierten Tokens und Assertions. In diesem Modus kann die Relying Party direkt die Aussagen der ausstellenden Quellen überprüfen und muss damit nicht alleine dem STIAM-Hub vertrauen. Die notwendigen Informationen (Zertifikate) zur Validierung der Token und Assertions kann die Relying Party aus den Metadaten entnehmen.

3.5 Security Token und STIAM-Protokolle

Der SuisseTrustIAM STIAM-Hub ist als Vermittler in der Lage, Security Tokens in einer standardisierten Form zu erzeugen und als Authentisierungs- und Berechtigungsinformation an die Relying Party zu übergeben. Diese Security Tokens und Attribute Assertions können auf verschiedene Arten ausgestellt werden. Dazu bestehen einschlägige Standards, wie u.a. SAML 2.0 oder WS-Trust bzw. WS-Federation.

Die folgende Tabelle enthält Protokolle, welche von den SuisseTrustIAM Entitäten verwendet werden können:

Protokoll	STIAM-Empfänger	STIAM-Hub	STIAM-Sender	STIAM-IdP	Bemerkung
SAML 2.0 Web Browser SSO-Profile mit HTTP POST Binding	SOLLTE	MUSS	SOLLTE	SOLLTE	• Für benutzerzentrierte Kommunikation
WS-Trust mit SAML-Token als Security Token	KANN	MUSS	KANN	KANN	• Für Service-zu-Service Kommunikation • Die vom STIAM-Hub ausgestellten Security Token sind SAML 2.0-

Protokoll	STIAM-Empfänger	STIAM-Hub	STIAM-Sender	STIAM-IdP	Bemerkung
					Assertions wie jene des Web Frontend • Ein SuisseTrustIAM-IdP/AA sollte WS-Trust unterstützen, wenn er Web-Services authentifizieren muss.
OpenID Connect	kann	KANN	kann	kann	Mit JSON Web Tokens
Weitere Protokolle (z.B. Mobile ID, OpenID, u.a.)	kann	KANN	kann	kann	Der STIAM-Hub wird künftig auch andere Protokolle unterstützen, um weitere kommerzielle Identity Provider einbinden zu können.

Tabelle 1: STIAM-Protokolle

Wie obenstehende Tabelle zeigt, sind SAML 2.0 und WS-Trust die Hauptprotokolle, welche in SuisseTrustIAM zur Anwendung kommen. Es soll aber auch möglich sein, weitere Protokolle in die SuisseTrustIAM Infrastruktur zu integrieren - insbesondere gegenüber kommerziellen Authentication Providern. Durch die Authentisierungsproxy-Funktion des STIAM-Hubs können andere Technologien leicht eingebunden und gegenüber den Relying Parties abstrahiert werden. ATOS hat in ihrem Bericht „SAML Proxying and Attribute Services“ [15] aufgezeigt, dass mit einem STIAM-Hub die Integration von Google als Identity Provider mit den Technologien OAuth 2.0 [16] [17] und OpenID Connect (OIDC) [7] sehr einfach umsetzbar ist.

Auf der anderen Seite ist aber auch eine Anbindung von nicht-SAML-fähigen Relying Parties möglich. Auch hier bestehen mit OIDC, WS-Trust usw. andere Technologien, welche künftig integriert werden können.

3.6 Vertrauensbeziehung zwischen den Komponenten

Alle beteiligten Akteure (Identity Provider, Attribut-Autorität, Relying Party und STIAM-Hub) müssen sich gegenseitig vertrauen. Die Vertrauensbeziehungen werden auf zwei Ebenen umgesetzt:

- Der Kommunikationskanal zwischen STIAM-Hub und IdP/AA bzw. zwischen STIAM-Hub und Relying Party wird mittels 2-way SSL/TLS verschlüsselt und authentisiert. Dies bedingt die Ausrollung vertrauenswürdiger Serverzertifikate für alle beteiligten Services.
- Die Inhalte aller übermittelter Nachrichten (Request oder Assertion) vom und zum STIAM-Hub müssen fälschungssicher (digital signiert) sein.

- Die dazu benötigten Zertifikate müssen durch einen vertrauenswürdigen Certificate Service Provider (CSP) ausgestellt werden.

3.7 Session Handling

Die vom STIAM-Hub an die Relying Party vermittelten Identitäts- und Attributinformationen werden zeitnah von den zuständigen Quellen eingeholt und entweder vom STIAM-Hub selbst oder vom Konsumenten geprüft. Der STIAM-Hub speichert dabei grundsätzlich keine Identitätsinformationen. Es können aber folgende Ausnahmen festgehalten werden:

- Der STIAM-Hub kann zur Laufzeit Identitäts- und Attributinformationen eines Subjekts zwecks Aggregation für die Dauer einer Abfrage zwischenspeichern.
- Der STIAM-Hub kann nach erfolgter Authentisierung eines Subjekts den ‚Authentication State' in einem entsprechenden Session Cookie speichern, sofern dies die anfragende Relying Party zulässt[5].
- Der STIAM-Hub kann ‚aggregierte Attributinformationen' in einem Session Cookie verschlüsselt speichern[6].

3.8 Vertraulichkeit von Attributinhalten

Identitäts- und Attributinformationen zu einem Subjekt werden aus verschiedenen Quellen bezogen und vom STIAM-Hub vermittelt. Diese Attribute können Daten mit sensitiven Informationen beinhalten. Deshalb muss es möglich sein, diese Informationen nur für die anfragende Relying Party zugänglich zu machen. Folgende Funktionen werden in SuisseTrust-IAM optional zur Verfügung gestellt:

- Ein Informationslieferant kann den Inhalt eines Attributs für eine Relying Party verschlüsseln.
- Die notwendigen Informationen zum Verschlüsseln der Attributinformationen kann der Informationslieferant aus den Metadaten entnehmen.

3.9 Anonymisierung der Identitäten

Das Identity Linking anonymisiert implizit die digitalen Identitäten zwischen den SuisseTrust-IAM Informationslieferanten (IdP und AA), da jeder Link über einen eigenen Identifikator verfügt. Nur wer Zugriff auf die Link Table hat, kann die Identitäten miteinander verknüpfen.

Ausnahme: Wenn Proxying (wie in Kapitel 3.3.1 beschrieben) zur Anwendung kommt, sind alle beteiligten Services über denselben Identifikator in Kenntnis.

Anders sieht es zwischen STIAM-Hub und Relying Party aus. Der STIAM-Hub muss gegenüber der Relying Party einen Identifikator in seiner Antwort zurückgeben. Je nach gestellter

[5] Die Relying Party kann eine Option zur Authentisierung des Subjekts bereits zur Definitionszeit in ihren Metadaten oder jeweils zur Laufzeit innerhalb einer Anfrage vorgegeben.

[6] Die Gültigkeit der abgelegten Attributinformation darf die max. Gültigkeit des Attributs und die der Security Session nicht überschreiten.

Anforderung (insbesondere Schutz der Privatsphäre) kann der STIAM-Hub gegenüber einer Relying Party unterschiedliche Typen von Identifikatoren zurückgeben (vgl. dazu UID_Z in Abbildung 5 und Abbildung 6).

Identifikator	Beschreibung	Verwendung
Distributed ID	Der STIAM-Hub gibt an alle anfragenden Relying Parties immer denselben Identifikator eines Subjekts in seinen Antworten zurück. Der gemeinsam genutzte Identifikator kann auch über andere Kanäle im Vorfeld ausgetauscht werden (Out-of-Band[7] Linking).	Eine Distributed ID erlaubt einer Relying Party lokal eine digitale Identität beim ersten Login zu erstellen oder mit einer bereits bestehenden zu verbinden (Identity-Mapping). Da der Identifikator über mehrere Relying Parties bekannt ist, können erhaltene Attribute leicht Out-of-Band korreliert werden.
Persistent ID	Der Identity Provider (bzw. STIAM-Hub) gibt pro anfragende Relying Party immer einen unveränderten, bestimmten Identifikator eines Subjekts in seinen Antworten zurück. Ein persistenter Identifikator verbirgt die wahre Identität eines Subjekts gegenüber der anfragenden Relying Party.	Auch eine persistente ID erlaubt einer Relying Party lokal eine digitale Identität beim ersten Login zu erstellen oder mit einer bereits bestehenden zu verbinden (Identity-Mapping). Da der Identifikator nur für eine Relying Party bestimmt ist, ist es viel schwieriger, auf direktem Weg Benutzeraktivitäten zwischen unterschiedlichen Relying Parties zu korrelieren.
Transient ID	Transiente Identifikatoren verfolgen dasselbe Ziel wie persistente Identifikatoren, nur wird in diesem Fall vom STIAM-Hub pro Login Session eines Subjekts ein zufälliger Identifikator an die Relying Party zurückgegeben.	Eine Relying Party kann anhand des erhaltenen Identifikators die Identität eines Subjekts zwischen zwei einzelnen Sessions nicht mehr verknüpfen. Zugriffsberechtigungen müssen auf Attributinformationen basieren.
Requested ID	Die Relying Party kann in ihrem Authentication Request zur Laufzeit einen ihr bekannten Identifikator angeben. Der STIAM-Hub muss seine Antwort auf diesen Identifikator beziehen, damit die Relying Party in	Eine Relying Party fragt beim STIAM-Hub nach weiteren Attributen zu einem bereits authentifizierten Subjekt nach. Der verwendete Identifikator muss beiderseits bekannt sein.

[7] Über einen anderen (zweiten) Kanal übermittelt

Identifikator	Beschreibung	Verwendung
	der Lage ist, die erhaltenen Identitätsinformationen mit lokalen Benutzerdaten zu verknüpfen.	

Tabelle 2: Typen von Identifikatoren

Zu beachten ist, dass unabhängig von den in Tabelle 2 aufgeführten Typen von Identifikatoren eine Verlinkung der Identitäten immer dann möglich ist, wenn IdP/AA und RP je über genügend identifizierende Attribute zu einem Subjekt verfügen und diese zur Laufzeit übertragen werden.

Der STIAM-Hub gibt pro Subjekt und RP eine *Persistent ID* oder eine *Transient ID* in seiner Antwort heraus.

3.10 Nachvollziehbarkeit von Prozessen

Zwecks Nachvollziehbarkeit müssen Prozesse, welche zur Definitionszeit wie auch zur Laufzeit vollzogen werden, fälschungssicher gespeichert und für eine rechtlich vorgegebene Zeit aufbewahrt werden. Die Erfassung und Speicherung aller Kommunikationsabläufe und deren eindeutige Zuordnung zu einem Subjekt wird bewusst gefordert. Wo bestimmte Informationen erfasst und gespeichert werden, ist in Kapitel 5.6 näher beschrieben. Einzelne Daten müssen zentral aufgezeichnet werden, da die peripheren Komponenten (AA, IdP und RP) jeweils nur über die für sie notwendigen Informationen verfügen und somit keine Gesamtübersicht über einen Laufzeitprozess festgehalten werden kann.

Der Betreiber eines STIAM-Hubs muss in der Lage sein, die Aufbewahrungspflicht der protokollierten Informationen gemäss schweizerischen Datenschutzauflagen erfüllen zu können.

3.11 Kategorisierung von Attributen

Ausgehend vom Rahmenkonzept muss die SuisseTrustIAM Plattform die folgenden Anwendungsszenarien zur Laufzeit unterstützen können:

- Ein Benutzer soll als Privatperson und Bürger den STIAM-Hub nutzen können, um die digitale Identität bestätigen und um optional persönliche Informationen durch den STIAM-Hub aggregieren zu lassen.
- Benutzer oder Services (Maschinenaccounts) eines Unternehmens sollen mit Hilfe des STIAM-Hubs auf Dienste ausserhalb der eigenen Organisation zugreifen können, um im Namen dieses Unternehmens autorisierte online-Zugriffe machen zu können.

In beiden Fällen werden vom STIAM-Hub Identitätsinformationen in Form von Attributen vermittelt, welche aber ganz unterschiedliche Verwendungszwecke haben. Zum einen sind persönliche Informationen im Spiel, welche zur Herausgabe an eine Relying Party das Einverständnis des Benutzers zwingend voraussetzen und zum anderen handelt es sich um unternehmensspezifische Informationen, wie die Zugehörigkeit zum Unternehmen und einem Funktionsnachweis, welche keine explizite Zustimmung des Benutzers erforderlich machen.

Google hat in seinem Technologieüberblick ‚Overlap of Identity Technologies' [18] den Begriff der ‚Identity Camps' kreiert. Zusammenfassend unterscheidet Google die zwei Katego-

rien Enterprise-IAM und Internet-IAM Camp. Die beiden Camps unterscheiden sich in erster Linie durch die Frage, wem die Identitätsdaten gehören und wer demzufolge bei der Auslieferung sein Einverständnis geben muss.

- *Enterprise-IAM:* Ressourcen und insbesondere Identitätsdaten (HansMuster@Organisationsverzeichnis) gehören der Organisation. Diese entscheidet im Rahmen geltender Gesetze und Verträge über die Weitergabe der Daten. Der einzelne Mitarbeiter („Hans Muster“) spielt im Rahmen dieser Entscheidung eine sekundäre Rolle. In Abhängigkeit der zu übermittelnden Informationen sind keine Benutzereinwilligung (consent) und keine benutzerzentrierte (user-centric) Kommunikation notwendig.
- *Internet-IAM:* Ressourcen und insbesondere die Identitätsdaten (HansMuster@Facebook) gehören dem Individuum. Dieses alleine muss über die Weitergabe von Informationen entscheiden können. Im Gegensatz zur Enterprise-IAM Kategorie sind hier die Anforderungen nach Benutzereinwilligung und benutzerzentrierter Kommunikation unumgänglich.

Die beiden Szenarien werden vielfach in parallelen Infrastrukturen und nicht auf einer gemeinsamen Plattform betrieben. In einem Umfeld, in welchem sowohl Enterprise-IAM wie auch Internet-IAM Szenarien abgedeckt werden sollen, muss die Art der Herausgabe eines Attributs steuerbar sein.

Freigabe von persönlichen Informationen

- Der Benutzer muss die Möglichkeit haben, Authentisierungsbestätigungen und persönliche Attribute gegenüber einer anfragenden Relying Party freizugeben.
- Die Form der Freigabe soll vom Benutzer gewählt werden können:
    - Der Benutzer bestätigt pro anfragende Relying Party die Herausgabe von Authentisierungsbestätigungen und persönlichen Attributen jedes Mal erneut.
    - Der Benutzer kann pro anfragende Relying Party das Einverständnis für die Herausgabe einer Authentisierungsbestätigung und eines Sets an Attributen einmalig geben. Danach werden die angeforderten Informationen vom STIAM-Hub automatisch an die RP weitergeleitet, bis sich entweder das Set an Attributen ändert, oder der Benutzer ein erneutes Einverständnis einfordert.

Freigabe von Attributen im Organisationskontext

- Authentisierungsbestätigungen und Attribute eines Subjekts im Organisationskontext können ohne Einwilligung des Subjekts an eine Relying Party übermittelt werden. Sie beschreiben und autorisieren das Subjekt im Zusammenhang mit seiner Tätigkeit in der Organisation.
- Die Herausgabe von Informationen über Mitarbeitende (bzw. Maschinenaccounts) müssen von einer Organisation bzw. einem IdP/AA auf bestimmte Relying Parties eingeschränkt werden können. Damit soll ermöglicht werden, innerhalb von Suisse-TrustIAM Identitäten und Attribute mit spezieller Semantik nur für bestimmte Bereiche zugänglich zu machen.

3.12 Attributmanagement

Attribute müssen in SuisseTrustIAM von allen beteiligten Komponenten eindeutig referenziert werden können. Die Definition/en (Namensgebung, Syntax, Typ) werden/wird auf dem STIAM-Hub zentral abgelegt und verwaltet. Die Prozesse zur Qualifizierung und Administration von Attributen sind nicht Bestandteil dieser Dokumentation. Diese werden in einem separaten Dokument spezifiziert.

4 Anforderungen

4.1 SuisseTrustIAM Vermittlerinfrastruktur

In Tabelle 3 sind die aus Kapitel 3 und dem SuisseTrustIAM Rahmenkonzept [3] resultierenden Anforderungen an die SuisseTrustIAM Vermittlerinfrastruktur zusammengefasst.

Nr.	Bezeichnung	Beschreibung
A1	Identität des Subjekts	Die Feststellung der Identität eines Subjekts wird eindeutig nachgewiesen und mit einer definierten Qualität versehen.
A2	Zuordnung von Attributen	Attribute sind - unabhängig von deren Qualität - immer zu einer bestimmten digitalen Identität zuordnungsbar.
A3	Koordination der Identifikatoren[8]	Die Identifikatoren eines Subjekts sind für alle peripheren Entitäten (Identity Provider, Relying Party und Attribut-Autorität) gegenüber einer lokalen digitalen Identität eindeutig referenzierbar.
A4	Authentizität eines Attributs	Es ist möglich zu überprüfen, wer ein Attribut ausgegeben hat und wann dieses ausgestellt wurde.
A5	Kategorisierung von Attributen	Identitätsinformationen sind zwischen persönlichen und unternehmensbezogenen Inhalten zu unterscheiden.
A6	Schutz der Privatsphäre	Der Benutzer hat die Möglichkeit, die Herausgabe von Attributen zu kontrollieren.
A7	Limitierung der Herausgabe	Es ist möglich, die Sichtbarkeit und Herausgabe eines Attributs für einen bestimmten Kreis von Konsumenten (Relying Parties) einzugrenzen.
A8	Aussagekraft eines Attributs	Unabhängig der jeweiligen Herkunft ist überprüfbar, welche Aussagekraft ein bestimmtes Attribut hat. Ein Attribut verfügt daher über einen Qualitätswert, welcher Auskunft über die erfolgte Prüfung des Inhalts gibt.
A9	Blacklisting von Attributen und Attributlieferanten	Um in Bezug auf die Qualität von Attributen verbindlich überprüfbare Vertrauensverhältnisse aufbauen zu können, sind Verfahren zum Sperren eines Attributs bzw. eines Attributlieferanten notwendig.
A10	Aufbau von Vertrauensbeziehungen	Alle beteiligten Parteien (Identity Provider, Attribut-Autorität, Relying Party und STIAM-Hub) haben die Möglichkeit, die Kommunikation mit ihrem Partner und die Nachrichteninhalte vertrauenswürdig zu verifizieren.

