eCH-0167 Concept cadre SuisseTrustIAM

Titre	Concept cadre SuisseTrustIAM
Code	eCH-0167
Type	Norme
Stade	Défini
Version	1.0
Statut	Approuvé
Validation	2014-06-04
Date de publication	2014-08-14
Remplace	--
Langues	Allemand (original) et français (traduction)
Annexes	aucune
Auteur(s)	Groupe spécialisé Identity & Access Management Gerhard Hassenstein, Haute école spécialisée bernoise, gerhard.hassenstein@bfh.ch Ronny Bernold, Haute école spécialisée bernoise, ronny.bernold@bfh.ch Thomas Selzam, Haute école spécialisée bernoise, thomas.selzam@bfh.ch Olivier Brian, Haute école spécialisée bernoise, olivier.brian@bfh.ch
Editeur / distributeur	Association eCH, Mainaustrasse 30, Case postale, 8034 Zurich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Condensé

SuisseTrustIAM doit mettre à disposition un service générique Identity & Access Management pour les domaines de la cyberadministration, de la cybersanté, de la cyberéducation et de la cyberéconomie dans toute la Suisse. La plus importante et la plus innovante des fonctionnalités proposées consiste en une infrastructure de transmission, qui permet de légitimer de manière qualifiée les attributs (rôle) via un registre ou un répertoire pour un sujet authentifié (représenté par une eIdentity) d'une entreprise ou organisation, y compris la traçabilité.

Ce concept cadre décrit le mode de fonctionnement fondamental de l'ensemble de la Community SuisseTrustIAM. Le présent document a pour but d'en décrire les différents composants et leurs fonctions. Ce document pose les bases de la spécification technique, organisationnelle et sémantique. Le concept cadre définit une plateforme aussi générique que possible, à laquelle tant les fournisseurs de solutions que les registres, les organisations et les autres sources, en tant que fournisseurs de données, peuvent se connecter en toute simplicité. En tant que modèle, il doit en outre servir à présenter autant d',use cases', exigences et d'éventuels protocoles de communication que possible.

Sommaire

Liste des figures

Liste des tableaux

1 Statut du document

Le présent document a été ***approuvé*** par le Comité d'experts. Il a force normative pour le domaine d'application défini dans le domaine de validité stipulé.

2 Introduction

Toutes les formulations se réfèrent aux personnes des deux sexes.

2.1 Classement

La vision de l'administration interconnectée exposée dans la norme eCH-0126 et les processus transversaux qui y sont associés dans la cyberadministration suisse requièrent une administration d'identité et d'autorisation (IAM) transversale. La norme eCH-0107 décrit cet IAM fédéré et définit des principes, des règles et le cadre règlementaire pour la conception du système d'IAM. SuisseTrustIAM représente un concept d'Identity & Access Management fédéré, qui doit être compris comme une variante de solution possible. Outre SuisseTrustIAM, il existe d'autres concepts d'IAM fédérés (SWITCH-aai par exemple)

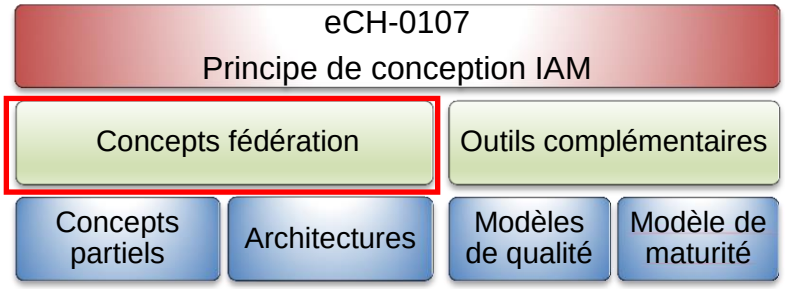

Figure 1 Classement du cadre de normalisation

2.2 Champ d'application

SuisseTrustIAM doit mettre à disposition un service générique Identity & Access Management pour les domaines de la cyberadministration, de la cybersanté, de la cyberéducation et de la cyberéconomie dans toute la Suisse. La plus importante et la plus innovante des fonctionnalités proposées consiste en une infrastructure de transmission, qui permet de légitimer de manière qualifiée les attributs (rôle) via un registre ou un répertoire pour un sujet authentifié (représenté par une eIdentity) d'une entreprise ou organisation, y compris la traçabilité.

