eCH-0167 SuisseTrustIAM Rahmenkonzept

Name	SuisseTrustIAM Rahmenkonzept
Standard-Nummer	eCH-0167
Kategorie	Standard
Reifegrad	Definiert
Version	1.0
Status	Genehmigt
Genehmigt am	2014-06-04
Ausgabedatum	2014-06-06
Ersetzt Standard	--
Sprachen	Deutsch (Original) und Französisch (Übersetzung)
Beilagen	keine
Autoren	Fachgruppe Identity und Access Management Gerhard Hassenstein, Berner Fachhochschule, gerhard.hassenstein@bfh.ch Ronny Bernold, Berner Fachhochschule, ronny.bernold@bfh.ch Thomas Selzam, Berner Fachhochschule, thomas.selzam@bfh.ch Olivier Brian, Berner Fachhochschule, olivier.brian@bfh.ch
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 soll schweizweit generische Identity & Access Management-Services für E-Government, E-Health, E-Education sowie für die E-Economy zur Verfügung stellen. Als wichtigste und innovativste Funktionalität wird eine Vermittlerinfrastruktur angeboten. Sie ermöglicht einen qualifizierten Nachweis von Attributen (Rolle) via Register oder Verzeichnis für ein authentifiziertes Subjekt (repräsentiert durch eine eIdentity) einer Unternehmung oder Organisation, einschliesslich der Nachverfolgbarkeit.

Dieses Rahmenkonzept beschreibt die Basis-Funktionsweise der gesamten SuisseTrustIAM-Community. Zweck des Dokuments ist es, die verschiedenen Komponenten und deren Funktionen zu beschreiben. Dieses Dokument ist die Basis für technische, organisatorische und semantische Spezifikation. Das Rahmenkonzept definiert eine möglichst generische Plattform, an die sich sowohl Lösungsanbieter wie auch Register, Organisationen und weitere Quellen als Datenlieferanten einfach anbinden können. Es soll ausserdem als Modell dazu dienen, möglichst viele ‚use cases', Anforderungen und mögliche Kommunikationsprotokolle abzubilden.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Status des Dokuments

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

2 Einleitung

Sämtliche Formulierungen beziehen sich auf Angehörige beider Geschlechter.

2.1 Einordnung

Die Vision der Vernetzten Verwaltung in eCH-0126 und die damit verbundenen übergreifenden Prozesse im schweizerischen E-Government rufen nach einer behördenübergreifenden Identitäts- und Berechtigungsverwaltung (IAM). eCH-0107 beschreibt dieses föderierte IAM und definiert Prinzipien, Regeln und den Ordnungsrahmen für die IAM-Systemgestaltung. SuisseTrustIAM bildet ein Konzept für föderiertes Identity und Access Management ab und ist so als mögliche Lösungsvariante zu verstehen. Neben SuisseTrustIAM bestehen weitere föderierte IAM-Konzepte (beispielsweise SWITCH-aai)

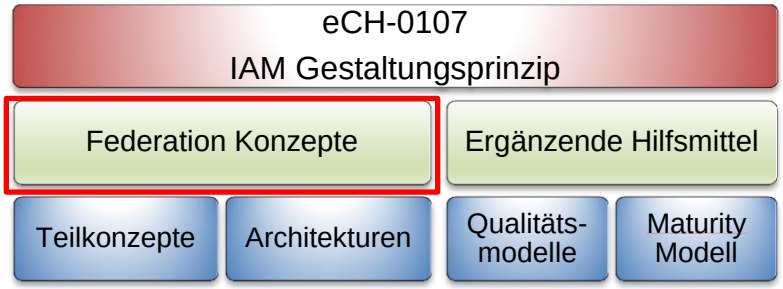

Abbildung 1 Einordnung Standardisierungs-Framework

2.2 Anwendungsgebiet

SuisseTrustIAM soll schweizweit generische Identity & Access Management-Services für E-Government, E-Health, E-Education sowie für die E-Economy zur Verfügung stellen. Als wichtigste und innovativste Funktionalität wird eine Vermittlerinfrastruktur definiert. Sie ermöglicht einen qualifizierten Nachweis von Attributen (Rolle) via Register oder Verzeichnis für ein authentifiziertes Subjekt (repräsentiert durch eine eIdentity) einer Unternehmung oder Organisation, einschliesslich der Nachverfolgbarkeit.

2.3 Vorteile

Das Rahmenkonzept definiert eine möglichst generische Plattform, an die sich sowohl Informationskonsumenten wie auch Informationslieferanten (primär Register, Organisationen und weitere Quellen) einfach anbinden können. Damit soll verhindert werden, dass für verschiedene Services jeweils spezifische Lösungen erarbeitet werden müssen. Dieses Rahmenkonzept soll ausserdem als Modell dazu dienen, möglichst viele ‚use cases', Anforderungen und mögliche Kommunikationsprotokolle abzubilden.

2.4 Inhaltlicher Schwerpunkt

Dieses Dokument beschreibt die Basis-Funktionsweise der gesamten SuisseTrustIAM-Community. Zweck des Rahmenkonzepts ist es, die verschiedenen Komponenten und deren Funktionen zu beschreiben. Es dient als Basis für die technische, organisatorische und semantische Spezifikation.

3 Konzept SuisseTrustIAM

Ziel der gesamten Lösung ist es, Authentifikations- und Attributinformationen von Informationslieferanten (Authentifikation- und Attribut-Autoritäten) über die Vermittlerinfrastruktur (STIAM-Plattform) an Informationskonsumenten weiterzugeben.

Die SuisseTrustIAM-Community mit ihren Teilnehmern kann grob in 3 Kategorien unterteilt werden:

- Informationskonsumenten (Relying Party)
- Informationslieferanten
  - Authentifikation- und Attribut-Autoritäten
- Vermittlerinfrastruktur

In Abbildung 1 wird die STIAM-Grobstruktur graphisch dargestellt. Das Gesamtsystem ist in vier Teile (farblich unterschieden) aufgeteilt, um eine Abgrenzung der Funktionen zu verdeutlichen. Dabei werden Informationslieferanten in Authentifikation- und Attribut-Autoritäten unterteilt.

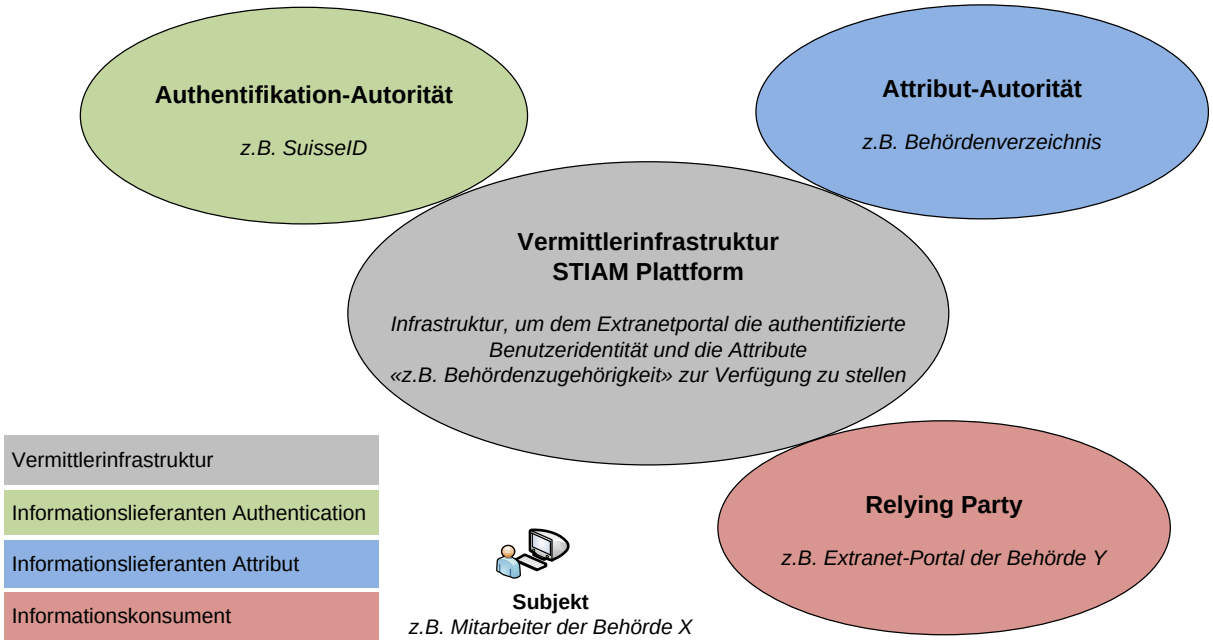

Abbildung 2 Grobstruktur STIAM

Zentraler Bereich der STIAM-Plattform ist der STIAM-Broker, der die Vermittlerinfrastruktur bereitstellt. Angebunden an den STIAM-Broker sind die Informationskonsumenten (Relying Parties) und Informationslieferanten (Authentifikation- und Attribut-Autoritäten). Der STIAM-

Sender ist die standardisierte Schnittstelle zu Attribut-Autoritäten (in der Regel Verzeichnisse und Register). Ein spezielle Attribut-Autorität ist das ‚User Data Repository', das in Kapitel 5.4 näher beschrieben wird. Der STIAM-Empfänger realisiert die standardisierte Schnittstelle zu einer Relying Party (beispielsweise ein Portal) mit verschiedenen Applikationen und Services. Mit Authentifikation-Autoritäten, beispielsweise der SuisseID, werden externe Authentifikationsanbieter bezeichnet, die von der STIAM-Plattform unterstützt werden und als vertrauenswürdig gelten.