[8] Die in A15 aufgeführte Anonymisierung der Identität steht nicht im Widerspruch zu A3, da es sich hier nicht um eine globale Identität handelt, sondern um lokal referenzierbare Identitäten.

Nr.	Bezeichnung	Beschreibung
A11	Vertraulichkeit von Attributinhalten	Es wird sichergestellt, dass Nachrichteninhalte vertraulich übermittelt werden können.[9]
A12	Minimale Auskunft	Es wird sichergestellt, dass eine anfragende Partei nur die für sie notwendigen (registrierten) Informationen abfragen und erhalten kann.[10]
A13	Zuständigkeit der Quelle	Es wird sichergestellt, dass ein Attributlieferant nur Identitäts-informationen ausstellen kann, für welche er zuständig ist.[10]
A14	Nachvollziehbarkeit	Es ist möglich einen Authentisierungs- und Attributausgabe-prozess für eine bestimmte Zeit nachvollziehen zu können.
A15	Anonymisierung von Identitäten	Die Identität eines Subjekts wird gegenüber den beteiligten Parteien anonymisiert (siehe dazu Fussnote 8 auf Seite 29).
A16	Attributsyntax	Die Syntax eines Attributs wird für alle beteiligten Parteien eindeutig definiert.
A17	Attributsemantik	Die Semantik eines Attributs wird für alle beteiligten Parteien eindeutig definiert.
A18	Administration	Organisationen haben die Möglichkeit, ihre Mitarbeitenden, ihre angebotenen Dienste und ihre Ressourcen einfach und selbstständig zu administrieren.
A19	Step-up Authentifizierung	Ein durch einen Informationskonsumenten während einer Session angeforderter höherer Authentifizierungsgrad führt zu einer erneuten Authentifizierung des Subjekts.
A20	Überprüfung der Au-thentifizierung	Ein Attributlieferant hat die Möglichkeit die erfolgte Authentifi-zierung eines Subjekts selbst zu überprüfen.
A21	Single Logout	Ein Subjekt kann über die Relying Party (bzw. über deren Anwendung) die laufenden Sessions auf anderen RPs durch den STIAM-Hub terminieren lassen.
A22	Login Session Hand-ling	Ein Subjekt bleibt nach erfolgter Authentisierung durch einen IdP auf dem STIAM-Hub authentifiziert. Eine Anfrage nach weiteren Attributen (auch durch eine andere Relying Party) ist ohne erneute Authentifizierung des Subjekts möglich, so-lange diese Nachfrage kein höherer Authentication-Level er-fordert. Wenn die Anfrage einer RP ein höheres Authenticati-

[9] Attribute können sensitive Informationen beinhalten und müssen deshalb nur einem be-rechtigten Konsumenten (Relying Party) in vertraulicher Form zugänglich gemacht werden können.

[10] Diese Anforderung ist Teil der Governance und muss durch die Gestaltung entsprechen-der Prozesse gewährleistet werden.

Nr.	Bezeichnung	Beschreibung
		on-Level erfordert, so kommt A19 zum Zug.

Tabelle 3: Anforderungen an SuisseTrustIAM Vermittlerinfrastruktur

4.2 STIAM-Empfänger

Die STIAM-Empfänger (Relying Party) definieren pro Ressource bestimmte Vorgaben bezüglich Authentifizierungsgrad des Benutzers und Qualität eines geforderten Attributs in ihren Metadaten. Die vom STIAM-Hub erhaltenen Antworten können sie gemäss ihren eigenen Richtlinien entsprechend validieren:

Funktion	Beschreibung
RP-01	Der STIAM-Empfänger MUSS die Authentifizierung des Subjekts an den STIAM-Hub als vertrauenswürdige Instanz delegieren.
RP-02	Der STIAM-Empfänger KANN zur Definitionszeit einen bestimmten Identity Provider vorwählen.
RP-03	Der STIAM-Empfänger MUSS in Abhängigkeit der zu kontrollierenden Ressource die Qualitätsstufe der Identität (QAA-Level) vorgeben.
RP-04	Der STIAM-Empfänger KANN die durch einen Identity Provider ausgestellten Security Token selbst validieren, wenn der STIAM-Hub den Identity Relaying Modus unterstützt (HUB-LZ-11).
RP-05	Der STIAM-Empfänger KANN die Überprüfung der Attribute Assertions an den STIAM-Hub als vertrauenswürdige Instanz delegieren.
RP-06	Der STIAM-Empfänger KANN zur Definitionszeit die Qualitätsstufe eines für ihn erforderlichen Attributs vorgeben.
RP-07	Der STIAM-Empfänger MUSS eines der in Kapitel 3.5 beschriebenen und vom STIAM-Hub unterstützten STIAM-Kommunikationsprotokolle unterstützen.
RP-08	Der STIAM-Empfänger KANN die durch eine zuständige Attribut-Autorität ausgestellte Attribute Assertions selbst validieren, wenn der STIAM-Hub den Identity Relaying Modus unterstützt (HUB-LZ-11).
RP-09	Der STIAM-Empfänger SOLLTE SSO-Sessions unterstützen, wenn Single Logout (SLO) unterstützt werden soll (vgl. Kapitel 5.5).
RP-10	Wenn STIAM-Empfänger ein verschlüsseltes Attribut von einem STIAM-Sender, der Verschlüsselung unterstützt anfordert (AA-LZ-02), MUSS er auch in der Lage sein dieses korrekt zu verarbeiten.

4.3 STIAM-IdP

Ein STIAM-IdP hat in SuisseTrustIAM die Funktion, ein Subjekt zu authentifizieren. Es kann sich dabei um einen kommerziellen IdP handeln oder um einen SuisseTrustIAM integrierten IdP/AA einer Organisation. Mit welchen Authentifizierungsmitteln und Credentials ein IdP das Subjekt authentifiziert, ist nicht Teil der SuisseTrustIAM Standardisierung. Damit die Registrierung und Authentifizierung eines Subjekts für alle Entitäten der SuisseTrustIAM Plattform transparent prüfbar ist, sind durch die Identity Provider bestimmte Informationen zur Qualität der erfolgten Benutzeridentifizierung und Authentifizierungsmethode entsprechend dem Qualitätsmodell aus dem eCH-Standard eCH-0170 [4] anzugeben.

Funktion	Beschreibung
IDP-01	Der STIAM-IdP MUSS eines der in Kapitel 3.5 beschriebenen und vom STIAM-Hub angebotenen Kommunikationsprotokolle unterstützen.
IDP-02	Der STIAM-IdP MUSS die durch eine Relying Party angefragten Authentifizierungsinformationen in fälschungssicherer Form (digital signiert) zurücksenden.
IDP-03	Der STIAM-IdP MUSS als Teil seines Authentifizierungsstatements einen ihm bekannten - pro Subjekt eindeutigen - Identifikator zurücksenden.
IDP-04	Der STIAM-IdP SOLLTE die Qualitätsstufe der Benutzeridentifizierung und der Authentifizierungsmethode in standardisierter Form als Teil seines Authentifizierungsstatements (Nachweis) angeben.
IDP-05	Der STIAM-IdP MUSS das Linking Protokoll zur Registrierung durch den Benutzer unterstützen (vgl. Kapitel 6.1).
IDP-06	Der STIAM-IdP MUSS gegenüber dem STIAM-Hub immer eine Persistent ID verwenden.

4.4 STIAM-Sender

Der STIAM-Sender (Attribut-Autorität) stellt Attribute nach Eingang einer Anfrage für ein bestimmtes Subjekt aus. Eine Attribut-Autorität stellt nur Attribute aus, für welche sie autoritative Quelle ist. In dieser Funktion hat sie bestimmte Vorgaben zu erfüllen, hat aber auch die Möglichkeit, Bedingungen an die Ausstellung eines Attributs zu knüpfen.

Funktionen zur Laufzeit:

Funktion	Beschreibung
AA-LZ-01	Der STIAM-Sender KANN die durch den Identity Provider ausgestellten Security Token selbst validieren, wenn der STIAM-Hub den Identity Relaying Modus unterstützt (HUB-LZ-11).
AA-LZ-02	Der STIAM-Sender KANN ein angefordertes Attribut mit dessen Inhalt für einen bestimmten Empfänger verschlüsseln.

Funktion	Beschreibung
AA-LZ-03	Der STIAM-Sender MUSS gegenüber dem STIAM-Hub pro Subjekt einen eindeutigen Identifikator führen.
AA-LZ-04	Der STIAM-Sender MUSS die vom STIAM-Hub gelieferte Identität der anfragenden Relying Party interpretieren und auf die intern verwendete Identität abbilden.
AA-LZ-05	Der STIAM-Sender MUSS eines der Verfahren zur Identitäts- und Attributvermittlung (Proxying Kapitel 3.3.1, Identitätsübergabe Kapitel 3.3.2) unterstützen.
AA-LZ-06	Der STIAM-Sender MUSS die durch den STIAM-Hub angefragten Attributinformationen in fälschungssicherer Form (digital signiert) zurücksenden.
AA-LZ-07	Der STIAM-Sender MUSS eines der in Kapitel 3.5 beschriebenen und vom Hub angebotenen Kommunikationsprotokolle unterstützen.
AA-LZ-08	Der STIAM-Sender MUSS prüfen können, ob der STIAM-Hub berechtigt ist, die angefragten Attribute abzufragen.
AA-LZ-09	Der STIAM-Sender KANN einen vom STIAM-Hub unabhängigen „User Consent“ ermöglichen[11].
AA-LZ-10	Der STIAM-Sender MUSS das Linking Protokoll zur Registrierung durch den Benutzer unterstützen (vgl. Kapitel 6.1).
AA-LZ-11	Der STIAM-Sender MUSS die vom STIAM-Hub angefragten Attribute interpretieren und auf die intern verwendeten Attribute abbilden.
AA-LZ-12	Der STIAM-Sender MUSS die Identitäten, für die er Attribute bereitstellt, und deren Attribute verwalten.
AA-LZ-13	Der STIAM-Sender SOLLTE eine Funktionalität zum Ein-/Ausschliessen der von ihm verwalteten Identitäten an der Identity-Federation bereitstellen (User Filtering).

Funktionen zur Definitionszeit:

Die folgenden Funktionalitäten gehören zur Administration des STIAM-Senders und werden zur Definitionszeit festgelegt (siehe Kapitel 7.5.4.4).

Funktion	Beschreibung
AA-DZ-01	Der STIAM-Sender MUSS eine Qualitätsstufe zur Identifizierung des Subjekts (QAA-Level aus [4]) für die Ausgabe eines bestimmten Attributs angeben.

[11] Aus Gründen der Benutzerfreundlichkeit sollte möglichst nur einmal die Zustimmung des Benutzers eingeholt werden.

Funktion	Beschreibung
AA-DZ-02	Der STIAM-Sender KANN für die Ausgabe eines Attributs einen bestimmten Identity Provider vorgeben.
AA-DZ-03	Der STIAM-Sender KANN selbst nochmals die Authentifizierung des Subjekts veranlassen.
AA-DZ-04	Der STIAM-Sender MUSS für ein von ihm bereitgestelltes Attribut eine Qualitätsstufe entsprechend eCH-0171 [5] angeben.
AA-DZ-05	Der STIAM-Sender KANN die Verwendung eines Attributs für einen bestimmten Kreis von Lösungsanbietern (Bereich) eingrenzen.

4.5 STIAM-Hub

Der STIAM-Hub in SuisseTrustIAM deckt mehrere Funktionen der IAM Geschäftsservices ab. Zur Laufzeit agiert er als *STIAM-Hub* und vermittelt zwischen den Entitäten. Zur Definitionszeit deckt er die Funktion eines *Trust*- und *eIdentity-Services* ab, indem sich Subjekte und Organisationen auf dem STIAM-Hub registrieren können.

Trust- und *eIdentity Services* sind administrative Prozesse als Teil des Benutzer- und Organisationsmanagements und werden hier in der Funktionsbeschreibung nur grob aufgeführt. Eine detailliertere Beschreibung der Funktionen ist in der SuisseTrustIAM Geschäftsarchitektur eCH-0169 [19] zu finden.

Funktionen zur Laufzeit:

Funktion	Beschreibung
HUB-LZ-01	Der STIAM-Hub MUSS einen zentralen Discovery Service führen.
HUB-LZ-02	Der STIAM-Hub MUSS dem Subjekt in Abhängigkeit des geforderten QAA-Levels eine Liste möglicher Identity Provider zur Auswahl geben.
HUB-LZ-03	Der STIAM-Hub MUSS eines der in Kapitel 3.5 beschriebenen Kommunikationsprotokolle unterstützen.
HUB-LZ-04	Der STIAM-Hub MUSS zur Laufzeit für anfragende Relying Parties die Funktion eines Authentisierungsproxys übernehmen.
HUB-LZ-05	Der STIAM-Hub MUSS die Authentizität der Attribute Assertions prüfen.
HUB-LZ-06	Der STIAM-Hub MUSS zur Laufzeit für anfragende Relying Parties die Funktion eines Attributaggregators übernehmen.
HUB-LZ-07	Der STIAM-Hub SOLLTE Proxying als Verfahren zur Identitäts- und Attributvermittlung unterstützen (vgl. Kapitel 3.3.1).
HUB-LZ-08	Der STIAM-Hub MUSS die Identitätsübergabe als Verfahren zur Identitäts- und Attributvermittlung unterstützen (vgl. Kapitel 3.3.2**)**.

Funktion	Beschreibung
HUB-LZ-09	Der STIAM-Hub MUSS die durch eine Relying Party angefragten Authentifizierungs- und Attributinformationen in fälschungssicherer Form (digital signiert) zurücksenden.
HUB-LZ-10	Der STIAM-Hub MUSS den in Kapitel 3.4.1 beschriebenen Identity Proxy Mode unterstützen.
HUB-LZ-11	Der STIAM-Hub SOLLTE den in Kapitel 3.4.2 beschriebenen Identity Relaying Mode unterstützen.
HUB-LZ-12	Der STIAM-Hub MUSS im Rahmen der Attributvermittlung die Möglichkeit bieten, das Einverständnis des Subjekts (User Consent) zur Herausgabe von einzelnen Attributen einzuholen.[12]
HUB-LZ-13	Der STIAM-Hub MUSS als Authentisierungsproxy ein eigenes Session Handling für authentifizierte Benutzer unterhalten.
HUB-LZ-14	Der STIAM-Hub MUSS in der Lage sein, die Identität der anfragenden Relying Party an die Attribut-Autorität weiterzuleiten.
HUB-LZ-15	Der STIAM-Hub SOLLTE anonymisierte RP-spezifische Identifikatoren (Persistent ID) unterstützen.
HUB-LZ-16	Der STIAM-Hub MUSS anonymisierte zufällige Identifikatoren (Transient ID) unterstützen.
HUB-LZ-17	Der STIAM-Hub MUSS alle Kommunikationsvorgänge im Rahmen der Authentisierungs- und Attributvermittlung loggen.
HUB-LZ-18	Der STIAM-Hub MUSS seine Identitäten verwalten.

Funktionen zur Definitionszeit:

Funktion	Beschreibung
HUB-DEF-01	Der STIAM-Hub MUSS einen Linking Service zur Verwaltung der Subjekte zur Verfügung stellen.
HUB-DEF-02	Der STIAM-Hub MUSS einen Dienst zur Verwaltung der Organisationen und deren Entitäten zur Verfügung stellen.
HUB-DEF-03	Der STIAM-Hub MUSS die erfassten Entitäten einer Organisation in Form von Metadaten aggregieren.

[12] Bei der Definition der angebotenen Attribute (Kapitel 7.5.4.4) wird festgelegt, ob ein User Consent für ein Attribut notwendig ist bzw. ob der STIAM-Hub oder der STIAM-Sender diesen einholt.

Funktion	Beschreibung
HUB-DEF-04	Der STIAM-Hub MUSS die aggregierten Metadaten fälschungssicher publizieren.
HUB-DEF-05	Der STIAM-Hub MUSS einen Dienst zum Attributmanagement zur Verfügung stellen.
HUB-DEF-06	Der STIAM-Hub MUSS alle administrativen Prozesse zur Organisations- und Subjektverwaltung loggen.

5 Protokolle zur Laufzeit

5.1 Authentisierung und Attributaggregation

Die in SuisseTrustIAM zur Anwendung kommenden Authentifizierungs- und Attributaggregationsverfahren werden in diesem Kapitel näher beschrieben. Wie in Kapitel 3.3 bereits erwähnt, sind dazu zwei unterschiedliche Verfahren möglich. Stellvertretend für den Authentisierungs- und Attributaggregationsprozess wird das direkte Verfahren mittels Identitätsübergabe (vgl. Kapitel 3.3.2) auf den folgenden Seiten detailliert dargestellt und beschrieben.

In diesem Verfahren übermittelt der STIAM-Hub (15) einem STIAM-Sender (Attribut-Autorität) die Identität des Subjekts im Vorfeld der unmittelbar darauf folgenden Attributabfrage (16). Dieser Lösungsansatz ermöglicht es, eine parallele Abfrage von Attributen bei Attribut-Autoritäten mit unterschiedlichen Identifikatoren zu machen. In Abbildung 7 ist das komplette Verfahren in einem Sequenzdiagramm festgehalten.