2.3 Avantages

Le concept cadre définit une plateforme aussi générique que possible, à laquelle tant les consommateurs d'informations que les fournisseurs d'informations (en priorité les registres, organisations et autres sources) peuvent se connecter. Le but est d'éviter de devoir élaborer des solutions spécifiques pour les différents services. En tant que modèle, ce concept cadre doit couvrir autant de ‚use cases', d'exigences et d'éventuels protocoles de communication que possible.

2.4 Priorité en termes de contenu

Ce document décrit le mode de fonctionnement de base de l'ensemble de la Community SuisseTrustIAM. Le concept cadre a pour but d'en décrire les différents composants et leurs fonctions. Il pose les bases de la spécification technique, organisationnelle et sémantique.

3 Concept SuisseTrustIAM

L'objectif de la solution globale est de transmettre les informations d'authentification et d'attributs des fournisseurs d'informations (autorités d'authentification et d'attributs) aux consommateurs d'informations via l'infrastructure de transmission (plateforme STIAM).

Avec ses participants, la Community SuisseTrustIAM se décompose grossièrement en 3 catégories:

- Consommateurs d'informations (Relying Party ou partie de confiance)
- Fournisseurs d'informations
  - Autorités d'authentification et d'attributs
- Infrastructure de transmission

La figure 1 est une représentation graphique grossière de la structure STIAM. Le système global se décompose en quatre parties (aux couleurs distinctes) dans un souci d'illustrer la délimitation des différentes fonctions. Les fournisseurs d'informations sont répartis entre autorités d'authentification et d'attributs.