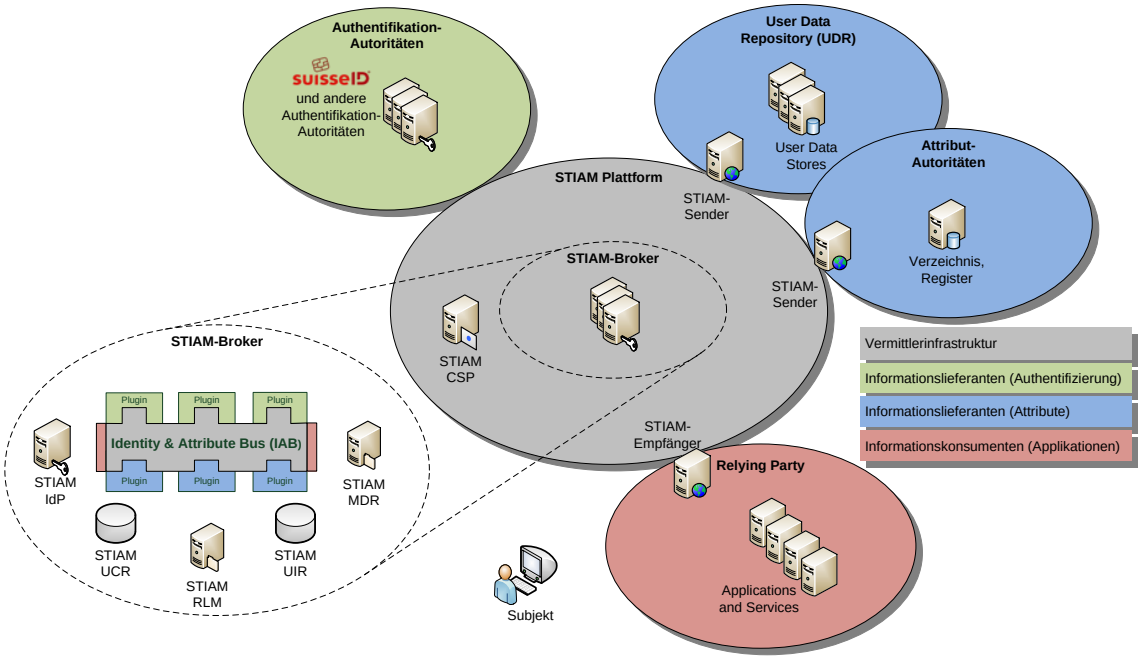

Abbildung 3 Komponenten STIAM

Eine Organisation (beispielsweise eine Firma oder ein E-Government-Dienst), die die STIAM-Plattform nutzen will, kann einzelne oder mehrere Rollen in diesem Gesamtsystem einnehmen. Sie kann entweder ausschliesslich die Rolle eines Informationskonsumenten bekleiden oder zusätzlich die Rolle eines Informationslieferanten übernehmen.

3.1 Abgrenzung STIAM- Broker, -Plattform, -Community

In diesem Konzept werden die Begriffe STIAM-Broker, STIAM-Plattform und STIAM-Community folgendermassen verwendet:

STIAM-Broker
Der STIAM-Broker beinhaltet die Basisdienste, die die zentrale Vermittlerinfrastruktur der STIAM-Plattform bilden (siehe Kapitel 5.1).

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

STIAM-Community
Die STIAM-Community bilden alle Teilnehmer, die mit der STIAM-Plattform interagieren und die einheitliche Spezifikation berücksichtigen.

4 Rahmenarchitektur

4.1 Architekturprinzipien

Architekturprinzipien werden als 'best practice' verstanden.

- MUST: Der STIAM-Broker kennt die angebunden Authentifikation- und Attribut-Autoritäten und nimmt damit für eine Relying Party (STIAM-Empfänger) eine Authentifikations- und Attributvermittlerrolle ein.
- MUST: Der STIAM-Broker agiert als Vermittler von eIdentities mit ihren Attributen. Er unterhält ein User Identifier Repository (STIAM-UIR), um Identifikatoren und Links zu externen Authentifikation-Autoritäten bereitzustellen.
- MUST: Die STIAM-Plattform speichert ausschliesslich Daten, die für den Betrieb und Support zwingend notwendig sind.
- MUST: Daten, die ein Subjekt selbst auf der Plattform eingetragen hat, werden in einem logisch vom STIAM-Broker getrennten User Data Repository gespeichert.
- MUST: Die STIAM-Plattform gewährleistet die Privacy ihrer Subjekte.
- MUST: Attribut-Autoritäten werden über einen standardisierten STIAM-Sender angeschlossen.
- MUST: Die Relying Party (STIAM-Empfänger) kommuniziert nur mit dem STIAM-Broker. Es gibt keine direkte Kommunikation zwischen dem STIAM-Empfänger und anderen Komponenten (Authentifikation- & Attribut-Autorität anderer Domänen oder STIAM-Sender).
- SHOULD: Die SuisseID-Infrastruktur kann durch die STIAM-Plattform sowohl als Authentifikation- wie auch als Attribut-Autorität integriert werden.
- SHOULD: Die Einbindung eines STIAM-Empfängers und STIAM-Senders ist einfach konfigurierbar.
- SHOULD: Vom STIAM-Broker vermittelte Attribute und Authentifikationen weisen standardisierte Qualitätswerte auf. Der STIAM-Empfänger kann die Qualitätswerte auswerten.
- SHOULD: Innerhalb der STIAM-Plattform vertrauen sich die Komponenten.
- MUST: Der STIAM-Broker authentifiziert STIAM-Empfänger und STIAM-Sender.
- SHOULD: Die STIAM-Plattform setzt auf bestehenden Standard-Protokollen auf und kann diese, wenn notwendig, in standardisierter Form erweitern.
- SHOULD: Die STIAM-Komponenten sind mandantenfähig.
-

5 Komponentenübersicht

In diesem Kapitel werden die im STIAM-Rahmenkonzept verwendeten Komponenten beschrieben.

5.1 STIAM-Broker

Der STIAM-Broker ist die zentrale Vermittlerinfrastruktur zwischen Relying Parties, Subjekten, Attribut-Autoritäten als Datenlieferanten und Authentifikation-Autoritäten anderer Domains. Er besteht aus dem Identity and Attribute Bus, STIAM-RLM, STIAM-MDR, STIAM-IdP und unterhält das User Identifier Repository mit den Identifikator-Daten und das User Credential Repository mit den Credential-Daten. Alle weiteren Daten werden von den registrierten Attribut-Autoritäten (AA) bei Bedarf bereitgestellt.

5.1.1 Identity and Attribute Bus

Der Identity and Attribute Bus kontrolliert interne Authentifikationsmethoden und vermittelt, wenn notwendig, Authentifikationsvorgänge mit externen Authentifikation-Autoritäten. Der Identity and Attribute Bus stellt Schnittstellen zu Authentifikation-Autoritäten (z.B. MobileID, SuisseID) via PlugIns zur Verfügung. Damit können Abfragen bei Extended SuisseID IdP's und SuisseID Claim Assertion Services (CAS) gemacht werden.