Der Benutzer (Subjekt) greift mit seinem Browser auf eine Applikation (Ressource) eines STIAM-Empfängers (Relying Party) zu. Der Zugang auf die Ressource wird durch eine Zugangskontrolle gesteuert. Das Subjekt wird zwecks Authentifizierung und Bestätigung von Attributen zum STIAM-Hub weitergeleitet. Der STIAM-Hub lässt das Subjekt beim entsprechenden IdP authentifizieren und holt die angeforderten Attribute bei den zuständigen Quellen ein. Der STIAM-Hub aggregiert sowohl die *Authentication Statements* wie auch die *Attribute Statements* zu einer eigenen Assertion und sendet diese an die Relying Party (STIAM-Empfänger) zurück.

Auf eine detaillierte Darstellung des zweiten Verfahrens mittels Proxying (vgl. Kapitel 3.3.1) wird an dieser Stelle verzichtet, da SAML-Proxying in der SAML-Core Standardisierung [20] genau spezifiziert wird und entsprechend auf andere Protokolle übertragbar ist.

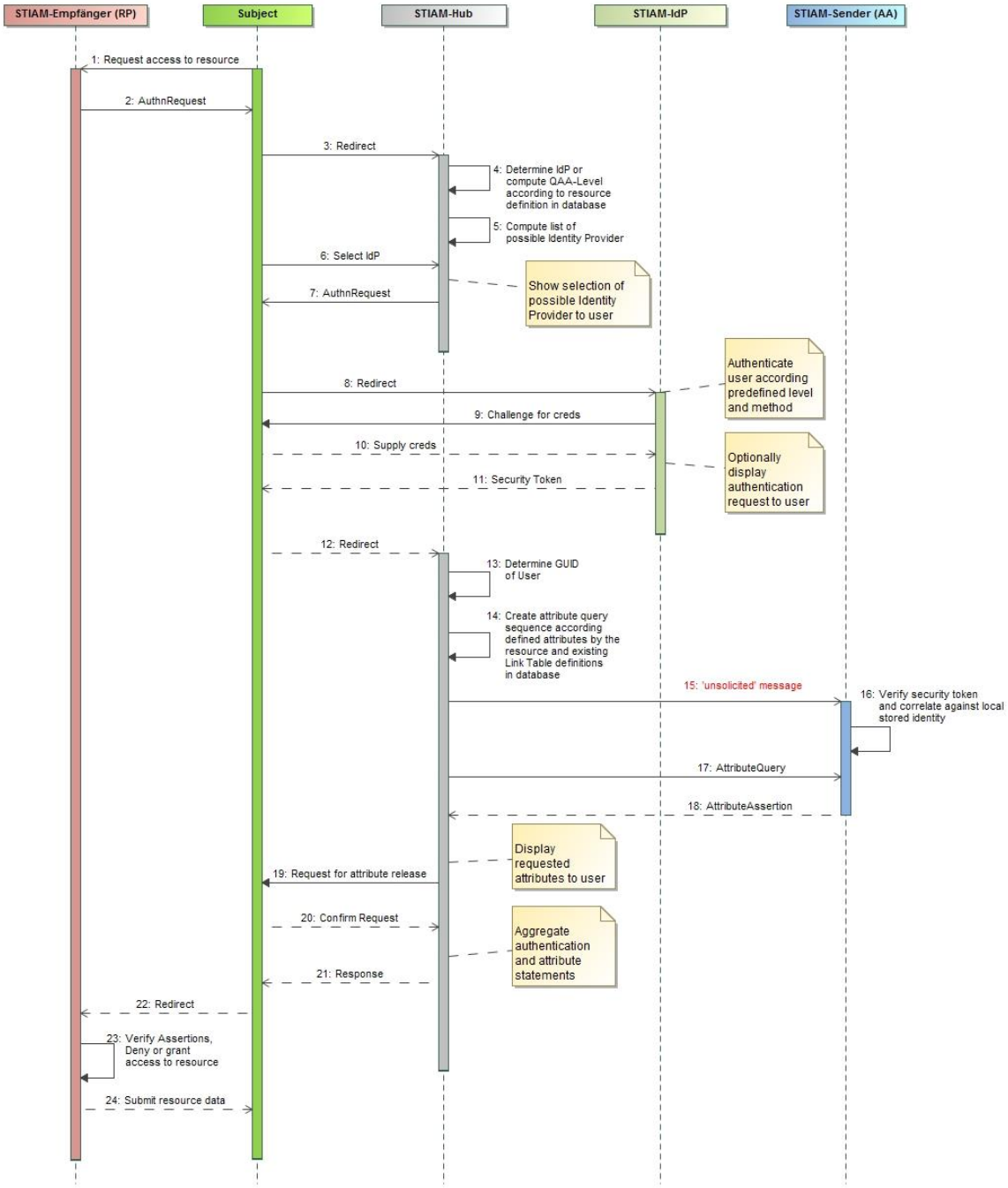


Abbildung 7: Direktes Attributaggregationsverfahren

Beschreibung zu Abbildung 7:

Schritt	Bemerkung
2	• Der STIAM-Empfänger (RP) sendet einen digital signierten *Authentication Request* mit Angaben zur Ressource, auf die der Benutzer zugreifen will, zum Browser des Benutzers.
3	• Der Browser leitet den *Authentication Request* weiter zum STIAM-Hub (Redirect).
4	• Der STIAM-Hub identifiziert den STIAM-Empfänger (RP-ID) und die ge-

Schritt	Bemerkung
	wünschte Ressource (RES-ID) aus Informationen des *Authentication Requests* in seiner Datenbasis. • Der STIAM-Hub muss die Signatur des STIAM-Empfängers (RP) verifizieren.
5	• Der STIAM-Hub stellt anhand der *Ressourcen Definition* in seiner Datenbasis eine Liste von möglichen Authentifizierungsdiensten (IdPs) zusammen. Dabei sind je nach *Ressourcen Definition* folgende Szenarien möglich: a) Die Ressource hat einen (oder mehrere) IdPs (*IdP-ID*) vorgegeben. Der STIAM-Hub zeigt auf seiner Webseite dem Benutzer die vordefinierten IdPs zur Wahl an. b) Die Ressource hat ein (oder mehrere) angebotenes Attribut (*Attr-ID*) definiert. Der STIAM-Hub bestimmt anhand der *Attr-ID* den darin verlangten QAA-Level. Anhand des höchsten QAA-Levels aller angeforderten Attribute zeigt der STIAM-Hub dem Benutzer eine Liste der [zur Abfrage bei entsprechenden Attribut-Autoritäten] in Frage kommenden IdPs an. Optional können in der *Attr-ID* auch direkt ein oder mehrere IdPs (*IdP-ID*) vorgegeben sein. In diesem Fall verfährt der Hub wie in Punkt a. c) Die Ressource hat einen erwünschten Authentifizierungslevel (QAA-Level) vorgegeben. Anhand dieses Werts stellt der STIAM-Hub eine Liste der in Frage kommenden IdPs zusammen und gibt diese dem Benutzer zur Auswahl. • Der STIAM-Hub sucht in seiner Datenbasis Attribut-Autoritäten (*AA-ID*), welche ein angefordertes Attribut zur Verfügung stellen können. Die zuvor ermittelten QAA-Levels bzw. IdPs werden gegen die QAA-Level-Anforderungen der Attribut-Autoritäten geprüft. Erkennt der STIAM-Hub einen Attributlieferanten, welcher für die Auslieferung eines bestimmten Attributs einen höheren QAA-Level fordert als bisher ermittelt, so muss der STIAM-Hub den QAA-Level anpassen und die Liste möglicher IdPs entsprechend korrigieren.
6	• Der Benutzer wählt anhand der (in Punkt 5 evaluierten) zur Auswahl stehenden Authentifizierungsdienste einen IdP aus.
7	• Der STIAM-Hub erstellt einen *Authentication Request* zuhanden des ausgewählten IdPs und sendet diesen zurück zum Browser.
8	• Der Browser leitet den *Authentication Request* zum Authentifizierungsdienst des gewählten IdPs weiter.
9	• Der IdP fordert den Benutzer zur Authentisierung auf (Username/Password, PKI basierend, etc.)
10	• Der Benutzer authentisiert sich gegenüber dem IdP.
11	• Der IdP authentifiziert den Benutzer und sendet ihm ein digital signiertes Security Token zurück. • Optional kann der IdP das Einverständnis vom Benutzer einholen, das

Schritt	Bemerkung
	Security Token an den anfragenden STIAM-Hub auszuliefern.
12	• Der Browser leitet das Security Token des IdPs zum STIAM-Hub weiter.
13	• Der STIAM-Hub kann anhand von Information aus dem Security Token die GUID des Benutzers in der Link Table im User Identifier Repository (UIR) bestimmen. Ist der Identifikator aus dem Security Token mit mehr als einer GUID verbunden, so muss der STIAM-Hub dem Benutzer übereinstimmende Accounts zur Auswahl vorlegen.[13]
14	• Der STIAM-Hub stellt in Abhängigkeit der in der Ressource geforderten Attribute eine *Attribute Query Sequence*[14] zusammen. Dabei muss er folgende Kriterien berücksichtigen: a) Die Ressource hat ein (oder mehrere) angebotenes Attribut (*Attr-ID*) definiert. Der STIAM-Hub bestimmt anhand der *Attr-ID* die *AA-ID* und überprüft, ob der Benutzer in seiner Link Table über einen entsprechenden AA-Link verfügt. b) Die Ressource hat ein (oder mehrere) Attribut mit einer Attributqualität (*Attr-Quality*) definiert. Der STIAM-Hub sucht in der Datenbasis nach Attribut-Autoritäten (*AA-ID*), welche das Attribut in der geforderten Qualität zur Verfügung stellen können und überprüft, ob der Benutzer in seiner Link Table über einen entsprechenden AA-Link verfügt. c) Die Ressource hat nur ein (oder mehrere) Attribut (*OID*) definiert. Der STIAM-Hub sucht in der Datenbasis nach Attribut-Autoritäten (*AA-ID*), welche das Attribut anbieten und überprüft, ob der Benutzer in seiner Link Table über den entsprechenden AA-Link verfügt. • Falls der Benutzer nicht über einen notwendigen AA-Link verfügt und das in der Ressource Definition angegebene Attribut als *required* bezeichnet ist, muss der STIAM-Hub dem Benutzer eine entsprechende Fehlermeldung anzeigen. • Hat der Benutzer mehrere AA-Links zu einem Attribut definiert, so muss der STIAM-Hub dem Benutzer die in Frage kommenden Attribut-Autoritäten zur Auswahl anzeigen.
15	• Der STIAM-Hub sendet eine unaufgeforderte, digital signierte Nachricht (*unsolicited message*) direkt[15] an den STIAM-Sender (AA).

[13] Es soll möglich sein, dass ein User mehrere Accounts in SuisseTrustIAM führen und in diesen Accounts denselben Identifikator verwenden kann (z.B. in zwei Accounts ein und dieselbe SuisseID mit einer SuisseID-Nr. als Identifikator).

[14] Attribute Query Sequence: Die Liste der AAs, welche Lieferanten der Attribute in geforderter Qualität sind.

[15] Diese Nachricht kann optional auch über den Browser des Benutzers gehen. Der benutzerzentrierte Weg drängt sich aber nur dann auf, wenn die Attribut Authority selbst das Einverständnis zur Herausgabe der Attribute vom Benutzer einfordern will.

Schritt	Bemerkung
	• Diese Nachricht beinhaltet ein Security Token (*Authentication Statement*) und zusätzlich einen von der Attribut-Autorität signierten[16] *AA-Identifier*.
16	• Der STIAM-Sender (AA) muss das vom STIAM-Hub erhaltene Security Token verifizieren und mit dem in seiner Datenbasis definierten *AA-Identifier* des Subjekts verbinden. • Die Attribut-Autorität muss ihre auf dem *AA-Identifier* geleistete Signatur verifizieren.[17]
17	• Der STIAM-Hub sendet einen *Attribute Request* an den Attribute Assertion Service des STIAM-Senders (AA). • Dieser Request beinhaltet die angeforderten Attribute und den unter Schritt 15 gesendete *AA-Identifier*.
18	• Der STIAM-Sender (AA) stellt eine *Attribut Assertion* zusammen, welche die Attribut-Werte enthält, und signiert diese digital.
19	• Der STIAM-Hub holt sich vom Benutzer für die angeforderten Attribute (einzeln oder gesamt) die Freigabe zur Weitergabe (*user consent*) an den STIAM-Empfänger.[18]
20	• Der Benutzer bestätigt die Freigabe der Attribute.
21	• Der STIAM-Hub erstellt eine digital signierte *Assertion,* bestehend aus den *Authentication Assertions* und *Attribute Assertions,* und sendet diese als *Response* an den Browser zurück.
22	• Der Browser leitet die *Response* an den STIAM-Empfänger (RP) weiter.
23	• Der STIAM-Empfänger muss die Signatur der Response verifizieren und kann die Antwort des STIAM-Hubs für den Zugangsentscheid auf die Ressource verwenden.
24	• Der STIAM-Empfänger verwehrt oder gewährt den Zugriff auf die Ressource anhand der Attributinhalte und der lokal definierten Policy.

5.2 Service-to-Service basierte Kommunikation

In Kapitel 3.5 wurde bereits aufgezeigt, welche Art Security Token und welche Protokolle in SuisseTrustIAM verwendet werden. Nebst der SAML 2.0 basierten benutzerzentrierten

[16] Die Attribut Authority signiert den Identifikator im Linking Protokoll (siehe Kapitel 7.1).

[17] Die Attribut Authority kann dadurch gefälschte Identifikatoren ausschliessen.

[18] Es ist auch möglich, dass die AA die Freigabe des Benutzers für ihre Attribute einholt. Dazu muss die Kommunikation zur Attributabfrage (Schritt 16 und 17) zwischen STIAM-Hub und STIAM-Sender über den Browser des Benutzers umgeleitet werden. Allerdings ist die zentrale Freigabe am STIAM-Hub meist benutzerfreundlicher.

Kommunikation sollen auch Webservices als *Requestor* eingebunden werden können. Dazu muss der STIAM-Hub auf Seite Relying Party WS-* Funktionalitäten nach WS-Trust [14] bzw. WS-Federation [12] unterstützen.

Die Art der ausgestellten Token sind auch für Webservices SAML Assertions, wie sie für die benutzerzentrierte Kommunikation verwendet werden.

Die Verfahren zur Einbindung von WS-Trust mit der STIAM-Hub Funktion verläuft ähnlich wie in Kapitel 5.1 Authentisierung und Attributaggregation beschrieben. Der STIAM-Hub agiert als vermittelnder Security Token Service (STS) der Ressource (RP). Der IdP/AA ist der STS des Requestors, bei welchem sich der Webservice authentisieren muss. Der Protokollablauf zur Laufzeit kann auf verschiedene Arten umgesetzt werden. Im Rahmen dieser technischen Architektur wird auf die möglichen Szenarien nicht weiter eingegangen.

5.3 Validierung von Identitäts- und Attributinformationen

Zur Definitionszeit kann sowohl eine Relying Party wie auch eine Attribut-Autorität mit der Option *Verify Assertion* gegenüber dem STIAM-Hub signalisieren, dass sie ausgestellte Security Tokens und Attribute Assertions im Original selbst zu validieren wünscht. Dies hat zur Folge, dass der STIAM-Hub in seiner generierten *Response* die aggregierten Token(s) und Assertion(s) in ihrer Originalform mit der Originalsignatur der ausstellenden Instanz einfügen muss (Vergleiche dazu Kapitel 3.4.2).

5.4 Vertraulichkeit von Attributen

Wie in Kapitel 3.8 aufgezeigt, muss die SuisseTrustIAM Infrastruktur die Möglichkeit bieten, Benutzerinformationen zwischen Attribut-Autorität und der anfragenden Relying Party zu verschlüsseln. Da diese beiden Komponenten nur über den STIAM-Hub kommunizieren, kann die Identität der RP nicht direkt dem STIAM-Sender übertragen werden. Dieser benötigt aber diese Identität um den ‚public key' in den Metadaten zu finden, damit er die Attribute Assertion für die anfragende Relying Party verschlüsseln kann.

Daher muss der STIAM-Hub die Identität der RP als Teil des Authentication Requests bzw. der Attributabfrage übermitteln.

5.5 Single Logout (SLO)

Single Logout (SLO) ermöglicht es einem Benutzer in einer STIAM-Domäne, alle laufenden Sessions mit einem ‚Click' zu beenden. Für SuisseTrustIAM ist diese Funktionalität ein wichtiger zusätzlicher Dienst, da ein Benutzer über den STIAM-Hub spielend mehrere Sessions zu unterschiedlichen STIAM-Empfängern (RP) erstellen kann. SLO hilft ihm dabei, diese Sessions sauber und einfach zu beenden.

Damit SLO funktioniert, müssen STIAM-Hub und STIAM-Empfänger für jeden Benutzer eine SSO Session führen. Abbildung 8 zeigt grob das Verfahren auf: Ein Benutzer beendet eine Session auf RP_1. Diese sendet einen entsprechenden *LogoutRequest* zum STIAM-Hub, welcher diesen validiert und auf Grund der *NameID* und des *SessionIndex* alle zu diesem Index gehörenden laufenden Sessions auf anderen RP beenden lässt.

Der Benutzer muss in Kenntnis darüber sein, dass er sich auf einer Webseite in einer SSO Session befindet und ein Logout zur Beendigung aller weiteren noch laufenden Sessions führt.

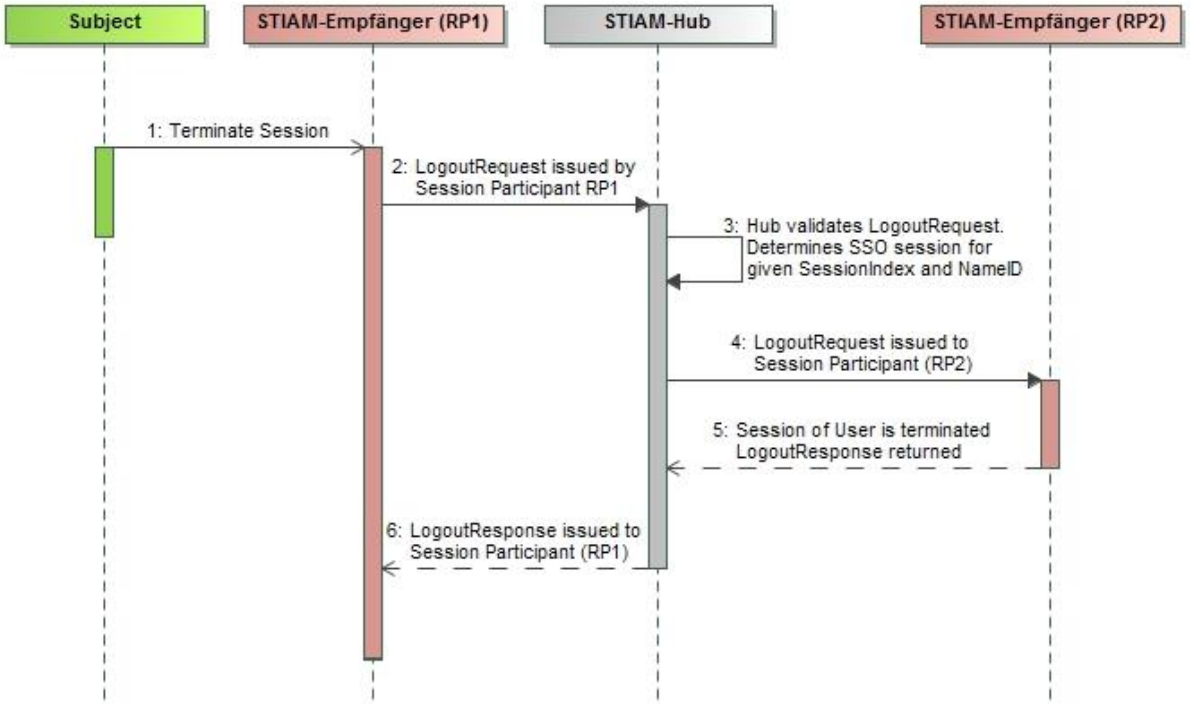


Abbildung 8: Single Logout Verfahren

5.6 Reporting, Logging und Monitoring

Für die SuisseTrustIAM-Infrastruktur besteht die Anforderung, eine Authentisierungs- und Attributvermittlung über eine bestimmte Zeitspanne nachvollziehen zu können. Je nachdem, wo und in welchem Umfang Kommunikationsdaten aufgezeichnet werden müssen, sind verschiedene Ansätze möglich.

Zentrales Logging

Teilfunktion des STIAM-Hubs ist ein Reporting-, Logging und Monitoring Dienst (RLM), welcher alle Kommunikationsvorgänge zur Laufzeit registriert. Dies wirft Datenschutzfragen auf, da die entsprechenden Vorgänge auf Vorrat zentral gespeichert werden. Der STIAM-Hub speichert alle Aktivitäten eines Laufzeitprozesses, die ein Subjekt auslöst, für eine bestimmte Zeit. In Abhängigkeit des verwendeten Verfahrens zur Übermittlung der Identitätsinformationen (vgl. dazu Kapitel 3.4) muss der STIAM-Hub unterschiedliche Daten speichern (vgl. dazu Tabelle 4).

Logging auf peripheren Komponenten

Aus Datenschutzgründen ist es empfehlenswert, Informationen nur dort zu speichern, wo sie anfallen und verwendet werden, also beim STIAM-Empfänger (RP), beim Identity Provider bzw. beim STIAM-Sender (AA). Dies steht aber im Widerspruch zur ebenfalls angestrebten Anonymisierung der vermittelten Identitäten. Das System SuisseTrustIAM geht - je nachdem

wer eine Assertion validiert - davon aus, dass eine Komponente in einem Laufzeitprozess nur genau über ein bestimmtes Set an Informationen zu einer digitalen Identität verfügt.

- Ein STIAM-Empfänger ist in der Regel nicht in Kenntnis aller Identitätsinformationen, welche ein Subjekt eindeutig identifizieren. Damit kann sie nur einen Teil des gesamten Vorgangs protokollieren.
- Der STIAM-IdP wiederum kennt die Identität, nicht aber die Attribute, die aus anderen Quellen vom STIAM-Hub aggregiert werden.
- Ein STIAM-Sender kennt in der Regel nur die Attribute und den (ihm bekannten) Identifikator. Nur der STIAM-Hub ist in Besitz aller Informationen und hat Kenntnis aller Vorgänge während einem Laufzeitprozess.

Aus diesen Überlegungen kann folgende Matrix zum Reporting-, Logging- und Monitoring-Verhalten der einzelnen Komponenten zusammengestellt werden:

	STIAM-Hub	STIAM-Empfänger	STIAM-IdP	STIAM-Sender
Verbindungsdaten	M/L	M/L	M/L	M/L
Vermittlungs-informationen	R/M/L	-	-	-
Attributinhalte	(R/M/L)[19]	L	-	L
Authentisierungs-informationen	R/M	-	L	-
Session-informationen des Subjekts	R/M/L	L	L	L

Tabelle 4: Reporting (R), Logging (L), Monitoring (M)

[19] Der STIAM-Hub muss Attributinhalte aufzeichnen, wenn er im Identity Proxy Mode (IP-Mode) operiert und ein Attribut ‚auditable' gesetzt ist (vgl. dazu Kapitel 7.5.4.4 auf Seite 60).

6 Protokolle zur Definitionszeit

6.1 Linking Protokolle

Man kann zwei Linking Protokolle zur Definitionszeit unterscheiden. Das IdP-Linking-Protokoll wird zwischen dem STIAM-Hub und einem STIAM-IdP verwendet. Es umfasst die Schritte 3 bis 10 des in Abbildung 9 aufgezeigten Prozesses. Das AA-Linking-Protokoll ist in Abbildung 10 aufgezeigt. Es wird zwischen dem STIAM-Hub und einem STIAM-Sender (AA) verwendet.

Vergleiche dazu auch die Prozessbeschreibungen „Verwaltung der IdP/AA-Links“ in Kapitel 7.3.2.

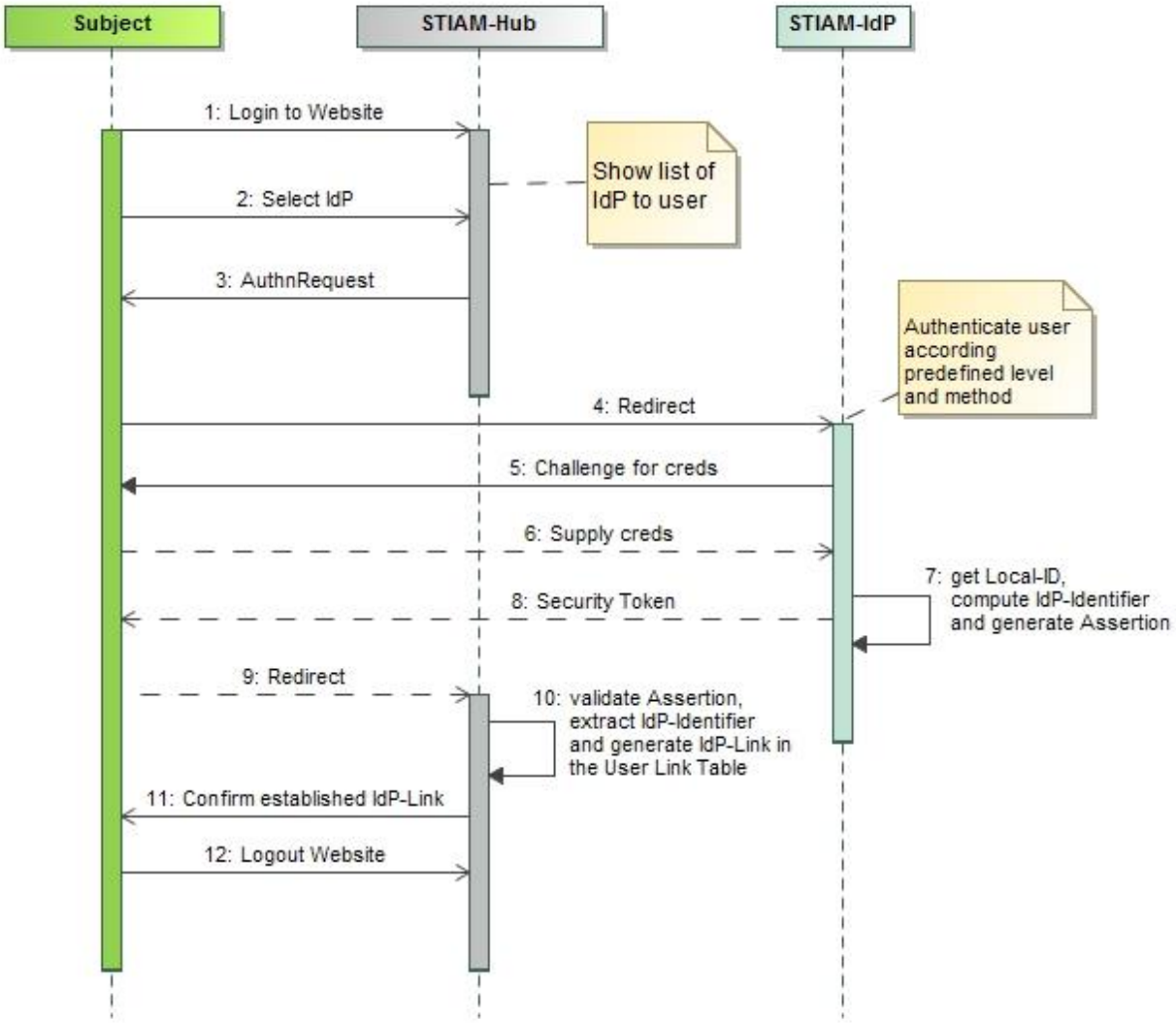


Abbildung 9: IdP-Linking-Protokoll

Beschreibung des IdP-Linking Protokolls

Mit dem IdP-Linking-Protokoll kann ein Benutzer interaktiv einen STIAM-IdP in seiner Link Table erfassen. Der STIAM-Hub gibt auf seiner Webseite einem Benutzer die Möglichkeit, einen möglichen IdP aus einer Liste zu wählen (1-2) und diesen zu verlinken. Der Benutzer wird vom STIAM-Hub auf den Authentication Service des STIAM-IdP weitergeleitet (3-4). Der

Benutzer wird von diesem durch die ihm bekannte und lokal übliche Methode authentifiziert (5-6). Der STIAM-IdP gibt in seiner Assertion einen von ihm berechneten signierten Identifikator des Benutzers an den STIAM-Hub zurück (8-9). Damit kann der STIAM-Hub den erhaltenen Identifikator in der Link Table des Benutzers ablegen (10).

Beim Erstellen und der Pflege der Identity Links muss der Hub sicherstellen, dass sich der Benutzer bei einem oder auch mehreren IdPs authentisiert, um entweder den höchsten QAA-Level der verknüpften Identitäten zu erreichen oder durch mehrfache Authentisierungen mit verschiedenen Credentials eine gleichwertige Sicherheit zu gewährleisten.[20]

Beschreibung des AA-Linking-Protokolls

Mit dem AA-Linking-Protokoll kann ein Benutzer interaktiv einen STIAM-Sender (AA) in seiner Link Table erfassen. Der STIAM-Hub gibt auf seiner Webseite einem Benutzer die Möglichkeit, eine mögliche AA aus einer Liste zu wählen (1-2) und diese zu verlinken. Der STIAM-Hub sendet dazu einen *Authentication Request* zum STIAM-Sender (4). Der STIAM-Sender erfordert eine Authentifizierung des Benutzers und leitet dazu den Authentication Request über den Browser des Benutzers an einen geeigneten IdP (5-10) weiter. Der verwendete IdP kann Teil der AA sein (interner oder lokaler IdP) oder die AA kann einen geeigneten STIAM-IdP verwendet. Der Benutzer wird vom gewählten IdP durch die ihm bekannte und lokal übliche Methode authentifiziert (7-8). Nach erfolgreicher Authentifizierung bestimmt der STIAM-Sender den lokalen Identifikator des Benutzers (11) und übergibt diesen signiert und mit einem Zeitstempel versehen als Security Token über den Browser des Benutzers (12-13) dem STIAM-Hub. Damit kann der STIAM-Hub den erhaltenen Identifikator in der Link Table des Benutzers ablegen (14).

Auch beim Erstellen und der Pflege der Attribute Links muss der Hub sicherstellen, dass sich der Benutzer so bei einem oder auch mehreren IdPs authentisiert, dass eine Qualität der Authentifizierung erreicht wird, die der höchsten Qualität der verknüpften Identitäten oder einer geeigneten Kombination von mehrfachen Authentisierungen mit verschiedenen Credentials mit gleichwertige Sicherheit entspricht.

[20] Zur Lösung des Problems der Ersterstellung der Identity Links kann ein sog. Bootstrap-Account vom STIAM-Hub zur Verfügung gestellt werden, der über eine einfache 2-Faktoren-Authentisierung verfügt. Dieser Account kann nur zu administrativen Zwecken, aber nicht gegenüber einer RP verwendet werden und sollte nach Erstellung des ersten Identity-Links deaktiviert werden. Im Problem-Fall könnte dieser Bootstrap-Account vom Helpdesk reaktiviert werden, um invalide Links zu korrigieren.

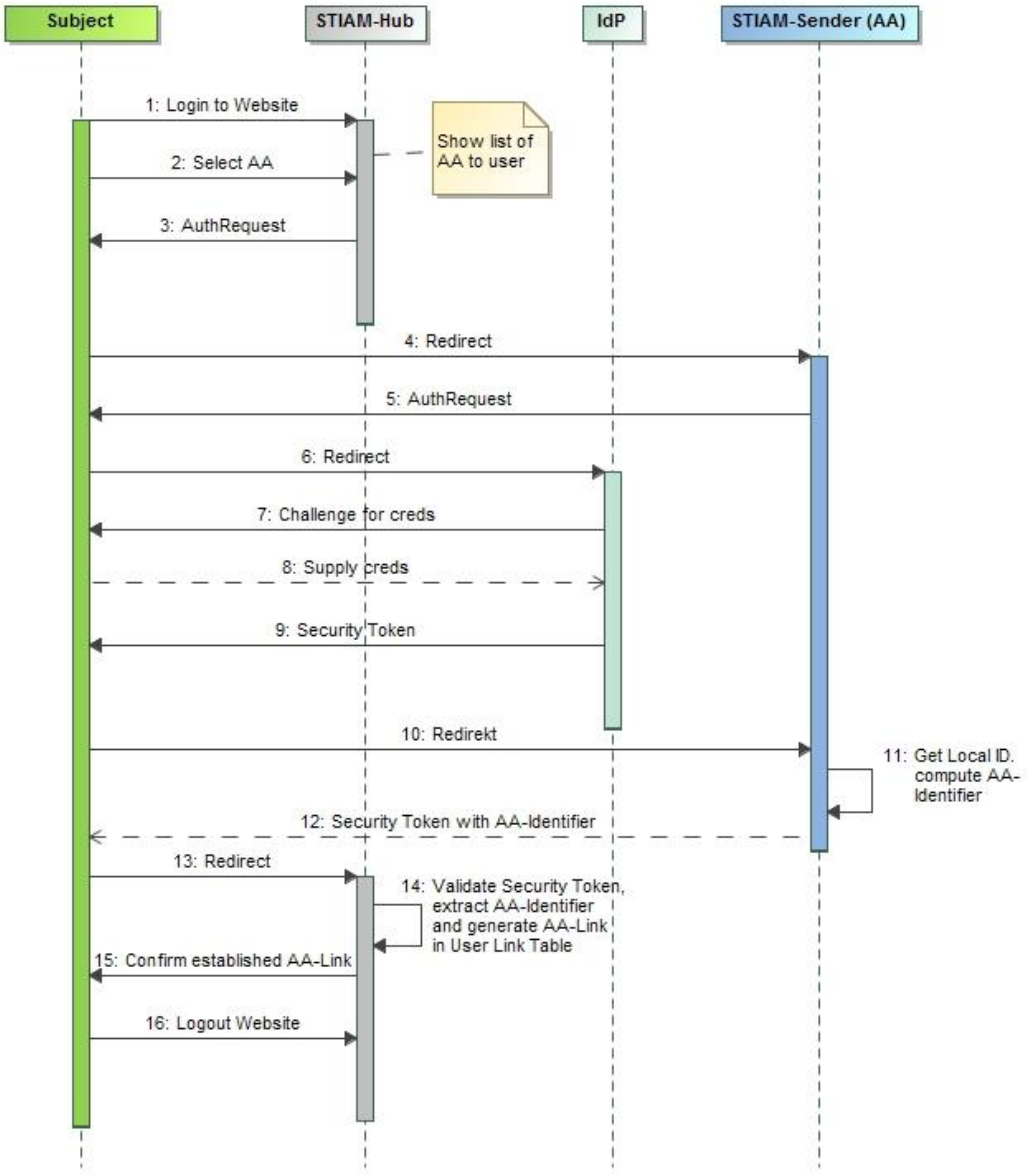


Abbildung 10: AA-Linking-Protokoll

6.2 Metadaten Aggregation und Verteilung

Über das Komponenten Management kann ein Systemverantwortlicher einer Organisation die bereitgestellten Komponenten hinzufügen und konfigurieren. In der Beschreibung der administrativen Prozesse in Kapitel 7 werden die einzelnen Schritte dazu detailliert beschrieben. Diese Informationen werden in der Datenbasis des STIAM-Hubs abgelegt. Für eine Attribut-Autorität können dabei Attribute mit ihren Parametern, Einschränkungen usw. definiert werden. Auf der anderen Seite, können für eine Relying Party - pro Ressource - die Anforderungen (Attribute, QAA-Level, Attribut-Qualität, usw.) festgelegt werden.