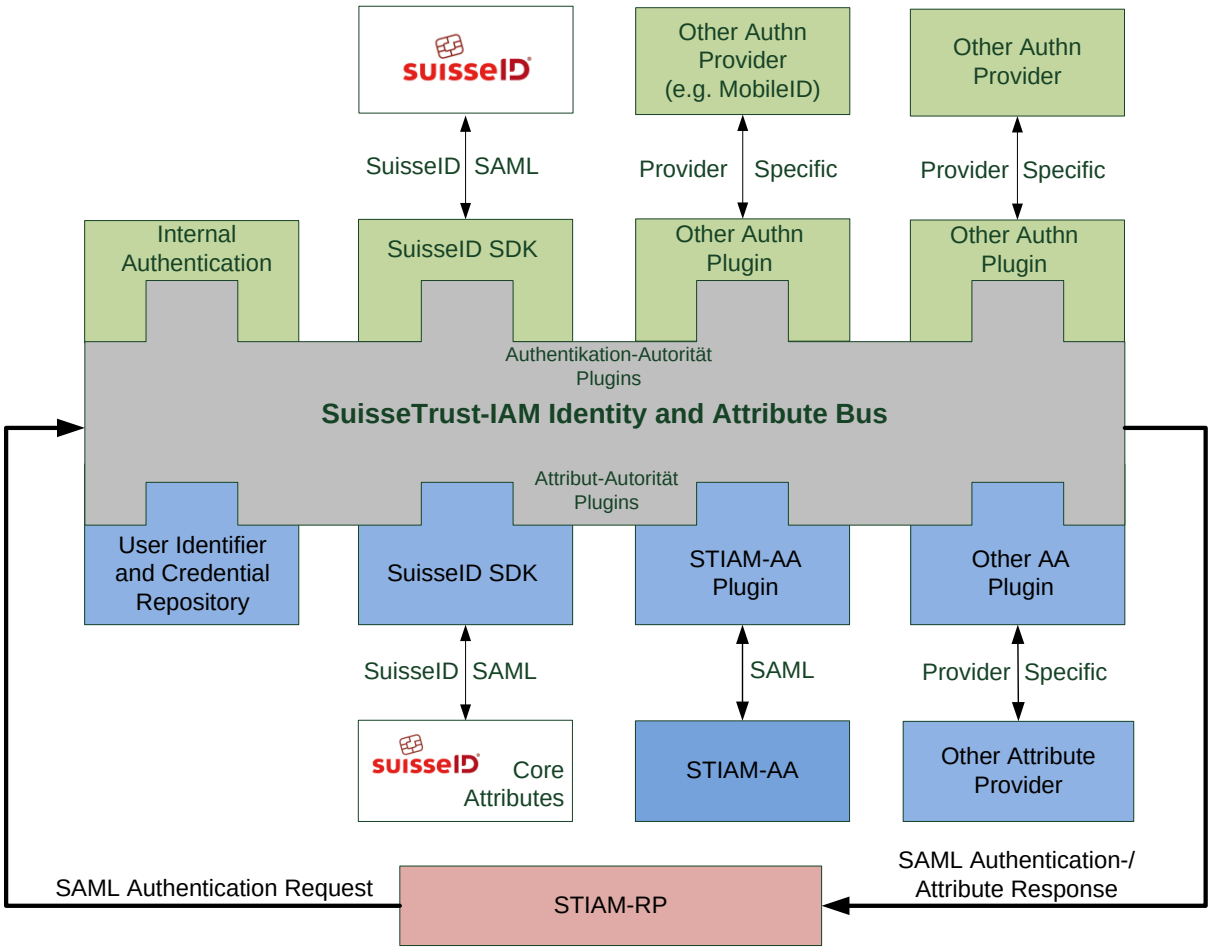

Abbildung 4 STIAM Identity and Attribute Bus

5.1.2 STIAM-IdP (Identity Provider)

Über den STIAM-IdP (Identity Provider) werden Subjekte authentifiziert. Die Authentifikation findet entweder lokal über das STIAM-UCR oder über eine externe Authentifikation-Autorität statt. Der STIAM-IdP benutzt zur externen Authentifikation das entsprechende IdP-Plugin des Identity und Attribute Bus.

5.1.3 STIAM-UIR (User Identifier Repository)

Jedes Subjekt hat auf der STIAM-Plattform einen eindeutigen Account mit einer GUID (Global Unique Identifier). An diese GUID ist das User Identifier Repository gekoppelt, in dem die externen Identifikator-Definitionen zu AA-Ressourcen verwaltet werden. Dies ermöglicht dem Subjekt über den STIAM-Broker, Daten aus einer Attribut-Autorität mit seinem Account zu

verbinden. Die Kennung, die im STIAM-UIR abgelegt wird, ist der Identifikator, der während dem Subjekt-Validierungsprozess von einem STIAM-Sender an den Broker übermittelt wird.

Meta-Attribut	Identifikator	AA
<Anwaltsberechtigung>	1234.5678.8910.1112	Anwaltsregister URI
<Stimmberechtigung>	234.234-324	Stimmregister Winterthur URI
<Unternehmenszugehörigkeit>	67889054123	Berner Fachhochschule AA URI
<Name>	STIAM-0001-0002-0003-0004	STIAM-UDR URI

Tabelle 1 Beispiel STIAM-UIR

5.1.4 STIAM-UCR (User Credential Repository)

Ebenfalls an die GUID ist das User Credential Repository gekoppelt, das pro Subjekt die Identifikatoren der Credentials und deren Quelle enthält. Dies ermöglicht dem STIAM-IdP, das Subjekt intern zu authentifizieren oder extern authentifizieren zu lassen.

Credentialtyp	Identifikator	Authentifikation-Autorität Quelle
<MobileID>	1234.5678.8910.1112	MobileID URI
<internal U/PW>	peter.muster	Internal
<BFH-ID>	mustepet	Berner Fachhochschule AuthnA URI
<SuisseID>	0001-0002-0003-0004	CoreIdP URI

Tabelle 2 Beispiel STIAM-UCR

5.1.5 STIAM-MDR (Metadata Registry)

Metadaten sind spezielle XML-Dokumente, welche alle notwendigen Informationen von Entitäten (Informationskonsumenten, Informationslieferanten) enthalten. Durch diese Metadaten können aus technischer Sicht Vertrauensbeziehungen zwischen diesen Entitäten innerhalb einer Community aufgebaut werden. Die STIAM-MDR ist ein zentraler Auskunftsdienst, welcher die Metadaten der Community für die STIAM-Plattform verwaltet und zur Verfügung stellt.

5.1.6 STIAM-RLM (Reporting, Logging und Monitoring)

Mit dem STIAM-RLM werden alle Vorgänge, welche vom STIAM-Broker vermittelt werden, im Sinne der zu erfüllenden Compliance geloggt und überwacht.

5.2 Relying Party (RP)

Die Relying Party bietet eine Dienstleistung in Form eines Webservices an, welche die Zugriffskontrolle über SuisseTrustIAM realisiert.

5.2.1 STIAM-Empfänger

Die von der Relying Party angebotene Ressource kommuniziert über den STIAM-Empfänger mit dem STIAM-Broker. Die Relying Party definiert, welche Attribute in welcher Qualität notwendig sind, um Zugriff auf eine geschützte Ressource zu erlauben. Um die Ressource zu nutzen, muss sich ein Subjekt beim STIAM-Broker authentifizieren und die von der Relying Party geforderten Attribute in entsprechender Qualität an den STIAM-Empfänger liefern.

5.3 Attribut-Autorität (AA)

Eine Attribut-Autorität ist eine Organisation oder ein Register, die bzw. das als Informationslieferant Attribute für die STIAM-Community bereitstellt.

5.3.1 STIAM-Sender

Über einen STIAM-Sender ist ein Verzeichnis an die STIAM-Plattform angebunden. Der STIAM-Sender ist als Kommunikationsmodul konzipiert, der die standardisierte SAML-Kommunikation zwischen der Attribut-Autorität und dem STIAM-Broker realisiert. Er ist möglichst einfach aufgebaut und kann Attribute aus unterschiedlichen Datenquellen (LDAP, SQL, etc.) beziehen.

5.4 STIAM-UDR (User Data Repository)

Das STIAM User Data Repository ist der spezifische Attributspeicher eines Subjekts. Darin werden alle subjektspezifischen Attribute verwaltet, die nicht von einer externen Attribut-Autorität bereitgestellt sind. Das STIAM User Data Repository verwaltet analog einer Attribut-Autorität die vom Subjekt selber eingebrachten Attribute. Das Subjekt pflegt seine Daten direkt über einen Service, der als STIAM-Empfänger konzipiert ist. Die Daten sind nicht Teil der STIAM-Plattform und sind von der STIAM-Plattform logisch getrennt. Durch die Trennung von STIAM-UDR und STIAM-UIR sollen Profiling und Datennachverfolgbarkeit durch den STIAM-Broker verhindert bzw. erschwert und der Schutz der subjektspezifischen Daten erhöht werden.

5.5 STIAM-CSP (Certification Service Provider)

Der STIAM–CSP stellt den Trust-Anchor und Certificate Issuer für die gesamte STIAM-Plattform dar. Implizit vertraut jedes Mitglied der STIAM-Plattform dieser Komponente.

6 Metadaten und Circle of Trust

Ein Circle of Trust (COT) stellt eine Menge von Relying Parties, Attribut-Autoritäten und mindestens einem Identity-Provider dar. In einem COT vertrauen sich diese Komponenten auf unterschiedlichen Ebenen. Um einen COT zu erstellen, müssen für diese Provider bestimmte Informationen in Form von Entitätsmetadaten erfasst und so publiziert werden, dass jedes Mitglied des COT die Authentizität und Integrität dieser Informationen überprüfen kann.

6.1 Rolle der STIAM-MDR

In der STIAM-Community hat jedes Mitglied (Informationslieferant, Vermittlerinfrastruktur und Informationskonsument) eine bestimmte Rolle. Notwendige Informationen zu dieser Funktion werden in den Entitätsmetadaten abgelegt. Diese enthalten unter anderem Informationen über:

- die Adresse und den Namen der Entität,
- die Endpunktkonfigurationen der Entität (URL),
- die Public-Key-Zertifikate für die Prüfung der digital signierten Nachrichten (Assertion) einer Entität.

In grösseren und komplexeren Umgebungen wird die Verwaltung dieser Entitätsmetadaten zentral durch einen dedizierten Service durchgeführt. Das vorliegende Konzept sieht dafür den STIAM-MDR Dienst vor. Dieser Dienst verwaltet und signiert die Entitätsmetadaten der Mitglieder zentral und publiziert sie in Form einer Community-Metadaten-Datei. Auf diese Weise können Informationen durch die Mitglieder der Community über andere Entitäten gefunden und überprüft werden.

Die STIAM-MDR bietet ein zentrales Verzeichnis aller notwendigen Informationen der Broker-, STIAM-Sender und STIAM-Empfänger. Diese Datei wird periodisch bzw. nach jeder Änderung von der STIAM-MDR neu signiert. Zur Signatur verwendet die STIAM-MDR ein von der STIAM-CSP ausgestelltes Zertifikat, das von allen Komponenten in der STIAM Umgebung als vertrauenswürdig anerkannt wird.