Diese Metadaten müssen vom STIAM-Hub aggregiert werden und den STIAM-Komponenten digital signiert zur Verfügung gestellt werden. Dabei erhält ein IdP/AA die Metadaten der STIAM-Empfänger (RPs) und umgekehrt eine RP die Metadaten der IdP/AAs (vergleiche dazu auch die Metadaten Elemente in Abbildung 5 und Abbildung 6).

Da sich in den Metadaten auch die Zertifikate der einzelnen STIAM-Komponenten befinden, können hiermit auch die notwendigen Vertrauensbeziehungen aufgebaut werden.

7 Administrative Prozesse und Datenmodell

Die administrativen Prozesse können in vier Bereiche aufgeteilt werden, welche sich auf der Prozesslandkarte (Abbildung 12) und im Datenmodell (Abbildung 13) wiederfinden. Diese Bereiche widerspiegeln die Hauptfunktionen des STIAM-Hubs auf administrativer Ebene:

1. *Account Management:* Bewirtschaftung der Accountdaten der Subjekte im User Identifier Repository und der Link-Table.
2. *Organisation Management:* Verwaltung der Organisationsdaten und -berechtigungen. Zusätzlich werden hier die verantwortlichen Personen einer Organisation mit ihren Privilegien und Rollen administriert.

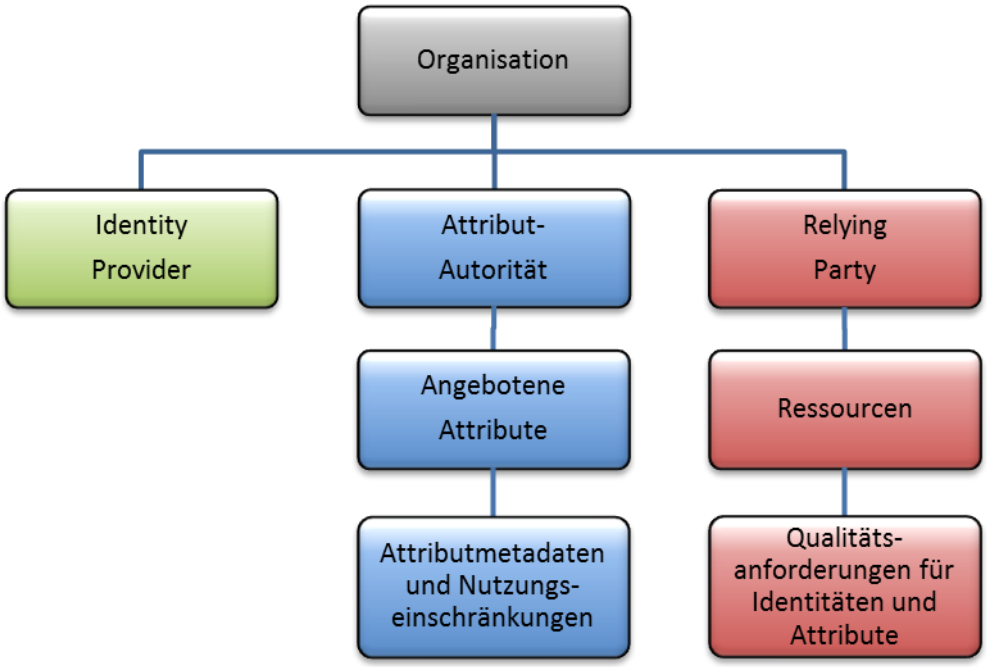


Abbildung 11: Ausprägungen der Organisation

3. *Komponenten Management:* Bewirtschaftung der SuisseTrustIAM Entitäten einer Organisation. Eine Organisation kann verschiedene Entitäten auf der SuisseTrustIAM-Plattform registrieren.
   Die notwendigen Informationen zu diesen Entitäten (Metadaten) werden ebenfalls in der Datenbasis des STIAM-Hubs abgelegt. Diese Informationen werden durch den Systemadministrator der Organisation (siehe OrgSysAdmin in Tabelle 5) erfasst und gepflegt. Eine Attribut-Autorität kann zusätzlich die von ihr angebotenen Attribute auf dem STIAM-Hub definieren, indem sie die entsprechenden Attributmetadaten und ihre Nutzungseinschränkungen erfasst. Auf der anderen Seite kann eine Relying Party in der Datenbasis pro kontrollierte Ressource ihre Anforderungen (Attribute, QAA-Level, Attribut-Qualität, usw.) festlegen.
4. *Attribut Management:* Eine weitere Aufgabe des SuisseTrustIAM STIAM-Hub ist die Definition, Pflege und Bekanntmachung der Attribute, welche in der Community zur

Anwendung gelangen sollen. Deshalb müssen, ebenfalls zentral, alle Attribute definiert werden, so dass diese für die Entitäten in den verschiedenen administrativen Prozessen referenzierbar werden.

In den aufgeführten administrativen Prozessen sind auch Prozesse für STIAM-IdP, -Sender und –Empfänger aufgeführt, soweit sie in Interaktion mit dem STIAM-Hub stattfinden. Alle weiteren administrativen internen Prozesse dieser Komponenten (lokales UserManagement, User Filtering, Mapping von Identitäten und Attributen) werden in diesem Dokument nicht behandelt.

In den nachfolgend dargestellten Prozessen sind neben dem Benutzer selbst, im Sinne einer natürlichen Person, drei spezifische Rollen zu unterscheiden. Diese werden in der Tabelle 5 summarisch aufgeführt und kurz beschrieben. Für eine detaillierte Beschreibung der Rollen sowie ihrer Aufgaben, Kompetenzen und Verantwortungen sei hier auch auf das Dokument eCH-0169 ‚SuisseTrustIAM Geschäftsarchitektur' verwiesen.

Rolle	Beschreibung
SuisseTrustIAM Systemadministrator (STIAM-SysAdmin)	Der STIAM-SysAdmin ist eine Rolle des Betreibers des STIAM-Hubs. Dieser übernimmt vor allem administrative Aufgaben im Rahmen des Organisation Managements bei der initialen Erstellung von Organisationen sowie der Erfassung entsprechender Informationen.
Organisationsverantwortlicher (OV)	Jeder Organisation muss vom STIAM-SysAdmin ein OV zugeordnet werden. Dieser erfasst und pflegt die spezifischen Organisationsinformationen und delegiert administrative Aufgaben im Zusammenhang mit den einzelnen Komponenten an einen oder mehrere OrgSysAdmin. Der OV erfüllt ausserdem eine Kontrollfunktion gegenüber dem OrgSysAdmin.
Systemadministrator einer Organisation (OrgSysAdmin)	Jeder Organisation wird vom zuständigen OV mindestens ein OrgSysAdmin zugeordnet. Dieser erfüllt im Rahmen des Komponenten Managements verschiedene Aufgaben im Zusammenhang mit der Verwaltung von Komponenten, Ressourcen und Attributen.

Tabelle 5: Beschreibung der Rollen innerhalb der administrativen Prozesse

7.1 Übersicht Prozesslandkarte

Wie einleitend bereits beschrieben, gliedert sich die Prozesslandkarte der administrativen Prozesse nach den vier sich auch im Datenmodell wiederfindenden Bereichen *Account Management*, *Organisation Management*, *Komponenten Management* und *Attribut Management*. Diesen werden die einzelnen administrativen Prozesse zugeordnet.

Als zusätzlichen Bereich findet sich auf der Prozesslandkarte das Trust Management. Dieses wird in der Grafik der Vollständigkeit halber dargestellt. Das Trust Management ist einerseits in Form von administrativen Teilprozessen in den anderen Hauptbereichen enthalten und

andererseits Bestandteil der Governance. So sind beispielsweise die Definition der Komponenten, die Aggregation und vertrauenswürdige Verteilung der Metadaten, die Festlegung einer gemeinsamen Zertifizierungsstelle als Vertrauensanker, sowie das zentrale Attributmanagement wichtige Teilprozesse des Trust Managements.

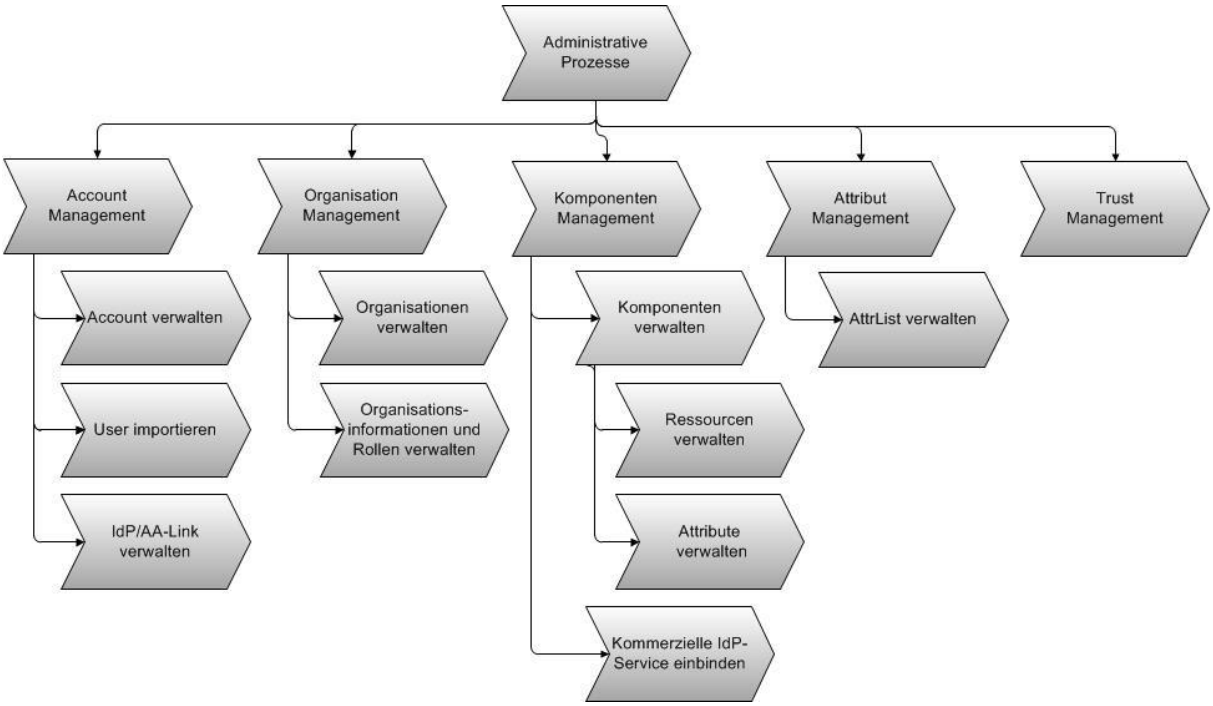


Abbildung 12: Prozesslandkarte administrativer Prozesse des STIAM-Hubs

Die einzelnen Prozesse und ihr Zusammenhang zum Datenmodell werden in den nachfolgenden Unterkapiteln ausführlich beschrieben. Es wird darauf hingewiesen, dass zwei Prozesse im Rahmen dieses Dokuments nicht weiter ausgeführt werden. Dabei handelt es sich einerseits im Komponenten Management um den Prozess "kommerziellen IdP-Service einbinden". Die Integration kommerzieller IdP-Services muss im Einzelfall betrachtet werden und eignet sich aktuell nicht für die Beschreibung von standardisierten Prozessabläufen. Ausserdem ist deren Umsetzung abhängig von Entscheidungen auf Stufe Steuerungsgremien.

Des Weiteren wird auch explizit nicht auf den Prozess "Attribute Liste verwalten" im Attribut Management eingegangen. Die Konzepte und Methoden in Hinblick auf die Definition, Verwaltung und Festlegung der Semantik bestimmter Attribute werden in einem zusätzlichen Dokument genauer spezifiziert.

7.2 Datenmodell

Das hier vollständig dargestellte Datenmodell wird in den nachfolgenden Kapiteln nach den vier Management-Bereichen geordnet (aufgeteilt). Darin werden die einzelnen administrativen Prozesse und die wichtigsten Teile des Datenmodells eines Bereichs detaillierter dargestellt und beschrieben. Das Datenmodell enthält nur die konzeptuell erforderlichen Objekte und kann daher weiter konkretisiert und erweitert werden.

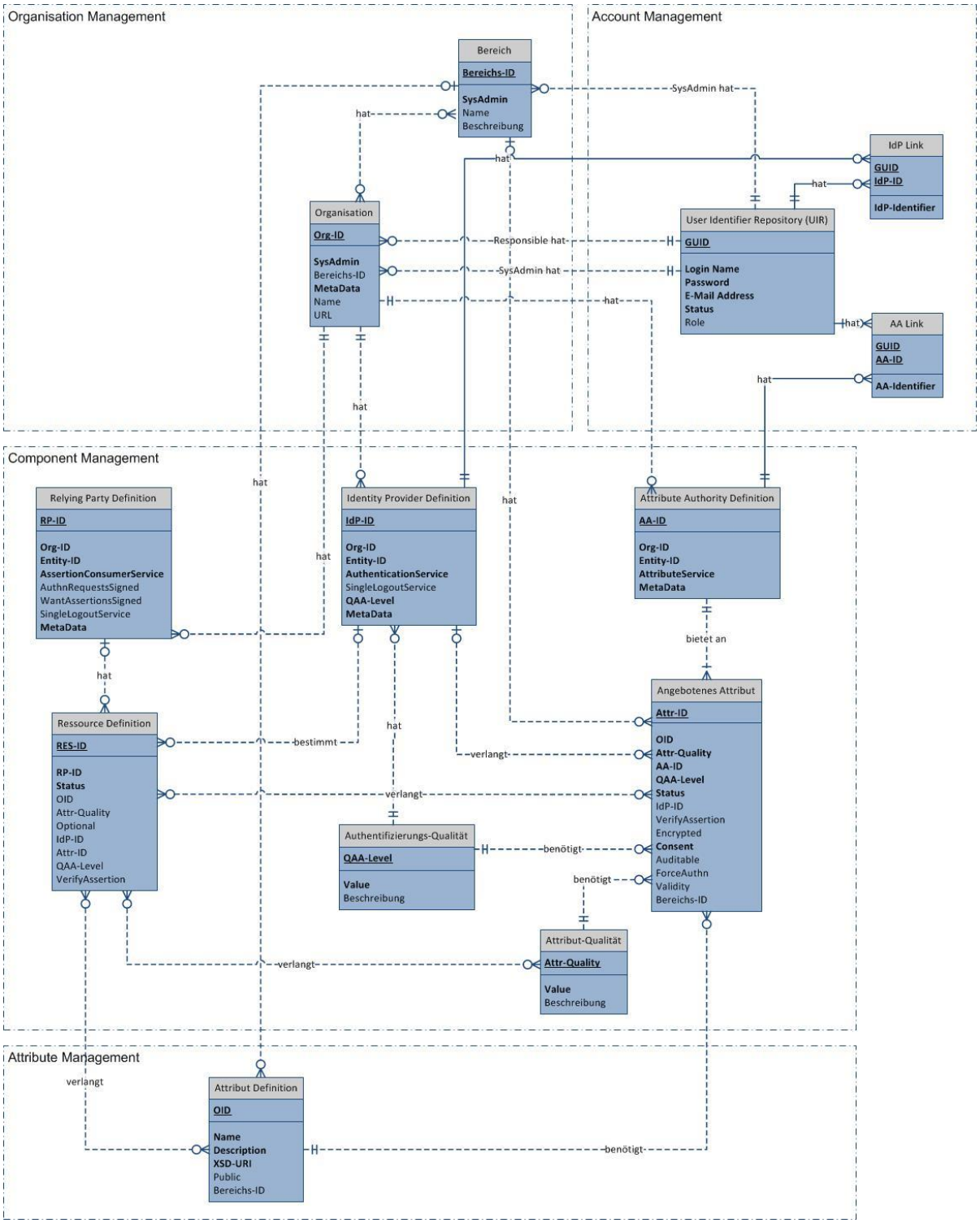


Abbildung 13: Datenmodell SuisseTrustIAM Broker[21]

[21] Um die Übersichtlichkeit des Datenmodells zu verbessern, wurde darauf verzichtet, bei *n:m* Beziehungen eine Zwischentabelle in das Modell aufzunehmen. Stattdessen sind direkte Verbindungen zwischen Tabellen eingezeichnet und entsprechend beschriftet.

7.3 Account Management

Das Account Management kann grob in die Verwaltung der eigentlichen Accountdaten und die Verwaltung der Links zu verschiedenen Komponenten unterteilt werden. Dies wiederspiegelt sich sowohl in den Prozessen als auch den dazugehörenden Bestandteilen des Datenmodells.

7.3.1 Accountdatenverwaltung

Ein Benutzer muss auf dem STIAM-Hub initial einen Account erstellen. Im Falle einer natürlichen Person kann dieser interaktiv auf einer Webseite des STIAM-Hubs erstellt werden. Zusätzlich ist es möglich, seine eigenen Accountdaten zu ändern und einen bereits erstellten Account wieder zu löschen.

7.3.1.1 Account verwalten

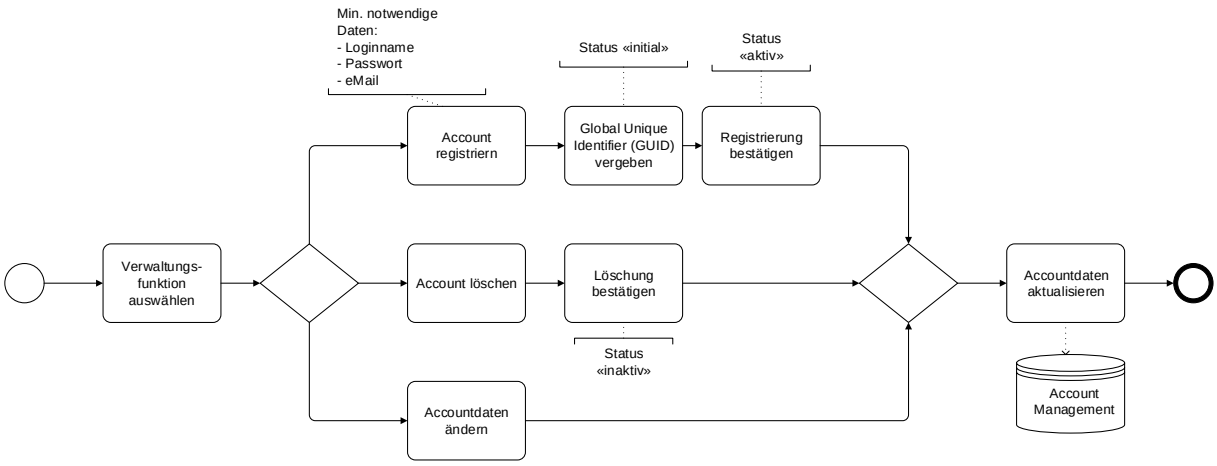


Abbildung 14: Prozess Account verwalten

Minimal notwendig für die Registrierung eines Accounts sind ein Loginname, ein Passwort sowie eine aktive E-Mail Adresse. Vom System wird jedem Benutzer ein Global Unique Identifier (GUID) vergeben, sowie der Accountstatus auf "initial" gesetzt. Sowohl die Aktivierung des Accounts als auch die Löschung eines solchen sind durch den Benutzer zu bestätigen, (was jeweils den Status des Accounts verändert).

Für Benutzer von Organisationen kann der Benutzer den Account eröffnen, muss aber bei Bedarf einen Bewilligungsprozess für die Freigabe durch einen Organisationsverantwortlichen angestossen können.

Die Accountdaten werden im Account Management, genauer im User Identifier Repository (UIR), abgelegt.

7.3.1.2 User importieren

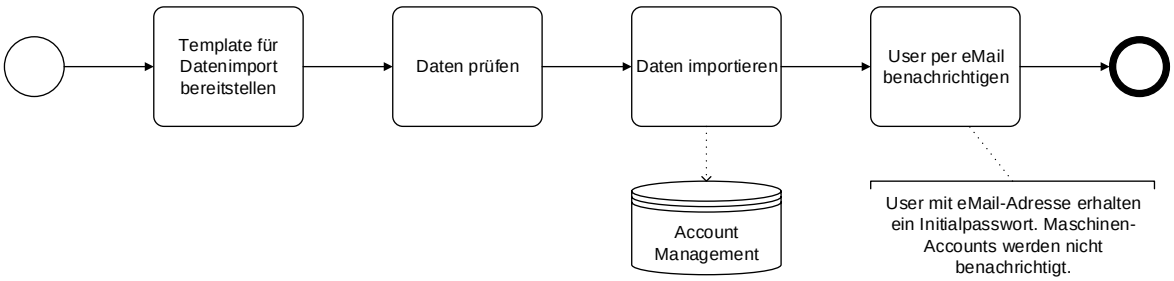


Abbildung 15: Prozess User importieren

Neben einer manuellen Registrierung eines Benutzers können Accounts auch von einem OrgSysAdmin einer Mitgliederorganisation durch einen Massenimport erstellt werden. Hierzu wird ein entsprechendes Template zur Verfügung gestellt. Die erstellten Benutzer erhalten eine Benachrichtigung inklusive Initialpasswort für den Zugriff auf den STIAM-Hub.

Auch in diesem Fall werden die Userdaten im Account Management, genauer im UIR erfasst. Dessen Inhalte werden im Folgenden beschrieben.

7.3.1.3 User Identifier Repository (UIR)

User Identifier Repository (UIR)
GUID
Login Name **Password** **E-Mail Address** **Status** Role

Das User Identifier Repository (UIR) beinhaltet die Accountinformationen eines Subjekts. Diese Informationen können, wie oben beschrieben, manuell erfasst oder durch einen Massenimport geladen werden.

Wie untenstehende Tabelle aufzeigt, beinhaltet das UIR nebst einigen Pflichtfeldern ein ‚Statusfeld', welches die in Abbildung 14 ersichtlichen Status beinhaltet.

Feldname	Bedeutung	Typ
GUID	Eindeutiger Bezeichner des Subjekts. Die GUID wird vom System einem Account zugewiesen	Primärschlüssel
Login Name	Loginname des Users	Pflichtfeld
Password	Bootstrap Passwort für den Useraccount	Pflichtfeld
E-Mail Address	E-Mail Adresse um den Account bestätigen zu lassen	Pflichtfeld
Status	Status des User-Accounts. Wertebereich: Initial, Active, Recover, Disabled, Inactive (Werte werden vom System zugewiesen)	Pflichtfeld
Role	Ein Subjekt kann optional eine Rolle in der Organisation einnehmen. Beispiel eines Wertebereichs: - Responsible (OV) - User-Management (OrgSysAdmin)	Optionales Feld

Feldname	Bedeutung	Typ
	- IdP/AA-Management (OrgSysAdmin) - RP-Management (OrgSysAdmin)	

Tabelle 6: User Identifier Repository

7.3.2 Verwaltung der IdP/AA-Links

Optional kann ein Subjekt einen oder mehrere Identity Provider (IdP) bzw. Attribute Authorities (AA) mit seinem Account verbinden.

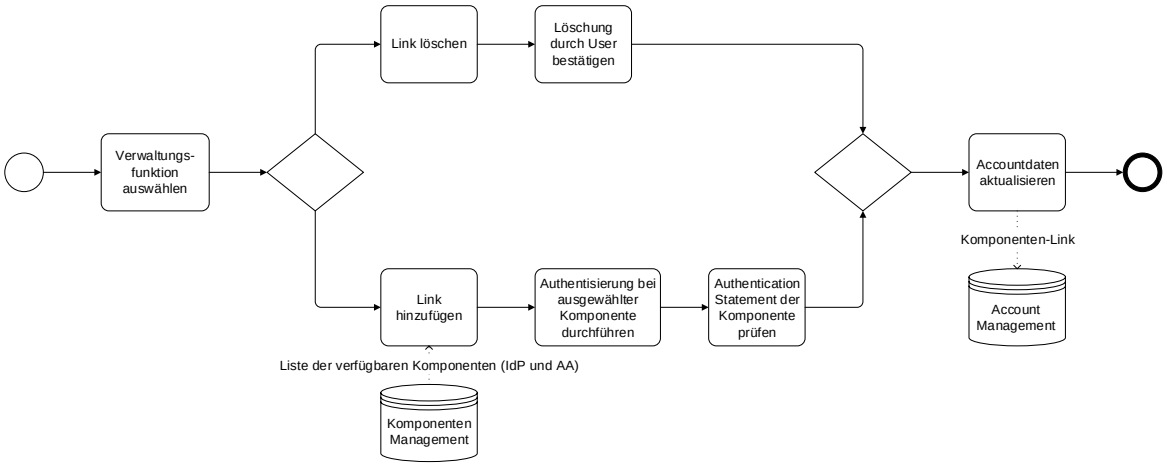
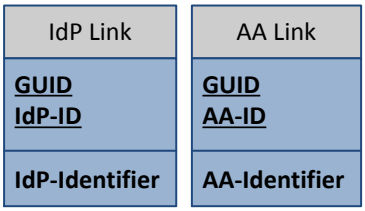


Abbildung 16: Prozess IdP/AA-Link verwalten

Hierzu werden dem User die im Komponenten Management (siehe Kapitel 7.5.1) erfassten IdP bzw. AA zur Auswahl dargeboten. Um eine entsprechende Komponente verlinken zu können, ist eine Authentifizierung des Benutzers gegenüber der Komponente notwendig (siehe Kapitel 6.1). Im Erfolgsfall stellt diese ein *Security Token* aus, welches durch den STIAM-Hub geprüft wird. Ist die Prüfung erfolgreich, wird der IdP/AA-Link im Account Management in der entsprechenden Link Table gespeichert.



Jeder Komponenten-Link wird von der jeweiligen Instanz mittels Identifikator bestätigt, womit eine eindeutige Zuordnung des Benutzers zum Zielsystem erfolgt.

Neben dem Hinzufügen eines neuen Komponenten-Links kann ein solcher auch durch den Benutzer gelöscht werden. Eine entsprechende Löschung ist durch den Benutzer zu bestätigen. Der entsprechende Komponenten-Link wird im Account Management entfernt.

7.4 Organisation Management

Um eine Organisation als SuisseTrustIAM-Mitglied zu erfassen, bedarf es zweier Prozesse, welche von unterschiedlichen Rollen ausgeführt werden müssen.

7.4.1 Organisation verwalten

Zunächst wird eine Organisation durch den STIAM-SysAdmin initial auf dem STIAM-Hub hinzugefügt. Eine Organisation erhält eine eindeutige Org-ID sowie einen Organisationsverantwortlichen (OV) zugeordnet. Die Org-ID wird vom System automatisch vergeben. Der STIAM-SysAdmin ordnet den OV zu. Hierbei muss für diesen bereits ein Account im Account Management vorliegen. Sowohl die Org-ID als auch die GUID des OV werden im Organisation Management gespeichert (siehe Tabelle 7).

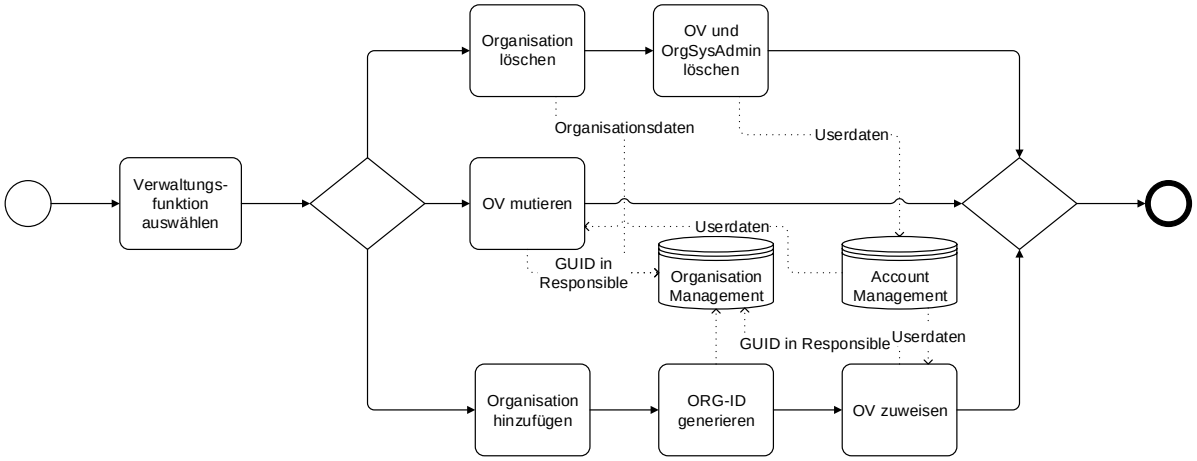


Abbildung 17: Prozess Organisationen verwalten

Neben dem Hinzufügen einer Organisation bleibt es ebenfalls dem STIAM-SysAdmin vorbehalten, den Organisationsverantwortlichen einer Organisation zu mutieren oder eine Organisation zu löschen. Wird eine Organisation gelöscht, muss vom System bzw. vom STIAM-SysAdmin überprüft werden, dass dieser keine Komponenten (siehe Kapitel 7.5.1) mehr zugeordnet sind. Ausserdem müssen allfällige Zuordnungen von Organisationsverantwortlichen und OrgSysAdmin im Account Management entfernt werden.

7.4.2 Organisationsinformationen und Rollen verwalten

Nachdem eine Organisation durch den STIAM-SysAdmin hinzugefügt wurde, obliegt es dem Organisationsverantwortlichen die Informationen der Organisation zu pflegen, sowie einen oder mehrere Systemadministratoren (OrgSysAdmin) zu ernennen.

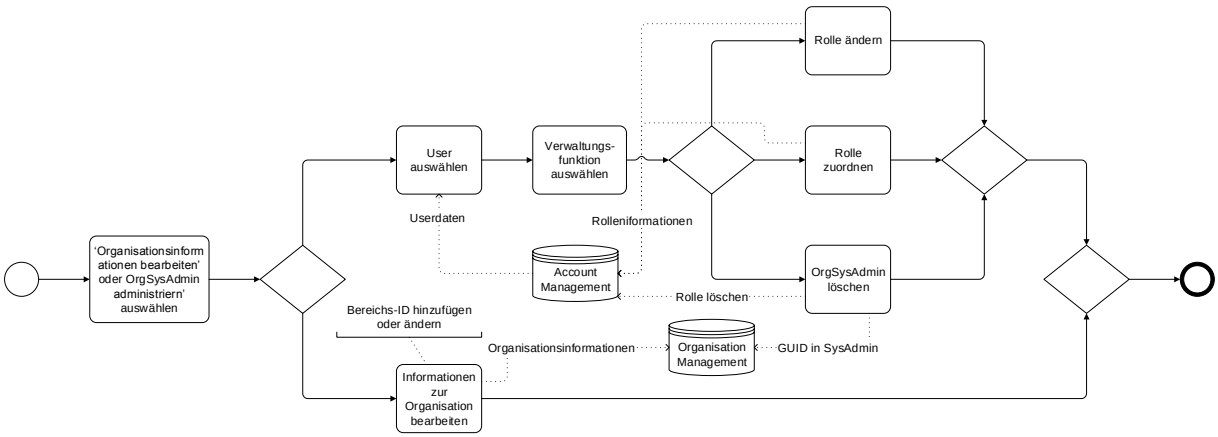


Abbildung 18: Prozess Organisationsinformationen und Rollen verwalten

Der OV erfasst eine Kontaktperson sowie zusätzliche Informationen (Name, Display Name, URL) zur Organisation. Eine Organisation kann zudem einem oder mehreren Bereichen zugeordnet werden (siehe Kapitel 2.3).

Nur einem bereits bestehenden User-Account kann vom OV eine spezifische Rolle als Org-SysAdmin zugeordnet werden. Es ist ebenfalls möglich, diese Rolle anzupassen sowie zu löschen. Im Organisationen Management wird die GUID des jeweiligen Accounts hinterlegt, wobei im Account Management Daten zur jeweiligen Rolle erfasst werden.

7.4.3 Organisation im Datenmodell

Die Definition einer Organisation als SuisseTrustIAM-Mitglied beinhaltet einige Pflichtfelder.
Eine Organisation hat einen oder mehrere Systemadministratoren (SysAdmin) haben. Optional kann eine Organisation einem oder mehreren Bereichen (Bereichs-ID) angehören. Zusätzlich müssen die Metadaten, z.B. ‚Contact Person' oder ‚Organization', abgelegt werden.

Eine Organisation kann beschreibende Merkmale, wie Name und URL, haben.

Feldname	Bedeutung	Typ
Org-ID	Eindeutiger Bezeichner der Organisation	Primärschlüssel
SysAdmin (OrgSysAdmin)	GUID des System Administrators einer Organisation. Der SysAdmin erhält in der UIR die entsprechende Rolle zugeteilt.	Fremdschlüssel
Bereichs-ID	Optionales Feld, welches die Zugehörigkeit zu einem Bereich (abgegrenzte Gruppe von Organisationen) bezeichnet. Eine Organisation kann sich in mehreren Bereichen befinden.	Optionales Feld
MetaData	Meta-Daten der Organisation	Pflichtfeld
Name	Name der Organisation	Optionales Feld
URL	URL der Organisation	Optionales Feld

Tabelle 7: Organisation Management

Ein Bereich stellt eine abgegrenzte Gruppe von Organisationen dar. Innerhalb dieser Gruppe können IdP/AA-Entitäten spezielle Attribute zur Verfügung stellen. Die Zugehörigkeit zu einem Bereich berechtigt dann eine Relying Party diese Attribute abfragen zu können.

Ein Bereich hat einen oder mehrere Systemadministratoren und kann zusätzliche Merkmale, wie Name und Beschreibung haben.

Feldname	Bedeutung	Typ
Bereichs-ID	Eindeutiger Bezeichner des Bereiches	Primärschlüssel
SysAdmin (OrgSysAdmin)	GUID des System Administrators eines Bereiches. Der SysAdmin erhält in der UIR die entsprechende Rolle zugeteilt.	Fremdschlüssel
Name	Name des Bereiches	Optionales Feld
Beschreibung	Beschreibung des Bereiches	Optionales Feld

Tabelle 8: Definition Bereich

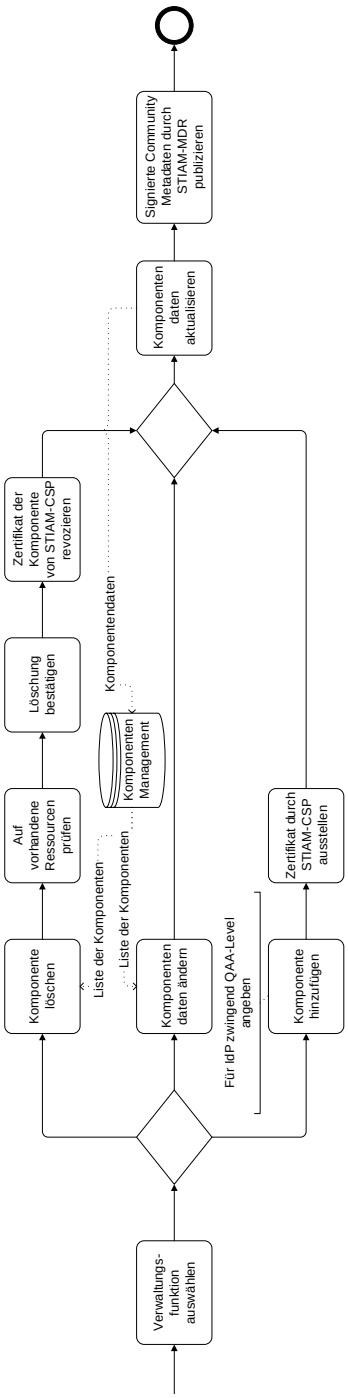
Um einen SysAdmin einer Organisation oder einem Bereich zuordnen zu können, muss dieser auf dem STIAM-Hub über einen Account verfügen.