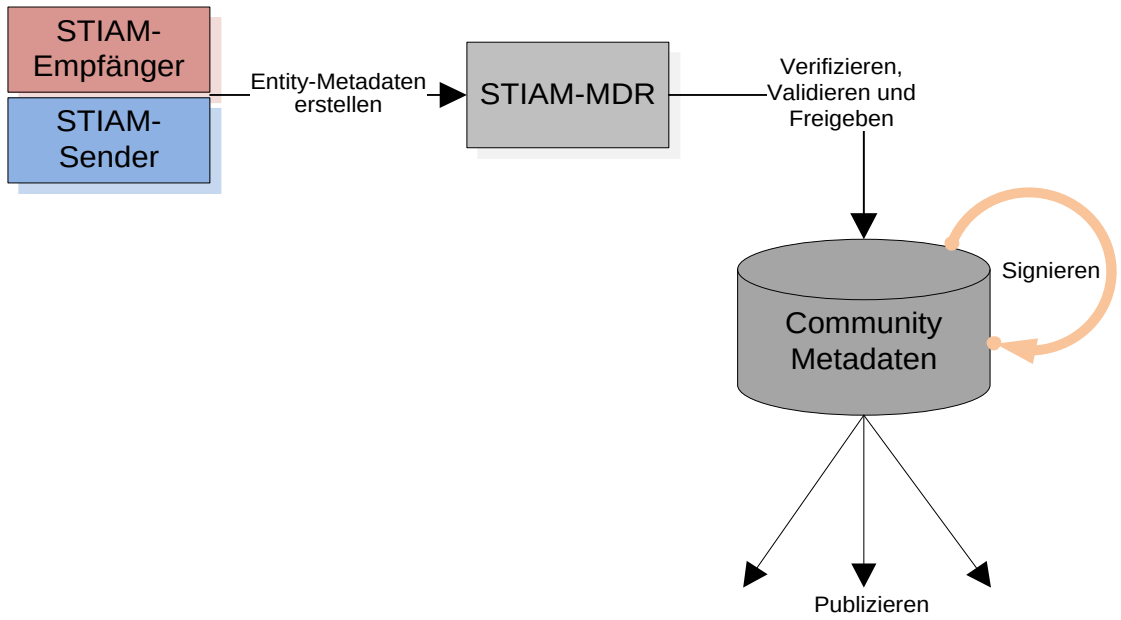

Abbildung 5 Funktion STIAM-MDR

Zur Registrierung in der STIAM-Plattform muss der Verantwortliche einer Organisation die Entitätsmetadaten seines STIAM-Senders oder STIAM-Empfängers erstellen (dies kann lokal oder direkt über eine Webapplikation auf der MDR erfolgen). Diese werden anschliessend im Rahmen eines Registrierungsprozesses auf Syntax, Inhalt und Berechtigung geprüft.

- Bei einem STIAM-Sender werden in den Entitätsmetadaten zusätzlich die Attribute angegeben, die vom Datenlieferanten angeboten werden sollen. Die Prüfung der angegebenen Attribute und deren Qualitätseinstufung erfolgen zur Definitionszeit im Rahmen des Registrierungsprozesses.
- Bei einem STIAM-Empfänger werden in den Entitätsmetadaten zusätzlich die für die Zugangsberechtigung erforderlichen Attribute angegeben. Auch hier müssen im Rahmen des Registrierungsprozesses die Angaben anhand vorliegender Richtlinien geprüft werden.

Nach erfolgreicher Überprüfung werden die Entitätsmetadaten des neuen Mitglieds von der MDR in die Community Metadaten integriert. Anschliessend wird diese signiert und publiziert.

6.2 Circle of Trust und STIAM-CSP

Wie im vorherigen Kapitel beschrieben, vertrauen sich die Mitglieder der STIAM-Plattform über einen Circle of Trust. Die Vertrauensbeziehungen zwischen den STIAM-Komponenten basieren auf X.509-Zertifikaten, die für unterschiedliche Anwendungen verwendet werden.

- SSL-Zertifikate werden verwendet, um die Kommunikation zwischen Webserver und -services abzusichern;
- Zertifikate, um beispielsweise SAML-Assertions zu signieren bzw. zu verschlüsseln;
- Zertifikate, um die Community Metadaten zu signieren.

Diese Zertifikate müssen von einem Certification Service Provider (CSP) ausgestellt werden, dem alle STIAM-Plattform-Komponenten vertrauen.

7 Szenario

Voraussetzung für die folgenden Szenarien ist eine erfolgte Registrierung des STIAM-Empfängers und des STIAM-Senders beim STIAM-Broker, sprich bei der STIAM-MDR (siehe 5.1.5).

Der Informationslieferant (STIAM-Sender) wird aufgrund der Attribut-Qualitätsanforderungen des Informationsbezügers (STIAM-Empfänger) definiert. Die Identifizierungsmethode wird ihrerseits durch den Qualitätsanspruch an die Authentisierung des Subjekts (Authentifikationsqualität) der jeweiligen Informationslieferanten (STIAM-Sender) definiert.

Grundszenario

In allen Szenarien ruft ein Subjekt einen Service einer Relying Party auf und wird zum STIAM-Broker weitergeleitet. Zuhanden des STIAM-Empfängers werden die geforderten Attribute vom STIAM-Broker zusammengetragen und übermittelt. Dabei können die Authentifikation und die Attribut-Assertion auf verschiedene Weise geschehen.

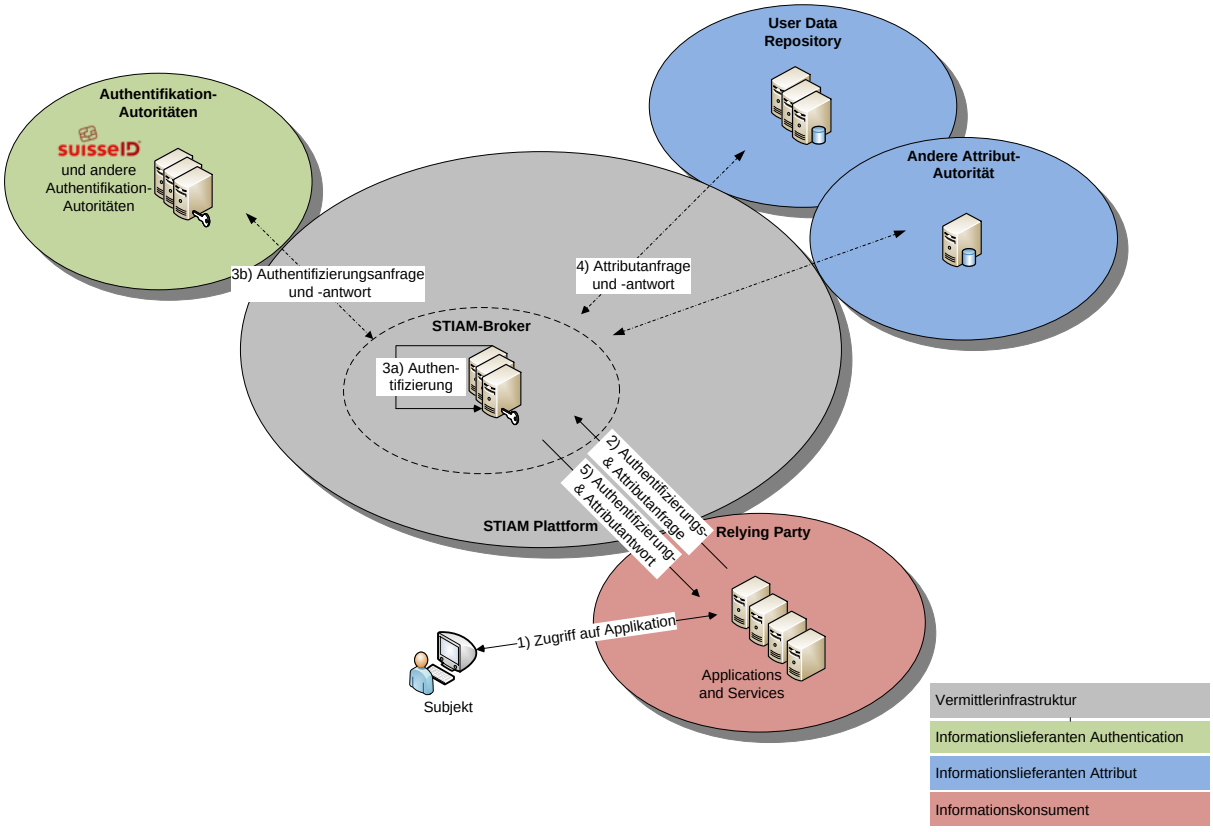

Abbildung 6 Szenario

8 Qualitätsmodell

Im Kontext von SuisseTrustIAM sind zwei Qualitäten von Bedeutung. Zum einen interessiert die Qualität eines identifizierten Subjekts (Authentifikationsqualität), daneben aber auch die Qualität der Attribut-Assertions (Attributqualität) zum Subjekt. Die Authentifikations- und Attributqualität können unterschiedliche Werte aufweisen.

8.1 Anforderungen

- MUST: Die Relying Party definiert beim STIAM-Broker den Qualitätswert der Authentifikation eines Subjekts.
- MUST: Die Relying Party definiert beim STIAM-Broker den Qualitätswert eines geforderten Attributs.
- SHOULD: Der STIAM-Broker kann in der Attribute Response den effektiven Qualitätswert eines Attributs an die Relying Party übergeben.
- MUST: Attribute Assertions werden durch den STIAM-Sender signiert.
- SHOULD: Die Relying Party kann die Attribut-Autorität eines Attribute Assertions selbst verifizieren.
- SHOULD: Das gesamte STIAM-Qualitätsmodell orientiert sich an ISO29115 QAA.
- MUST: Die Authentifikationsqualität in SuisseTrustIAM wird analog dem ISO29115-Standard definiert.
- MUST: Die Qualitätswerte liegen zwischen 1 und 4. Level 4 ist die höchstmögliche Qualität, Level 1 hingegen die tiefste.

9 Sicherheitsüberlegungen

Der Datenschutz in STIAM orientiert sich an den aktuellen Entwicklungen europäischer Projekte[1].

9.1 Datenschutz mit technischen Mitteln

Das STIAM-Konzept folgt zur Einhaltung der Datenschutzrichtlinien dem Grundsatz „Datenschutz wird, wo möglich, mit technischen Mitteln und organisatorischen Regeln durchgesetzt und wo immer notwendig mit rechtlichen Mitteln ergänzt“.