7.5 Komponenten Management

Im Komponenten Management werden die einzelnen Komponenten einer Organisation, also IdP, AA und Relying Party (RP), vom OrgSysAdmin verwaltet. Ausserdem werden im Falle einer Relying Party die Ressourcen sowie bei einer Attribut-Autorität die Attribute geführt.

7.5.1 Komponenten verwalten

Eine Komponente wird vom OrgSysAdmin hinzugefügt bzw. gelöscht oder deren Daten geändert.



Wird eine Komponente hinzugefügt, muss ein Zertifikat vom STIAM-CSP ausgestellt werden. Für das Hinzufügen eines IdP ist es zwingend notwendig, dass ein QAA-Level angegeben wird.

Wird eine bestehende Komponente gelöscht, ist zu überprüfen, dass keine Ressourcen mehr mit der Komponente in Beziehung stehen. Die definitive Löschung ist zu bestätigen und das vom SuisseTrustIAM-CSP ausgestellte Zertifikat zu revozieren. Alle Änderungen werden im Komponenten Management aktualisiert, was dazu führt, dass die Community Metadaten vom SuisseTrustIAM-MDR neu signiert und publiziert werden.

Abbildung 19: Prozess Komponente verwalten

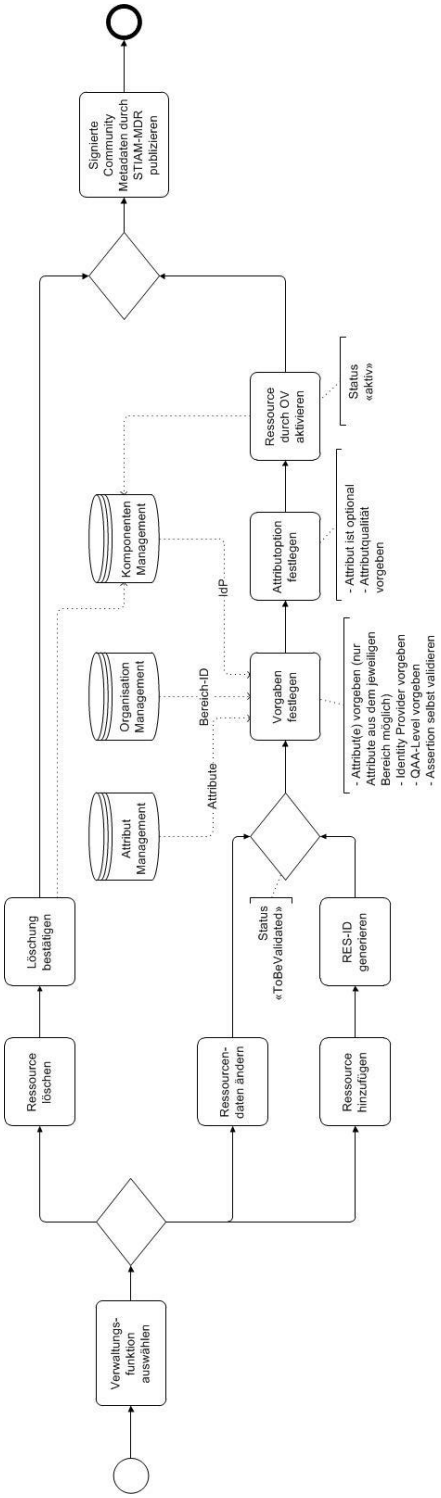


Abbildung 20: Prozesse Ressourcen verwalten

7.5.2 Ressourcen verwalten

Einer im Komponenten Management erfassten Relying Party werden vom OrgSysAdmin entsprechende Ressourcen zugeordnet.

Einer erstellten Ressource wird eine RES-ID vom System zugeordnet. Zu einer Ressource können optional verschiedene Vorgaben konfiguriert werden:

- Attribut(e) vorgeben (nur Attribute aus dem jeweiligen Bereich möglich)
- Identity Provider vorgeben (nur bestimmte IdP werden akzeptiert)
- QAA-Level vorgeben (minimal akzeptierter QAA-Level)
- Assertion selbst validieren

Zusätzlich sind folgende Attributoptionen konfigurierbar:

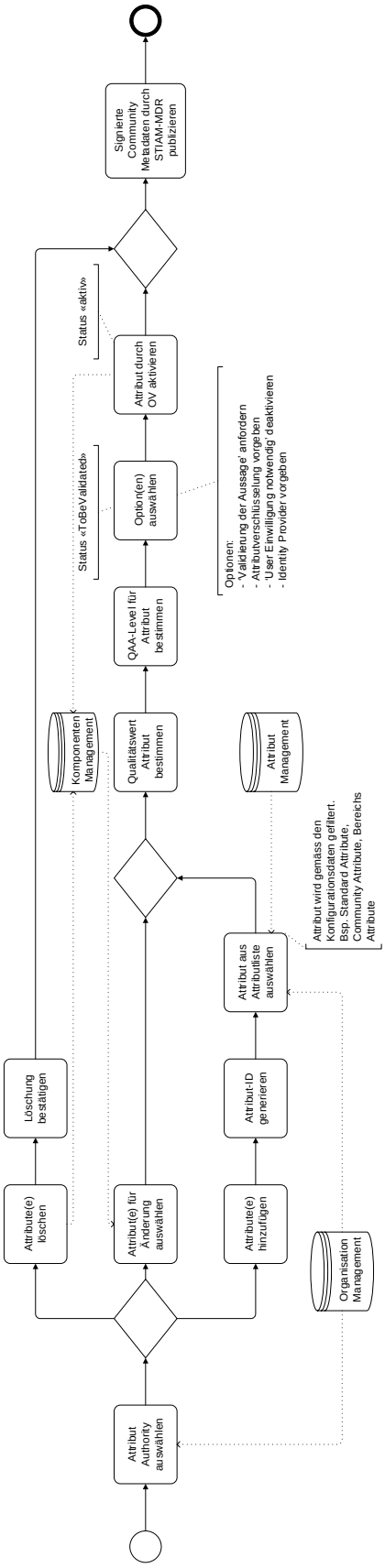
- Attribut ist optional
- Attributqualität vorgeben

Die vom OrgSysAdmin eingegebenen Informationen, sowie die konfigurierten Optionen zu einer Ressource müssen vom zuständigen OV validiert und die Ressource aktiviert werden. Erst dann ändert der Status der Ressource von "ToBeValidated" auf "aktiv".

Auf die gleiche Weise ist es auch möglich, dass die Daten einer bestehenden Ressource geändert werden. Wird eine bestehende Ressource einer anderen Relying Party zugeordnet, wird die entsprechend Zuordnung im Komponenten Management geändert, die Ressourcendaten hingegen unverändert übernommen. Es ist ausserdem möglich, eine bestehende Ressource zu löschen. Eine definitive Löschung ist in jedem Fall zu bestätigen. Alle Änderungen führen zu einer Publikation der signierten Community Metadaten durch das SuisseTrustIAM-MDR.

7.5.3 Attribute verwalten

Zu einer Attribut-Autorität werden entsprechende Attribute hinzugefügt oder gelöscht. Ausserdem können Änderungen an deren Konfiguration vorgenommen werden. Attribute werden vom OrgSysAdmin einer spezifischen AA zugeordnet.



Jede neue Attributzuordnung erhält eine Attribut-ID vom System. Das konkrete Attribut wird aus einer Liste der verfügbaren Attribute ausgewählt. Die Angaben zu den Attributen stammen hierbei aus dem Attribute Management. Die generierte Liste wird entsprechend der Konfigurationsdaten aus dem Organisation Management (beispielsweise nach Bereichs-ID) gefiltert. Zu jedem hinzugefügten Attribut muss ein Qualitätswert sowie ein QAA-Level angegeben werden (siehe Kapitel 7.5.4.4). Zusätzlich sind folgende Optionen konfigurierbar:

- "Validierung der Aussage" anfordern
- Attributverschlüsselung vorgeben
- "User Einwilligung notwendig" deaktivieren
- Identity Provider vorgeben

Auch im Falle der Attributverwaltung müssen die vom OrgSysAdmin eingegebenen Informationen, sowie konfigurierten Optionen vom zuständigen OV validiert und damit aktiviert werden. Erst dann ändert der Status der Ressource von "ToBeValidated" auf "aktiv".

Um ein oder mehrere zugeordnete Attribute definitiv zu löschen, ist eine Bestätigung notwendig. Alle Änderungen führen auch hier zur Publikation der signierten Community Metadaten durch das SuisseTrustIAM-MDR.

Abbildung 21: Prozess Attribute verwalten

7.5.4 Komponenten, Ressourcen und Attribute im Datenmodell

Bei der Aufnahme einer Organisation als SuisseTrustIAM Mitglied wird, wie in Kapitel 7.4 beschrieben, ein Organisation-Objekt erstellt. Unter diesem Objekt können vom OrgSysAdmin die einzelnen Komponenten (IdP, AA, RP) erstellt werden. Die notwendigen Attribute werden in den folgenden Tabellen abgelegt:

- Identity Provider Definition
- Attribute Authority Definition
- Relying Party Definition
- Ressource Definition

Zusammen mit den Organisations-Metadaten (Organization, Contact Person) aus Kapitel 7.4 können aus diesen Daten die gesamten Metadaten für die SuisseTrustIAM-Community gebildet werden.

7.5.4.1 Definition von QAA-Level und Attribut-Qualität

Voraussetzung für die Definition der einzelnen Komponenten ist die Definition der Authentifizierungs- und Attribut-Qualität.

Die Authentifizierungs-Qualität muss entsprechend dem „eCH-0170 Qualitätsmodell für elektronische Identitäten“ [4] definiert werden. Dazu muss für jede mögliche Stufe ein eindeutiger Bezeichner und der Wert (Value) definiert werden. Optional kann eine Beschreibung angegeben werden.

Feldname	Bedeutung	Typ
QAA-Level	Eindeutiger Bezeichner des QAA-Levels	Primärschlüssel
Value	Qualitätsstufe	Pflichtfeld
Beschreibung	Beschreibung des QAA-Levels	Optionales Feld

Tabelle 9: Definition Authentifizierungs-Qualität (QAA-Level)

Die Attribut-Qualität muss entsprechend dem „eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID“ [5] definiert werden. Dazu muss für jede mögliche Qualitäts-Stufe ein eindeutiger Bezeichner und der Wert (Value) definiert werden. Optional kann eine Beschreibung angegeben werden.

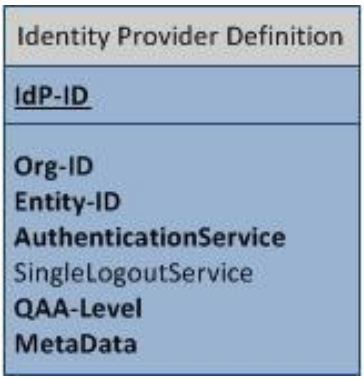
Feldname	Bedeutung	Typ
Attr-Quality	Eindeutiger Bezeichner der Attribut-Qualität	Primärschlüssel
Value	Qualitätsstufe	Pflichtfeld
Beschreibung	Beschreibung der Attribut-Qualität	Optionales Feld

Tabelle 10: Definition Attribut-Qualität

7.5.4.2 Identity Provider Definition

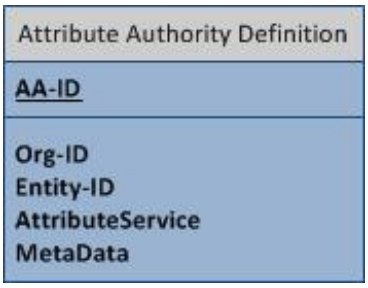
Feldname	Bedeutung	Typ
IdP-ID	Eindeutiger Bezeichner des IdP	Primärschlüssel
Org-ID	Organisation, zu welcher der IdP gehört	Fremdschlüssel
Entity-ID	Eindeutiger Name der Entity	Pflichtfeld
AuthenticationService	URI für den Authentifizierungsservice	Pflichtfeld
SingleLogoutService	URI für den SingleLogoutService des IdP	Optionales Feld
QAA-Level	Gibt den Authentifizierungslevel des IdP an	Fremdschlüssel
MetaData	Meta-Daten des IdPs	Pflichtfeld

Tabelle 11: Identity Provider Definition



Als Identity Provider (IdP) können STIAM-IdPs, kommerzielle Identity Provider (z.B. SuisseID) und Identity Provider einer Organisation definiert werden.

7.5.4.3 Attribute Authority Definition



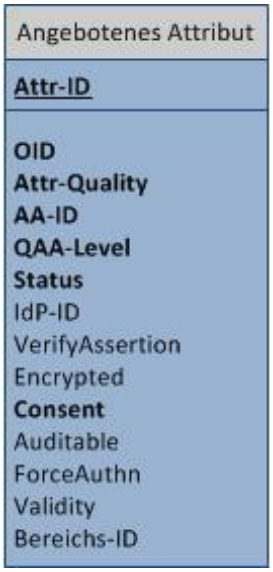
Eine Attribut-Autorität ist ein Service einer Organisation, welcher auf eine Attribute Request Message die angeforderten Attribute in signierter Form (Attribute Assertion) an den STIAM-Hub zurücksendet. Welche Nachrichten zur Laufzeit zwischen STIAM-Hub und AA ausgetauscht werden, kann dem Kapitel 5.1 entnommen werden.

Feldname	Bedeutung	Typ
AA-ID	Eindeutiger Bezeichner der AA	Primärschlüssel
Org-ID	Organisation, zu welcher der AA gehört	Fremdschlüssel
Entity-ID	Eindeutiger Name der Entity	Pflichtfeld

Feldname	Bedeutung	Typ
AttributeService	URI für den Attribute Assertion Service	Pflichtfeld
MetaData	Meta-Daten der AA, inklusive die Schlüsselinformationen zum Verifizieren der Signatur	Pflichtfeld

Tabelle 12: Attribute Authority Definition

7.5.4.4 Angebotenes Attribut



Attribute Authorities können Attribute innerhalb der SuisseTrustIAM-Community anbieten. Diese Attribute benötigen eine Attribute-ID (Attr-ID) und einen Object Identifier (OID) welcher das Attribut definiert.

Eine Organisation, welche ein Attribut anbietet, muss einen Mindest-Authentifizierungs-Level (QAA-Level) angeben und das Attribut mit einem Qualitätswert (Attr-Quality) versehen.

Ein angebotenes Attribut muss einen Status haben.

Es wird festgelegt (Consent), ob ein User Consent notwendig ist und welche Komponente ihn einholt.

Optional kann ein Anbieter verlangen, dass er die Authentifizierung eines Identity Providers selbst prüfen kann.

Optional kann die Nutzung eines Attributs von einem Anbieter für einen bestimmten Bereich eingegrenzt werden.

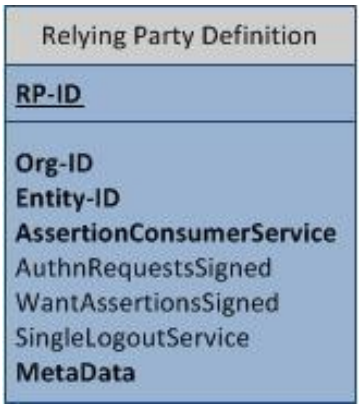
Feldname	Bedeutung	Typ
Attr-ID	Eindeutiger Bezeichner eines Attributs	Primärschlüssel
OID	Object Identifier (OID) zur Attribut Definition	Fremdschlüssel
Attr-Quality	Qualität des angebotenen Attributs Wertebereich entsprechend eCH-0171 [5]	Fremdschlüssel
QAA-Level	Quality Authentication Assurance Level der eID des Subjekts Wertebereich [1..4]	Fremdschlüssel
AA-ID	Verweis auf die ID des Anbieters	Fremdschlüssel
Status	Status des angebotenen Attributs	Pflichtfeld
IdP-ID	Vorgegebener Identity Provider	Fremdschlüssel

Feldname	Bedeutung	Typ
VerifyAssertion	AA verlangt zusätzliche Authentifizierung des Subjekts. Damit muss der STIAM-Hub im ‚Identity Relay Modus'[22] antworten.	Optionales Feld
Encrypted	Attributinhalt muss verschlüsselt werden	Optionales Feld
Consent	Gibt an, ob das Einverständnis des Users erforderlich ist und welche Komponente es einholt: • Hub: Default Wert, User Consent wird vom Hub eingeholt • AA: User Consent wird vom STIAM-Sender eingeholt. • Public: Kein User Consent	Pflichtfeld
Auditable	Gibt an, ob der STIAM-Hub den Inhalt des Attributs loggen darf.	Optionales Feld
ForceAuthn	Mit der Herausgabe dieses Attributs ist eine zeitnahe Authentifizierung des Subjekts durch einen IdP zwingend vorgeschrieben.	Optionales Feld
Validity	Gibt eine Zeit an, wie lange ein Attribut in einem Cookie zwischengespeichert werden darf.	Optionales Feld
Bereichs-ID	Ordnet ein Attribut einem Bereich zu.	Fremdschlüssel

Tabelle 13: Angebotenes Attribut

7.5.4.5 Relying Party Definition

Eine Organisation kann einen Service Provider Service definieren, welcher die Security Tokens und Attribute Assertions entgegennimmt. Unterhalb dieses Service Providers, welcher im Sinne eines Portals zu verstehen ist, können eine oder mehrere Ressourcen als Applikationen definiert werden.



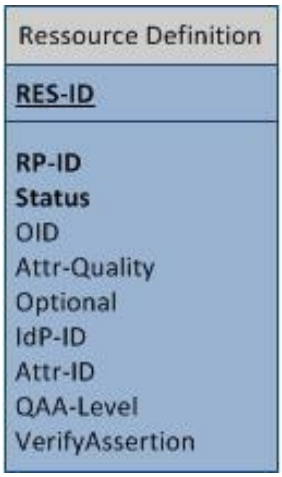
Feldname	Bedeutung	Typ

[22] Vergleiche Kapitel 3.4.2

Feldname	Bedeutung	Typ
RP-ID	Eindeutiger Bezeichner einer RP	Primärschlüssel
Org-ID	Organisation, zu welcher die RP gehört	Fremdschlüssel
Entity-ID	Eindeutiger Name der Entity	Pflichtfeld
AssertionConsumerService	URI des Service Provider Services	Pflichtfeld
AuthnRequestsSigned	Gibt an, ob die Relying Party ihre Authentication Requests signiert absendet	Optionales Feld
WantAssertionsSigned	Gibt an, ob Assertions vom STIAM-Hub signiert werden müssen	Optionales Feld
SingleLogoutService	URI für den SingleLogoutService des Service Providers	Optionales Feld
MetaData	Meta-Daten der RP, inklusive der Schlüsselinformationen zum Verschlüsseln und Verifizieren der Signatur	Pflichtfeld

Tabelle 14: Relying Party Definition

7.5.4.6 Ressource Definition



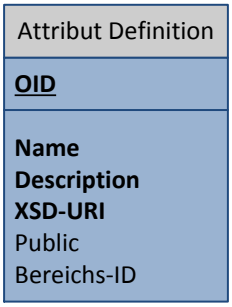
Eine Relying Party als Service Provider kann eine oder mehrere Ressourcen definieren. Die Ressource wird im Authentication Request zur Laufzeit von der Relying Party in Form einer Indexnummer an den STIAM-Hub übermittelt. Der STIAM-Hub kann damit in den Ressource Definitionen die vorgegebenen Anforderungen auslesen. Damit ist er darüber informiert, welche Attribute und optionalen Anforderungen für einen Zugriff auf die Ressource verlangt sind.

Feldname	Bedeutung	Typ
RES-ID	Eindeutiger Bezeichner einer Ressource	Primärschlüssel
RP-ID	Referenzierende Relying Party	Fremdschlüssel
Status	Status der Ressource	Pflichtfeld
OID	Direkter Verweis auf ein oder mehrere Attribute, welche für den Entscheid einer Zugriffsberechtigung auf die Ressource benötigt werden	Fremdschlüssel
Attr-Quality	Ein SysAdmin kann pro definierte OID einen	Fremdschlüssel

Feldname	Bedeutung	Typ
	Qualitätswert vorgeben	
Optional	Gibt pro Attribut an, ob es ‚optional' sein kann. Standardmässig ist in SuisseTrustIAM ein Attribut immer erforderlich.	Optionales Feld
IdP-ID	Pro Ressource kann ein Identity Provider vorgegeben werden.	Optionales Feld
Attr-ID	Angabe von einem oder mehreren ‚Angebotenen Attributen', welche für den Entscheid einer Zugriffsberechtigung auf die Ressource benötigt werden.	Optionales Feld
QAA-Level	Pro Ressource kann eine Authentifizierungsstufe (QAA-Level) vorgegeben werden.	Fremdschlüssel
VerifyAssertion	Damit fordert die Ressource beim STIAM-Hub den ‚Identity Relay Modus' an.	Optionales Feld

Tabelle 15: Ressource Definition

7.6 Attribut Management



Jedes Attribut verfügt über einen eindeutigen Object Identifier (OID) und über bestimmte Informationen welche das Attribut weiter definieren.

Nebst Name und Beschreibung fallen darunter weitere technische Informationen wie die Syntax, der Namensraum und der Wertebereich. Diese werden als Link zu einer Attributschema XSD-Datei gekennzeichnet.

Feldname	Bedeutung	Typ
OID	Eindeutiger Bezeichner eines Attributs	Primärschlüssel
Name	Friendly-Name des Attributs	Pflichtfeld
Description	Beschreibung des Attributs	Pflichtfeld
XSD-URI	Link auf Attributschema	Pflichtfeld
Public	Damit kann das Einverständnis des Users zur Herausgabe eines Attributs übersteuert werden	Optionales Feld
Bereichs-ID	Ordnet ein Attribut einem oder mehreren Bereichen (Domänen) zu	Optionales Feld

Tabelle 16: Attribut Definition

8 Sicherheitsüberlegungen

Die hier vorliegende SuisseTrustIAM Architektur versucht möglichst viele Privacy- und Sicherheitsanforderungen zu berücksichtigen. Dennoch konnten nicht alle Fragen, gerade bezüglich Schutz der Privatsphäre und der Sicherheit, geklärt werden. Angriffsmöglichkeiten und vorsätzliche Missbrauchsszenarien, zum Beispiel, müssen laufend überprüft und diskutiert werden.

Szenario	Beschreibung	Wahrscheinlichkeit	Schadenspotential
Falsche LinkedID	Ein Benutzer verlinkt mutwillig falsche Identitäten auf dem STIAM-Sender oder einem IdP mit seinem Account.	Gering. Benutzer braucht Zugang zu den falschen Identitäten.	Mittel. Der Benutzer bekommt evtl. unberechtigt Zugang/Zugriff bei RPs.
Schwache AA-Identität	Wenn ein Angreifer die Credentials eines ‚schwachen' AA-Accounts eines anderen Benutzers kennt, so kann er zur Definitionszeit falsche Attribute an seine Identität binden.	Gering. Angreifer muss Account-Informationen erlangen.	Mittel. Der Angreifer bekommt evtl. unberechtigt Zugang/Zugriff bei RPs.
Diebstahl Security Token	Security Token wird beim Übertragen auf den Browser des Benutzers abgefangen.	Gering.	Gering. Der Täter kann die Identität des Benutzers übernehmen und innerhalb der Security-Session die begonnenen Tätigkeiten des Benutzers fortsetzen.
Zentrales Logging	Das zentrale Logging auf dem STIAM-Hub (vgl. Kap. 5.6) wirft Datenschutzfragen auf, da die entsprechenden Vorgänge auf Vorrat zentral gespeichert werden.	Mittel.	Gering. Aktivitäten der Benutzer innerhalb der Identity Federation werden nachvollziehbar.

Tabelle 17: Sicherheitsüberlegungen

9 Verwandte Themen

In der folgenden Tabelle sollen einige dieser Themen, welche in diesem Dokument nur am Rand oder gar nicht thematisiert wurden, aufgelistet werden. Diese Liste versteht sich als Anregung zu künftigen Versionen von SuisseTrustIAM und ist sicherlich nicht als abschliessend zu betrachten.

Thema	Beschreibung
Inter-Federation	Wie sieht eine Integration einer bereits bestehenden Identity Federation aus? Beispielsweise wenn SWITCH-aai in SuisseTrustIAM integriert werden soll?
Organisationsinternen Identity Federation	Wie sehen die Anforderung und das Vertrauensmodell der Identity Federation innerhalb einer Organisations aus. Auf welche Funktionalitäten kann verzichtet werden? Welche neue Anfordrungen, z.B. Provisioning, Überwachung von Berechtigungen kommen hinzu
Einbindung öffentlicher Register	Wie können öffentliche Register ohne Authentifizierungsmöglichkeit als Attribute Authority eingebunden werden? Wie stellt man ein verlässliches Identity Mapping her?
Request on behalf of...	In der jetzigen Architektur geht man davon aus, dass der STIAM-Hub immer berechtigt ist, über ein bestimmtes Subjekt bei einer AA eine Anfrage zu einem Attribut zu machen. Wenn die AA die erfolgte Authentifizierung des Subjekts nicht selbst prüfen will, so akzeptiert sie jede vom STIAM-Hub signierte Anfrage zu einer AA-ID als Identifikator. Was ist, wenn RP und AA ein höheres Vertrauen fordern? Was ist, wenn RP und AA sich davon überzeugen müssen, dass der Hub zu diesem Zeitpunkt für dieses Subjekt tatsächlich dieses Attribut anfordern darf? Der AA muss also überprüfen können, ob der Hub wirklich in Vertretung des anfragenden RP handelt?

Tabelle 18: Weitere Themen

10 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein eCH dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellt, oder welche eCH referenziert, 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.

11 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 und Bibliographie

[1] IETF, «Key words for use in RFCs to Indicate Requirement Levels,» March 1997. [Online]. Available: http://www.ietf.org/rfc/rfc2119.txt.

[2] eCH, «eCH-0107 IAM-Gestaltungsprinzipien,» [Online]. Available: http://www.ech.ch/.

[3] Berner Fachhochschule, «eCH-0167 SuisseTrustIAM-Rahmenkonzept,» [Online]. Available: http://www.ech.ch.

[4] eCH, «eCH-0170 Qualitätsmodell für elektronische Identitäten,» [Online]. http://www.ech.ch.

[5] eCH, «eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID,» [Online]. http://www.ech.ch.

[6] N. Klingenstein, «Attribute Aggregation and Federated Identity,» in *International Symposium on Applications and the Internet Workshop*, 2007.

[7] OpenID Foundation, «OpenID Connect,» 2013. [Online]. Available: http://openid.net/connect/.

[8] IETF, «JSON Web Token (JWT),» 2014. [Online]. Available: http://tools.ietf.org/html/draft-ietf-oauth-json-web-token-20.

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

[10] OASIS, “Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0,” March 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.

[11] Berner Fachhochschule, «eCH-0169 SuisseTrustIAM-Geschäftsarchitektur,» [Online]. Available: www.ech.ch.

[12] Oasis, «Web Services Federation Language (WS-Federation) Version 1.2,» May 2009. [Online]. Available: http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf.

[13] IBM, «Understanding WS-Federation,» May 2007. [Online]. Available: http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-fed/WS-FederationSpec05282007.pdf?S_TACT=105AGX04&S_CMP=LP.

[14] OASIS, «WS-Trust 1.4,» February 2009. [Online]. Available: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.pdf.

[15] A. G. Oliver Pfaff, «SAML Proxying and Attribute Services,» 2012.

[16] IETF, «The OAuth 2.0 Authorization Framework,» October 2012. [Online]. Available:

http://www.rfc-base.org/txt/rfc-6749.txt.

[17] IETF, «The OAuth 2.0 Authorization Framework: Bearer Token Usage,» October 2012. [Online]. Available: http://www.rfc-base.org/txt/rfc-6750.txt.

[18] Google, «Overlap of identity technologies,» 2011. [Online]. Available: https://sites.google.com/site/oauthgoog/Overlap.

[19] Berner Fachhochschule, «eCH-0168 SuisseTrustIAM-Standardprozesse,» 2013.

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

[21] OASIS, March 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.

[22] D. Chadwick und G. Inman, «Attribute Aggregation in Federated Identity Management, , May 2009, pp. 33-40.,» 2009.

[23] SECO, [Online]. Available: http://www.suisseid.ch.

[24] eCH Fachgruppe IAM, 2010. [Online]. Available: http://www.isb.admin.ch.

[25] SWITCH, 2012. [Online]. Available: www.switch.ch/aai.

[26] Internet2, [Online]. Available: http://www.internet2.edu.

[27] O. Pfaff, «Federated IdM Protocol – SAML 2.0 (Deep Dive),» 2012.

[28] Wikipedia, «Wikipedia - Die freie Enzykolpädie,» 2012. [Online]. Available: http://de.wikipedia.org/wiki/Martin-Notation. [Zugriff am 2012].

[29] University of Kent (UK), «Conceptual Model for Attribute Aggregation,» 2008. [Online]. Available: http://sec.cs.kent.ac.uk/shintau/ShintauConceptualModel.doc.

[30] OASIS, «SAML Metadata Specification,» 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0.

Anhang B – Mitarbeit & Überprüfung

Agosti Stefan	Berner Fachhochschule
Bernold Ronny	Berner Fachhochschule
Bürge Urs	Urs Bürge Beratung GmbH
Häni Hans	Berner Fachhochschule
Häring Ulrich	ATOS
Hassenstein Gerhard	Berner Fachhochschule
Laube-Rosenpflanzer Annett	Berner Fachhochschule eCH Fachgruppe IAM
Leiser Daniel	ATOS
Topfel Martin	Berner Fachhochschule eCH Fachgruppe IAM
Vinzens Marcel	Adnovum

Anhang C – Abkürzungen

IdP	Identity Provider
AA	Attribut-Autorität
RP	Relying Party
SSO	Single-Sign-On
SAML	Security Assertion Markup Language
IAM	Identity und Access Management
OID	Object Identifier
XSD	XML Schema Definition
URL	Uniform Resource Locator
URI	Uniform Resource Indicator
UIR	User Identifier Repository
STIAM	SuisseTrustIAM
SysAdmin	Systemadministrator
OrgSysAdmin	Systemadministrator einer Organisation
OV	Organisationsverantwortlicher
CSP	Certification Service Provider
CA	Certification Authority
RLM	Reporting, Logging, Monitoring
MDR	Metadata Registry

Anhang D – Glossar

Spezielle Begriffe welche in diesem Dokument verwendet werden, sind zu Beginn des Dokuments in Kapitel 2 beschrieben. Es wird an dieser Stelle auf ein weiteres Glossar verzichtet, da alle weiteren Begriffe bereits in den Dokumenten eCH-0107 [2] und eCH-0167 [3] umfassend beschrieben wurden.

Anhang E – Änderungskontrolle

Version	Datum	Beschreibung, Bemerkung	Name
0.5	13.12.2012	Initiale Version	Gerhard Hassenstein
0.6	15.12.2012	Mit ‚SuisseTrustIAM Standardprozesse' abgestimmte Version	Gerhard Hassenstein
0.7	03.01.2013	Anpassungen nach internem Review	Stefan Agosti
0.8	07.01.2013	Zusammenführung techn. Architektur und Standardprozesse	Stefan Agosti
0.9	22.02.2013	Anpassungen nach internem Review BFH	Gerhard Hassenstein
0.95	27.02.2013	Anpassungen nach Review ATOS	Gerhard Hassenstein
0.98	25.11.2013	Komplett überarbeitete Version	Gerhard Hassenstein Stefan Agosti
1.0	27.11.2013	Version nach internem Review	Gerhard Hassenstein Stefan Agosti
1.1	12.03.2014	Überarbeitung nach Meeting bei Atos	Gerhard Hassenstein Hans Häni Marcel Vinzens Urs Pfenninger Daniel Leiser
1.2	23.05.2014	Feedback Urs Bürge, Überarbeitung nach Meeting bei Atos, techologieneutral	Annett Laube-Rosenpflanzer
1.3	04.06.2014	Feedback der FG IAM, Vernehmlassungsversion	Annett Laube-Rosenpflanzer
1.4	03.09.2014	Feedback aus der Vernehmlassung	Annett Laube-Rosenpflanzer

Anhang F – Abbildungsverzeichnis

Abbildung 1: Einordnung des eCH-0168 Standards 8
Abbildung 2: STIAM-Komponenten 14
Abbildung 3: STIAM-Hub und Dienste 15
Abbildung 4: STIAM-Hub-Modell 16
Abbildung 5: Identität- und Attributvermittlung mittels Proxying 19
Abbildung 6: Identitäts- und Attributvermittlung mittels solicited Messages 20
Abbildung 7: Direktes Attributaggregationsverfahren 37
Abbildung 8: Single Logout Verfahren 42
Abbildung 9: IdP-Linking-Protokoll 44
Abbildung 10: AA-Linking-Protokoll 46
Abbildung 11: Ausprägungen der Organisation 48
Abbildung 12: Prozesslandkarte administrativer Prozesse des STIAM-Hubs 50
Abbildung 13: Datenmodell SuisseTrustIAM Broker 51
Abbildung 14: Prozess Account verwalten 52
Abbildung 15: Prozess User importieren 53
Abbildung 16: Prozess IdP/AA-Link verwalten 54
Abbildung 17: Prozess Organisationen verwalten 55
Abbildung 18: Prozess Organisationsinformationen und Rollen verwalten 55
Abbildung 19: Prozess Komponente verwalten 58
Abbildung 20: Prozesse Ressourcen verwalten 59
Abbildung 21: Prozess Attribute verwalten 60

Anhang G – Tabellenverzeichnis

Tabelle 1: STIAM-Protokolle 22
Tabelle 2: Typen von Identifikatoren 25
Tabelle 3: Anforderungen an SuisseTrustIAM Vermittlerinfrastruktur 30
Tabelle 4: Reporting (R), Logging (L), Monitoring (M) 43
Tabelle 5: Beschreibung der Rollen innerhalb der administrativen Prozesse 49
Tabelle 6: User Identifier Repository 54
Tabelle 7: Organisation Management 56
Tabelle 8: Definition Bereich 57
Tabelle 9: Definition Authentifizierungs-Qualität (QAA-Level) 61
Tabelle 10: Definition Attribut-Qualität 62
Tabelle 11: Identity Provider Definition 62
Tabelle 12: Attribute Authority Definition 63
Tabelle 13: Angebotenes Attribut 64
Tabelle 14: Relying Party Definition 65
Tabelle 15: Ressource Definition 66
Tabelle 16: Attribut Definition 66
Tabelle 17: Sicherheitsüberlegungen 67
Tabelle 18: Weitere Themen 68