In einem IAM wird eine vollständige Anonymisierung der Subjekte nie möglich sein. Die STIAM-Plattform fokussiert deshalb stark auf Pseudonymisierung.

- MUST: Die STIAM-Plattform schränkt die Verarbeitung personenbezogener Daten auf ein notwendiges Minimum ein.
- SHOULD: Die STIAM-Plattform verzichtet auf die Verwendung sprechender Identifikatoren.
- SHOULD: Die STIAM-Plattform setzt Pseudonyme als Identifikatoren ein.
- SHOULD: Die STIAM-Plattform verzichtet auf eineindeutige Identifikatoren.
- MUST: Die STIAM-Plattform verhindert oder erschwert die Verknüpfung der Identifikatoren, deren Verwendungszwecke und der personenbezogenen Daten.
- MUST: Die STIAM-Plattform löscht bestehende Verknüpfungen oder Korrelationen zwischen eIdentity und Identifikator, die nicht oder nicht länger für die Verarbeitung der Daten benötigt werden.
- MUST: Die STIAM-Plattform schränkt die Identifizierbarkeit der Subjekte auf ein notwendiges Minimum ein.[2]
- MUST: Die STIAM-Plattform speichert personenbezogene Daten logisch getrennt.

9.2 Verschlüsselung der Assertions

Optional ist im STIAM-Konzept auch die direkte Verschlüsselung der Attribute in der verschachtelten Assertion möglich. Damit kann ein vertraulicher Austausch von Attributwerten zwischen Attribut-Autorität und Relying Party ermöglicht werden. Dies hat aber zur Folge, dass die Werte der geforderten Attribute dem Subjekt nur vor der Verschlüsselung durch den STIAM-Sender zur Freigabe präsentiert werden können.

9.3 Benutzerzentriertheit und Interaktionen des Subjekts

Die STIAM-Plattform hat die Möglichkeit, als Datendrehscheibe für Identitätsdaten und weitere private Informationen eines Subjekts zu dienen. Auf der anderen Seite sollen über denselben Dienst auch Informationen ausgetauscht werden können, die das Subjekt in seiner Be-

[1] Insbesondere TURBINE (TrUsted Revocable Biometric IdeNtitiEs (2008) D1.4.1 Legal Issues of Identity Management Schemes), STORK1 (Secure IdenTity AcrOss BoRders LinKed (2009) D2.2 Report on Legal Interoperability) und TDL (Trust in Digital Life (2012) Architecture serving complex Identity Infrastructures).

[2] Vgl. TURBINE, 47.

ziehung zu einem Unternehmen, einer Organisation oder einer öffentlichen Funktion darstellt.

9.3.1 Natürliche Subjekte

Im ersten Fall gehören angeforderte Informationen (insb. Identitätsdaten) dem Individuum (z.B. hans.muster@facebook.com). Demzufolge muss dieses auch über die Weitergabe selbst entscheiden können (Attribut Stop-Schirm) und die Kommunikation erfolgt ausschliesslich benutzerzentriert über den Browser des Benutzers.

Im zweiten Fall geht es auch um Identitätsdaten, die aber (in der Regel) einer Organisation gehören, zu der der Benutzer in Beziehung steht (z.B. hans.muster@unternehmen.ch). Die Organisation entscheidet im Rahmen geltender Gesetze und Verträge über die Weitergabe dieser Daten an Dritte. Der einzelne Mitarbeiter muss im Rahmen dieser Entscheidung als Individuum nicht beipflichten. Aus diesem Grund ist auch keine benutzerzentrierte Kommunikation notwendig. Dies ermöglicht eine direkte Kommunikation zwischen Relying Party und Broker.

9.3.2 Service-Subjekte

Die STIAM-Plattform adressiert auch Services. Services-Subjekte unterscheiden sich speziell zur Laufzeit. Technische Subjekte werden vorwiegend eingesetzt, um optimierte Prozessabläufe zu realisieren. Deshalb macht es hier wenig Sinn, benutzerzentrierte Kommunikationsabläufe zu verfolgen. Alle Registrierungsprozesse werden jedoch von natürlichen Subjekten in Stellvertretung wahrgenommen.

Die STIAM-Plattform muss alle Szenarien berücksichtigen und standardisieren. Für die direkte, nicht benutzerzentrierte Kommunikation werden ausserhalb dieses Rahmenkonzepts zusätzliche Konzepte evaluiert. Ein vielversprechender Ansatz ist die ‚Backend Attribute Exchange' (BAE)[3] Spezifikation des US Federal ‚Identity, Credential and Access Management' (ICAM).

[3] Siehe:
http://www.idmanagement.gov/documents/BAE_v2_Overview_Document_Final_v1.0.0.pdf
http://www.idmanagement.gov/documents/BAE_v2_SAML2_Profile_Final_v1.0.0.pdf
http://www.idmanagement.gov/documents/BAE_v2_SAML2_Metadata_Profile_Final_v1.0.0.pdf
http://www.idmanagement.gov/documents/BAE_v2_Governance_Document_Final_v1.0.0.pdf

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 Subjekts, sich die allenfalls erforderlichen Rechte bei dem jeweils berechtigten Subjekt (Maschine, Person, Organisation) 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 & Bibliographie

[eCH-0107] eCH Fachgruppe IAM. eCH-0107 Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM). Version 2.0.

Anhang B – Mitarbeit & Überprüfung

Review	Hans Häni, Kanton Thurgau, B2.06
	Enno Hoffmann, Atos
	Steff Schnetzler, iWeb
	Patrick Graber, Swisscom
	Konrad Walser, Berner Fachhochschule
	Andreas Spichiger, Berner Fachhochschule
	Daniel Leiser, Atos
	Annett Laube-Rosenpflanzer, Berner Fachhochschule

Anhang C – Abkürzungen

AA	Attribut-Autorität
AuthnA	Authentifikation-Autorität
BAE	Backend Attribute Exchange
CAS	Claim Assertion Service
COT	Circle of Trust
CSP	Certification Service Provider
QAA	Quality of Authentication Assurance Levels
IAM	Identity und Access Management
IdP	Identity Provider
LDAP	Lightweight Directory Access Protocol
MDR	Metadata Registry
RP	Relying Party
RLM	Reporting-Logging-Monitoring
SAML	Security Assertion Markup Language
STIAM	SuisseTrustIAM
STORK	Secure IdenTity AcrOss BoRders LinKed

UCR	User Credential Repository
UDR	Userdata Repository
UIR	User Identifier Repository
XML	Extensible Markup Language

Anhang D – Glossar

Begriff	Definition
Assertion	Siehe *Authentication Assertion* oder *Attribute Assertion* [eCH-0107]
Attribut	Semantisches Abbild einer einem Subjekt zugeordneten Eigenschaft, die das Subjekt näher beschreibt. Der Identifikator und die Credentials sind ebenfalls Attribute. [eCH-0107] Jedes Attribut ist in einem Schema (Metaattribut) beschrieben und weist einen Attributwert auf.
Attribute Assertion	Bestätigung eines *Attributes* durch eine *Attribute Authority*. Entspricht einer SAML 2.0 Attribute Assertion [eCH-0107].
Attribut-Autorität (AA)	Eine Attribut-Autorität ist ein *Register* oder sonstiges *Verzeichnis* mit einem *Attribute Service* zur Pflege von Attributen und einem *Attribute Assertion Service* zur Ausstellung von *Attribute Assertions*. [eCH-0107] Informationslieferant, der über eine definierte Schnittstelle (STIAM-Sender) Attribute für die STIAM-Community bereitstellt.
Attribute Broker	Siehe STIAM-Broker
Attribute-Based Access Control (ABAC)	Konzept dynamischer Zuteilung von Zugriffsrechten basierend auf Attributen des Subjekts.
Auditing	a) Überprüfung der Policy-Konformität. b) Aufzeichnung aller Aktionen und Entscheide zur Gewähr-leistung der Nachvollziehbarkeit. [eCH-0107]
Authentication Authority	Eine technische *Entität* (Service), die Authentifikation als Dienstleistung anbietet und *Authentication Assertions* für *Subjekte* ausstellt. [eCH-0107]
Authentifikation-Autorität (AuthnA)	Eine AuthnA stellt einen *Authentication Service* zur Verfügung, gegen den sich das *Subjekt* authentifizieren kann. Der Authentication Service benutzt Credentials, die von einem *Credential Service* ausgestellt werden. Der Credential Service kann ein Bestandteil der AuthnA sein. Beispiele für Authentifikation-Autoritäten sind IdPs (nach SAML), OpenID Provider und MobilID Provider. [eCH-0107]
Authentication Proxy	Ist AuthnA(1) nicht in der Lage, einen Nutzer zu authentifizieren, kann er unter bestimmten Umständen als Authentication Proxy agieren, indem er selber einen eigenen Authentication Request an einen weiteren AuthnA sendet. Die Antwort vom AuthnA(2) kann der AuthnA(1) dann dazu verwenden, eine eigene Response zu generieren. Die Authentication Proxy Funktion wird im SAMLv2 Standard beschrieben und weitgehend definiert, heisst dort Identification Proxy.

Authentifikation	Vorgang der Überprüfung einer behaupteten *digitalen Identität.* Synonym: Authentifizierung. [eCH-0107]
Authentisierung	Nachweis der eigenen *digitalen Identität* eines *Subjekts*. [eCH-0107]
Authentifizierungsmerkmal	Das Authentifizierungsmerkmal kann auf Wissen (Passwort, PIN), auf Besitz (Zertifikat, privater Schlüssel) oder auf einer Eigenschaft (biometrisches Merkmal z.B. Stimme, Irisbild, Fingerabdruck) oder auf einer Kombination dieser Merkmale basieren. [eCH-0107]
Backend Attribute Exchange (BAE)	Attributabfrage im Hintergrund, üblicherweise durch eine Maschine. Ein Benutzer ist bei der Attributabfrage nicht direkt involviert, diese erfolgt ohne seine explizite Zustimmung.
Autorisierung	a) Administration: Definition der Zugangsregeln und Zugriffsrechte auf eine *eRessource*. b) Zur Laufzeit: Prüfen von Zugriffsberechtigung eines authentifizierten *Subjektes* auf eine *Ressource* und erteilen des Zugriffs zur Laufzeit. Dabei wird zwischen *Grob*- und *Feinautorisierung* unterschieden. [eCH-0107]
Benutzer	Menschliches Subjekt [eCH-0107]
Benutzerzentriertes Identitätsmanagement	Ermöglicht dem Benutzer die Auswahl spezifischer Credentials und Attribute zur Bearbeitung in Authentifikations- und Attribut-Anfragen und überlässt ihm so die Kontrolle über die eigene, digitale Identität. Das bedeutet nicht, dass der Benutzer jede Transaktion nochmals explizit genehmigen muss, aber dass die Daten immer durch die Identitätsverwaltung des Benutzers fliessen und direkt an seine digitale Identität gebunden sind.
Berechtigung	Recht eines Subjekts, bestimmte Ressourcen zu nutzen [eCH-0107]
Bearbeiten	Jeder Umgang mit Daten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten (kurz: Erstellen, Lesen, Verändern, Löschen, Übermitteln) von Daten.
Certification Authority (CA)	Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck digitale Zertifikate ausstellt. Synonym: Certification Service Providers (CSP) [eCH-0107]
Certification Service Provider (CSP)	Siehe Certification Authority (CA) [eCH-0107]
Circle of Trust (CoT)	Eine Menge von RP, AA und mindestens einer AuthnA, deren technischen und organisatorischen Komponenten sich auf unterschiedlichen Ebenen vertrauen.
Claim	Der Begriff Claim wurde in diesem Dokument explizit nicht verwendet, da verschiedene, einander z.T. widersprechende Bedeutungen existieren. Es wird empfohlen, den Begriff deshalb zu vermeiden. [eCH-0107]
Claim Assertion Service (CAS)	Der Claim Assertion Service ist ein spezielle *Attribute Authority*. Seine Aufgabe besteht darin, dem Benutzer zu erlauben, Eigenschaften, welche ihm von einer Organisation oder Register zugeteilt wurden, zu bestätigen. [eCH-0107]
Client	Technische Einrichtung (Anwendung, Webbrowser etc.), mit der das Subjekt auf die Ressource zugreift.

Community Metadaten	Signierter Zusammenzug von Entitätsmetadaten der Mitglieder einer STIAM-Community.
Credential	Nachweis zur Bestätigung einer *Identität* eines *Subjekts*. Im IAM-Kontext wird zur Bestätigung einer digitalen Identität eine Benutzerkennung (Identifikator) in Verbindung mit einem mit einem (oder mehreren) Authentifizierungsmerkmal(en) verwendet. Synonym: Identitätsnachweis [eCH-0107]
Datenlieferant	Siehe AA
Digitale Identität / Digital Identity / eIdentity	Repräsentation eines Subjekts. Eine digitale Identität (eIdentity) hat einen Identifikator (eindeutiger Name), meist zusammen mit einer Menge von zusätzlichen Attributen, welche innerhalb eines Namensraumes eindeutig einem Subjekt zugewiesen werden können. Ein Subjekt kann mehrere digitale Identitäten haben. [eCH-0107]
Digitales Zertifikat	Strukturierte Daten, die den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels bestätigen (auch Zertifikat oder Public-Key-Zertifikat). [eCH-0107]
Domäne	Administrative / technische Gemeinschaft oder Organisation mit einer gemeinsamen *Policy.* [eCH-0107]
Entitätsmetadaten	Metadaten einer AA oder RP zur Definition der Rolle einer Entität innerhalb der STIAM-Community.
Globally Unique Identifier GUID	Eindeutige Nummerierung, einem Subjekt zugeordnet, generiert bei dessen Registrierung auf der STIAM-Plattform. Verbindet die Einträge eines Subjekts in STIAM-UIR und STIAM-UCR.
Identifikator	Eine Zeichenkette, welche ein *eIdentity* innerhalb eines *Namensraumes* eindeutig bezeichnet. Ist Teil der Credentials. [eCH-0107]
Identität	Identität ist die Gesamtheit der ein *Subjekt* kennzeichnenden und als Individuum von allen anderen unterscheidenden Eigentümlichkeiten. Im IAM-Kontext wird hauptsächlich die *digitale Identität* eines *Subjekts* verwendet (siehe *digitale Identität*). [eCH-0107]
Entität	Ein aktives Element eines IT Systems, z.B. ein automatisierter Prozess oder eine Menge von Prozessen, ein Teilsystem, eine Person oder eine Gruppe von Personen mit definierten Funktionalitäten. [eCH-0107] Organisation mit definierter Rolle innerhalb einer STIAM-Community.
Funktion	Eigenschaft, die einem Subjekt bestimmte Aufgaben, Kompetenzen und Verantwortung innerhalb einer Organisation zuweist. Ein Subjekt kann mehrere Funktionen haben (vgl. Rolle). [eCH-0107]
Identity Provider (IdP)	*Entität*, die *digitale Identitäten* verwaltet und herausgibt. Ein IdP stellt einen *Authentication Service* und meist auch einen *Attribute Assertion Service* zur Verfügung. [eCH-0107]
Identitäts- und Zugriffsverwaltung / Identity und Access Management (IAM)	Alle Prozesse und Systeme um Subjekten den Zugriff auf die Ressourcen zu ermöglichen, die diese auf Grund ihrer Funktion in der Organisation benötigen. [eCH-0107]
Informationskonsument	Siehe RP
Informationslieferant	Siehe AA
Juristische Person	Juristische Person gemäss OR (Firmen, Behörden, Vereine etc.).

Lösungsanbieter	Siehe RP
Lösungsbezüger	Siehe Subjekt
Meta-Attribut	Bestandteil des Attribut-Schemas, Spezifizierung des Attributs.
Metadaten	Ein Mittel, um Vertrauen und technische Interoperabilität zwischen SAML Komponenten zu ermöglichen. Können auch verwendet werden, um Attributinformationen auszutauschen. [eCH-0107]
Namensraum	Anwendungsbereich (z.B. ein Unternehmen, ein Staat, eine Fachgemeinschaft, eine Sprachgemeinschaft), für welchen die Bedeutung einer Zeichenkette (z.B. Identifikator) definiert ist. [eCH-0107]
Natürliche Person	Natürlich Person gemäss OR.
Organisation	Organisatorische Einheit (Unternehmen, Verein, Amtsstelle, …) [eCH-0107]
Policy	Schriftlich festgehaltene Regelungen und Vorschriften, welche einzuhalten sind. [eCH-0107]
Quality Authentication Assurance (QAA)	Qualität der Authentifikation einer digitalen Identität gemäss ISO 29115:2013.
Register	Verzeichnisse in der Verwaltungssprache, wie z.B. die Einwohnerregister, Anwaltsregister, Zivilstandsregister, Handelsregister etc.. Sie werden in der Regel von offiziellen Stellen (Behörden) geführt. [eCH-0107]
Registration Authority	Optionale Instanz innerhalb einer Public Key Infrastructure (PKI). Sie arbeitet eng mit der CA zusammen und ist zuständig für das sichere Erfassen notwendiger Personalien. Sie überprüft die Identität, sendet den Antrag an die CA.
Relying Party (RP)	Die Relying Party nutzt IAM-Geschäftsservices und verarbeitet Informationen von IAM-Dienstanbietern für den Schutz seiner Ressourcen. Sie braucht zur Beurteilung der Berechtigung eines Ressourcenzugriffs nähere Informationen zu einem Subjekt. [eCH-0107]
Ressource	Service oder Daten, auf welche ein *Subjekt* zugreifen kann, wenn es sich authentisiert hat und es auf der Basis der benötigten Attribute autorisiert wurde. [eCH-0107]
Ressourcenverantwortlicher	Verantwortliche Stelle für die von der *Relying Party* verwalteten *Ressourcen* (z.B.: Anwendungsverantwortlicher, Serviceverantwortlicher, Dateninhaber). [eCH-0107]
Role based Access Control (RBAC)	Verfahren zur Zugriffssteuerung und -kontrolle auf Dateien oder Dienste (Deutsch: Rollenbasierte Zugriffskontrolle).
Rolle / Role	a) *Organisation*, *Subjekt*: Bestimmte Anzahl von Funktionen, die in einer Organisation ausgeführt werden. Einem *Subjekt* können eine oder mehrere Rollen zugeteilt werden. b) System, *Entität*: Aufgabe und Zweck einer *Entität* in einer Federation. Einer *Entität* können eine oder mehrere Rollen zugeteilt werden. [eCH-0107]
Security Assertion Markup Language (SAML)	SAML (Security Assertion Markup Language) wurde spezifiziert, um herstellerunabhängig Single Sign-On zu ermöglichen. SAML ist ein XML Framework, mit dessen Hilfe *Authentifizierungs-* und *Autorisierungsinformationen* ausgetauscht werden können. SAML wurde von einem internationalen Konsortium und im Rahmen der OASIS standardisiert. [eCH-0107]

Security Token	Ein Datenpaket, welches verwendet werden kann, um den Zugriff auf eine *Ressource* zu autorisieren. [eCH-0107]
Security Token Service STS	Infrastruktur, die in der Lage ist, Security Tokens nach SAML 2.0 Standard zu erzeugen, zu signieren und als Service zur Verfügung zu stellen
Service Level Agreement (SLA)	Bezeichnet einen Vertrag zwischen Auftraggeber und Dienstleister für wiederkehrende Dienstleistungen. [eCH-0107]
STIAM	SuisseTrust Identity and Access Management
STIAM-Account	Minimal gebildet durch Einträge in STIAM-IdP (E-Mail Addresse, Passwort, optionales 2. Kanal Authentifikationsmittel) und STIAM-UCR (GUID, STIAM-IdP-Identifikator, optionales Credential). Wird bei der Registrierung des Subjekts erstellt, muss danach vom Subjekt aktiviert werden. Jedes Subjekt hat auf der STIAM-Plattform mindestens einen STIAM-Account.
STIAM-Broker	Die zentrale Vermittlerinfrastruktur zwischen Subjekt, RP, AuthnA und AA. Er besteht aus dem Identity und Attribute Bus, STIAM-RLM, STIAM-MDR, STIAM-IdP, STIAM-UIR und STIAM-UCR. Ist ein Broker gemäss eCH-0107.
STIAM-Community	Die STIAM-Community bilden alle Teilnehmer, die mit einer STIAM-Plattform interagieren und die einheitliche Spezifikation (vgl. Policy) berücksichtigen.
STIAM-Empfänger	Kommunikationsmodul, das die standardisierte SAML-Kommunikation zwischen der RP und dem STIAM-Broker realisiert.
STIAM Identity und Attribute Bus	Vermittelt Authentisierungs- und Attributanfragen zwischen Subjekt, RP, AuthnA und AA. Nimmt die SAML-Requests der STIAM-Empfänger entgegen und leitet sie an die korrekte AuthnA und AA weiter. Danach nimmt er die Responses der STIAM-Sender entgegen und sendet die Informationen als aggregierte SAML-Response an die korrekte RP zurück.
STIAM-IdP	Interner IdP einer STIAM-Plattform. Dient dem Registrieren und Initialisieren von STIAM Accounts und liefert qualitativ minimale Authentifikation der Subjekte.
STIAM-Metadata Repository (STIAM-MDR)	Zentraler Auskunftsdienst der STIAM-Plattform, verwaltet und publiziert die Metadaten für die STIAM-Community.
STIAM-Plattform	Die STIAM-Plattform umfasst den STIAM-Broker sowie alle zusätzlichen STIAM-spezifischen Komponenten (STIAM-Sender, STIAM-Empfänger, STIAM-CSP) die den Betrieb der funktionalen Lösung ermöglichen.
STIAM-RLM (Reporting-Logging-Monitoring)	Zur Gewährleistung der Nachvollziehbarkeit und Nachweisbarkeit werden Zugriffe auf Ressourcen gespeichert. Mit dem STIAM-RLM sollen analog dazu alle Vorgänge, die vom STIAM-Broker vermittelt werden, geloggt und überwacht werden können.
STIAM-Sender	Kommunikationsmodul, das die standardisierte SAML-Kommunikation zwischen der AA und dem STIAM-Broker realisiert.
STIAM-UCR (User Credential Repository)	Enthält die Credentials der Subjekte und deren Quelle.

STIAM-UDR (User-data Repository)	Der Datensafe eines Subjekts, in dem alle subjekt-spezifischen Attribute verwaltet werden, die nicht von einer externen AA bereitgestellt werden. Das Subjekt trägt seine Attribute hier selber ein. Die STIAM-UDR ist eine spezielle Ausprägung einer AA. Sie ist logisch von der STIAM-Plattform getrennt und kommuniziert mit dieser über einen STIAM-Sender.
STIAM-UIR (User Identifier Repository)	Die User Identifier Repository verwalten die externen Identifier-Definitionen zu AA-Ressourcen und ermöglicht es der STIAM-Plattform, so Daten über ein Subjektaus einer AA und die intern identifizierte Person zu matchen.
Subjekt	Eine natürliche Person, Organisation oder ein Service, die auf eine *Ressource* zugreift oder zugreifen möchte. Ein Subjekt wird durch *digitale Identitäten* beschrieben. [eCH-0107]
Trusted Third Party	Vertrauenswürdige Instanz z.B. zur Verwaltung von öffentlichen Schlüsseln oder Zertifikaten. [eCH-0107] (Siehe auch STIAM-MDR)
Trust-Level	Zwischen den Beteiligten abgemachtes Vertrauensniveau, das Sicherheitsanforderungen für die Prozesse und die technologischen Komponenten festlegt. [eCH-0107]
UID	Unternehmens-Identifikationsnummer
Unternehmen	Siehe *Organisation* [eCH-0107]
User	Siehe *Benutzer* [eCH-0107]
Vermittlerinfrastruktur	Siehe STIAM-Broker
Vertrauen	Formell definierte Vertrauensbeziehung zwischen verantwortlichen Stellen, z.B. die formelle Beschreibung der Kriterien, die erfüllt sein müssen, damit sich zwei Organisationen, Entitäten, Domänen etc. gegenseitig vertrauen (engl. Trust).
Verzeichnis	Systematische Sammlung von Informationen mit gemeinsamen Merkmalen. [eCH-0107]
Zugriff	Interaktion mit einer Entität um eine oder mehrere ihrer Ressourcen zu manipulieren und oder zu nutzen. Zur Gewährleistung der Nachvollziehbarkeit und Nachweisbarkeit werden Zugriffe gespeichert. [eCH-0107]
Zugriffskontrolle	Überwachung und Steuerung des Zugriffs auf *Ressourcen*. Das Ziel ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen. [eCH-0107]

Anhang E – STIAM-UseCases

Use case ‚Standard STIAM'

Der STIAM-Empfänger verlangt für den Zugriff auf eine Ressource, dass sich das Subjekt mit einem bestimmten Set an Attribute Assertions von einem STIAM-Sender ausweist.

Das Subjekt authentisiert sich gegenüber dem STIAM-Broker mit einer bestimmten Identifikationsmethode (beispielsweise Username / Passwort oder eine höhere Zweifaktoren-Authentisierungsmethode) und beantragt dann das entsprechende Attribut vom STIAM-Sender.

Beispiel:

Das Subjekt verlangt Zugriff auf einen Bauservice, der zum Login die Firmenzugehörigkeit aus dem firmeninternen Attribut-Autorität-Register erfordert.

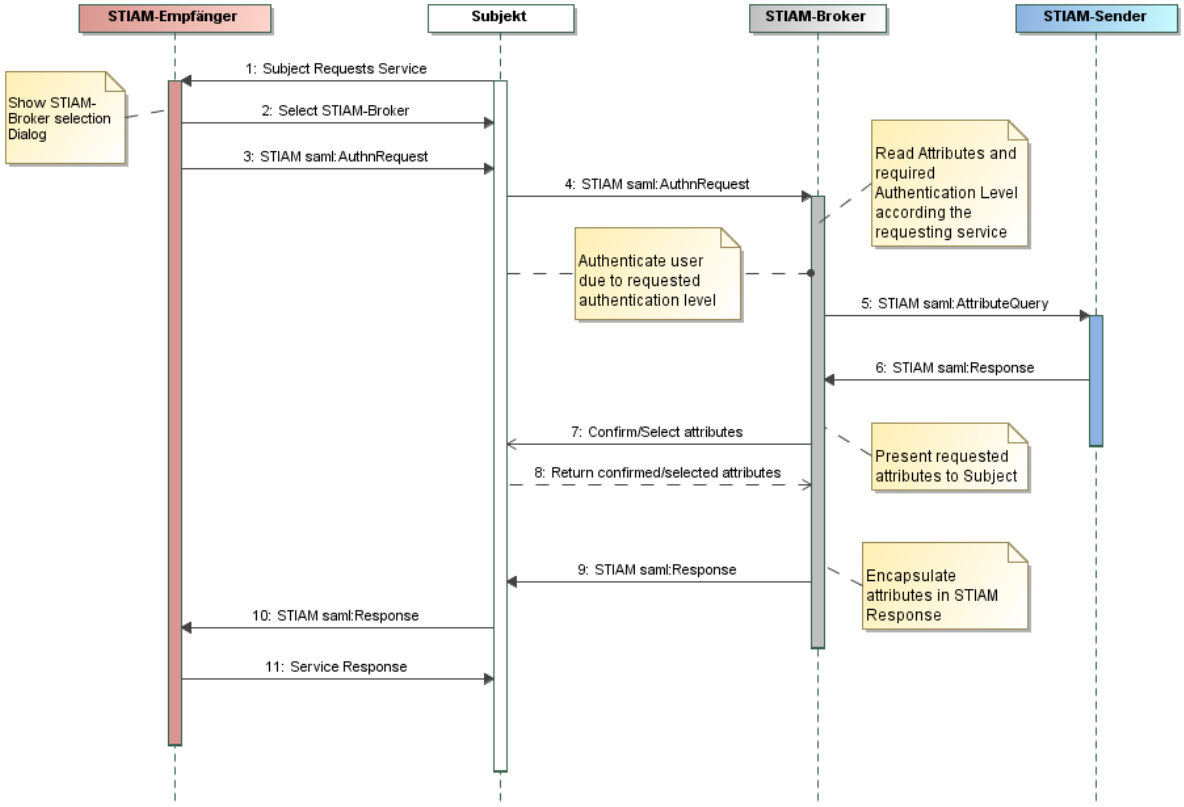

Abbildung 7 STIAM Authentisierungs- und Attribute-Request

Use case ‚Kombinierte STIAM-Anfrage'

Der STIAM-SP verlangt für den Zugriff auf eine Ressource, dass sich das Subjekt mit einer Menge von Attribute Assertions von mehreren Attribut-Autoritäten ausweist.

Das Subjekt authentisiert sich am STIAM-IdP mit einer internen Identifikationsmethode (beispielsweise Username / Passwort oder eine höhere Zweifaktoren-Authentisierungsmethode) und beantragt dann die entsprechenden Attribute von mehreren STIAM-Sendern. Diese müssen vom STIAM-Broker vor der Rückgabe an das Subjekt aggregiert werden.

Beispiel:

Das Subjekt verlangt Zugriff auf einen erweiterten Bauservice, der zum Login die Firmenzugehörigkeit aus dem firmeninternen Attribut-Autorität-Register und daneben den Status der entsprechenden UID aus dem UID-Register anfordert.

Use case ‚Andere Authentifikation-Autoritäten mit Attributabfrage STIAM'

Dieser Use case geht von einer Authentifikation bei einem externen IdP und einer Attributabfrage bei einem STIAM-Sender aus. Der externe IdP wird über ein ‚Other-Authn-Plugin' angesprochen. Der STIAM-Empfänger vertraut der Identifizierung der externen Authentifikation-Autorität aufgrund der definierten Qualitätskriterien und gewährleistet die entsprechenden Attributzugriffe. Der Trust entsteht über die Abbildung des ‚Other-Authn-Plugin' in einer Liste von vertrauenswürdigen externen Authentifikation-Autorität, die auf dem STIAM-Broker geführt wird.

Beispiel:

Das Subjekt wird für den Zugriff auf ein Webportal über eine externe Authentifikation-Autorität authentifiziert (z.B. MobileID).

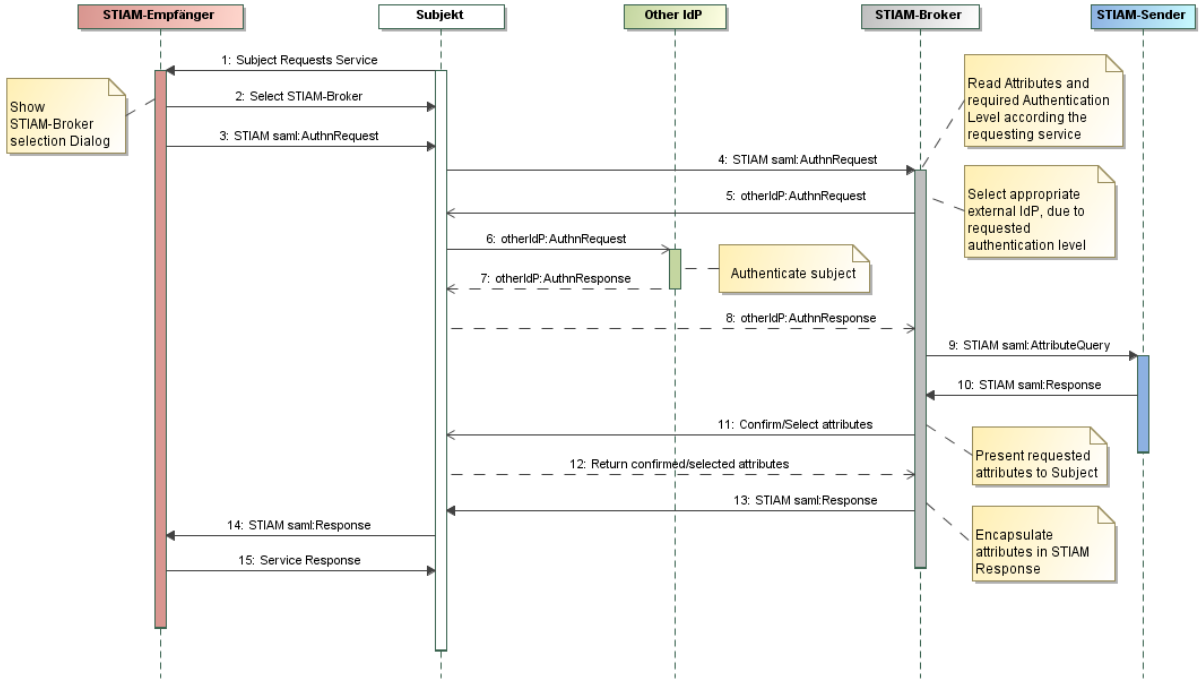

Abbildung 8 Andere Authentifikation-Autorität mit Attributabfrage STIAM'

Use case ‚SuisseID Core-Attribute'

Der STIAM-SP verlangt für den Zugriff auf eine Ressource vom Subjekt ein Attribut aus dem SuisseID-Core Set. Der STIAM-Broker leitet die Anfrage direkt an den IdP der SuisseID weiter. Dort authentisiert sich das Subjekt. Für diesen speziellen Use case benötigt das Subjekt keinen Identifikator innerhalb der STIAM-Plattform, kann aber auch keine zusätzlichen Attribute über eine AA aus einer anderen administrativen Domain beziehen.

Beispiel:

Das Subjekt verlangt Zugriff auf einen Weinshop, der zum Login das Geburtsdatum anfordert.

Use case ‚SuisseID CAS Abfrage'

Dieser Use case geht von einer SuisseID-CAI-Anfrage aus. Dabei soll ein Attribut von einem SuisseID-CAS abgefragt werden. Es muss dazu eine Authentifikation beim SuisseID-IdP erfolgen, da ein SuisseID-CAS grundsätzlich eine solche verlangt. Die über den STIAM-Broker angeforderten Attribute können in diesem Fall von einem als STIAM-Sender registrierten SuisseID-CAS geliefert und signiert werden, da die SuisseID-CAS-Spezifikation kein Trust-Verhältnis eines CAS zur bestehenden SuisseID-IdP-Umgebung vorsieht. Dies ermöglicht über den STIAM-Broker einen SuisseID-CAS-Dienst (zum Bsp. Notarenregister) mit einer bestimmten Qualität und einem daraus resultierenden Vertrauen jedem STIAM-Empfänger zugänglich zu machen.

Beispiel:

Das Subjekt verlangt Zugriff auf einen Service, der zum Login die Notarenbestätigung anfordert, die das Subjekt über den SuisseID-CAS-Notarenregister anfordern kann.

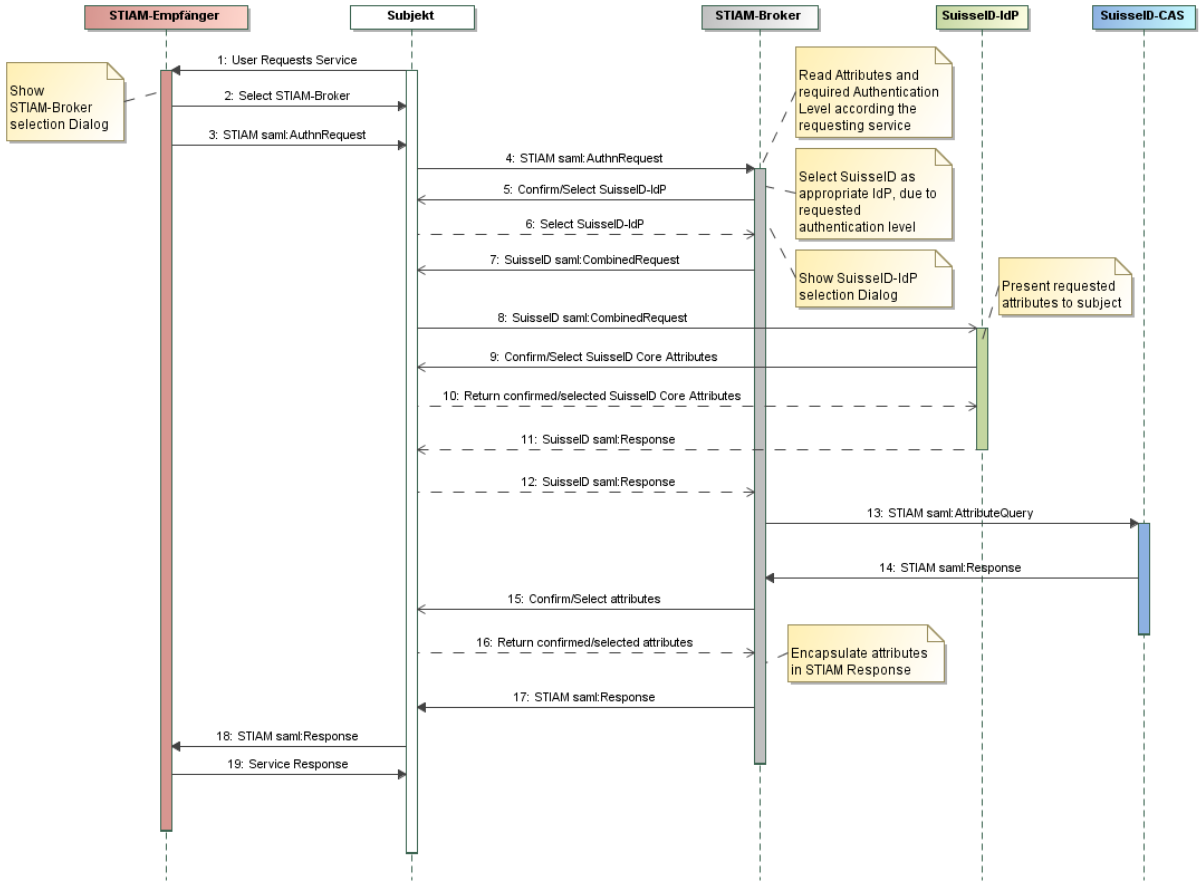

Abbildung 9 SuisseID-Authentisierung und –CAS-Abfrage über STIAM-Broker