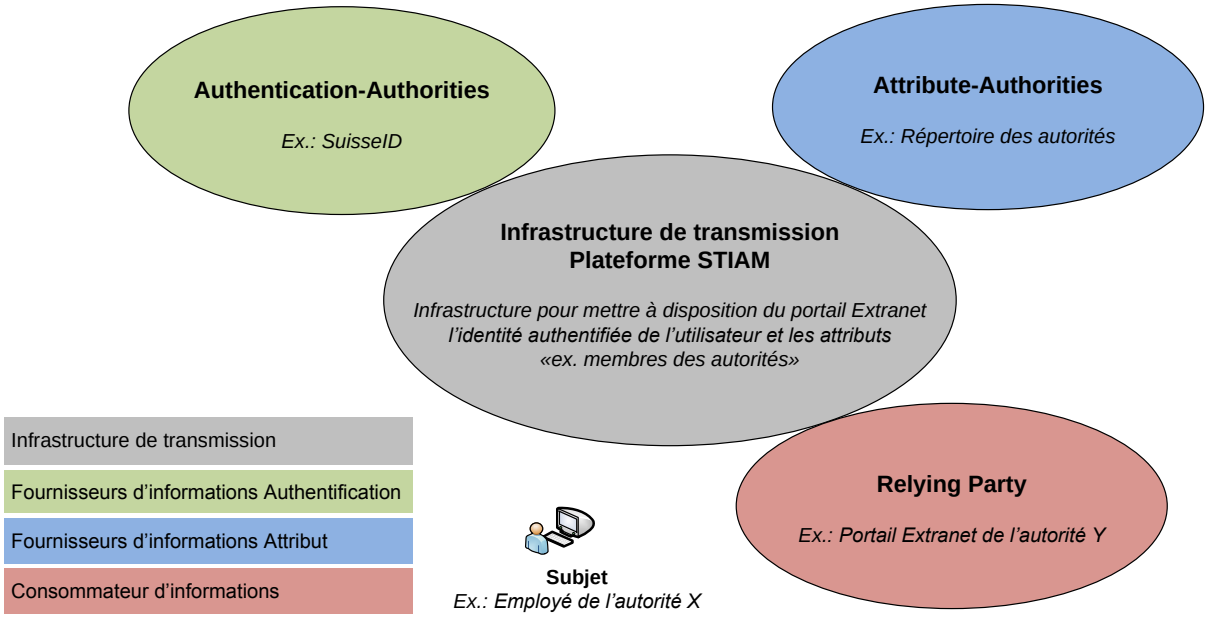

Figure 2 Structure grossière STIAM

La partie centrale de la plateforme STIAM est le Broker STIAM, qui met à disposition l'infrastructure de transmission. Les consommateurs d'informations (Relying Parties ou parties de confiance) et les fournisseurs d'informations (autorités d'authentification et d'attributs) sont reliés au Broker STIAM. L'émetteur STIAM est l'interface standardisée vers les autorités d'attributs (en règle générale répertoires et registres). L',User Data Repository', décrit plus en

détail au chapitre 5.4 représente une autorité d'attributs spécifique. Le destinataire STIAM met en œuvre l'interface standardisée vers une Relying Party (un portail par exemple) avec différents services et applications. Le terme autorités d'authentification (SuisseID par exemple) désigne des fournisseurs d'authentification externes, qui sont compatibles avec la plateforme STIAM et sont considérés comme dignes de confiance.

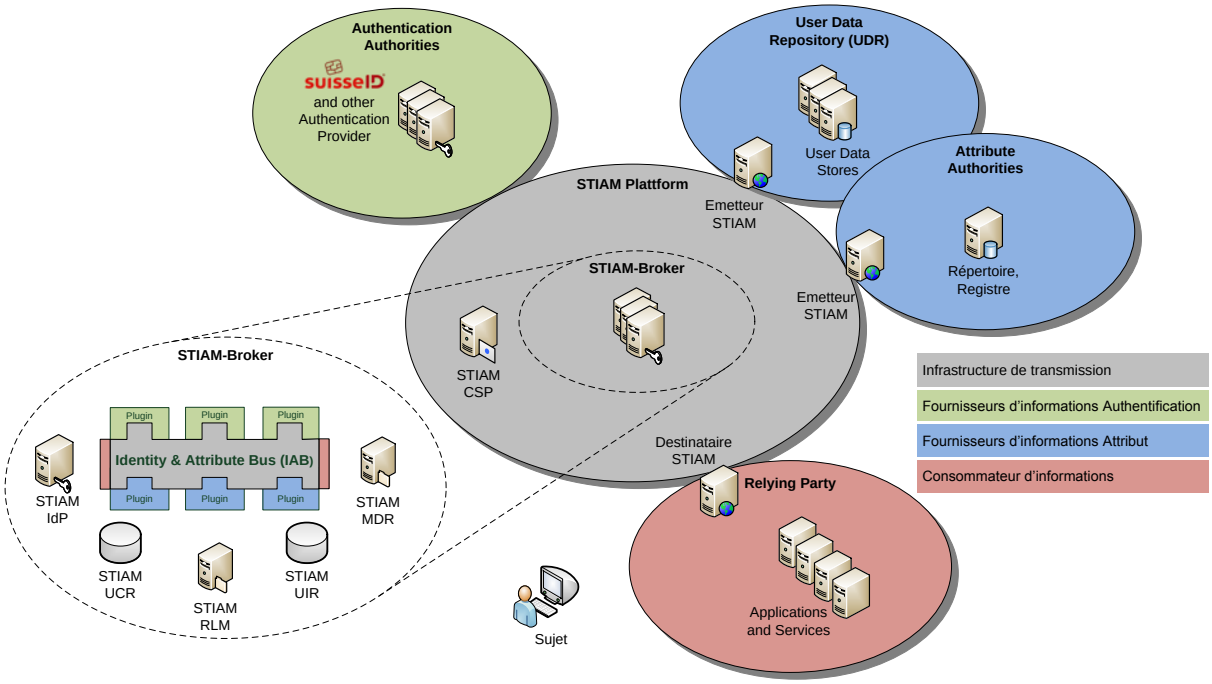

Figure 3 Composants STIAM

Une organisation (une entreprise ou un service de cyberadministration par exemple), qui désire utiliser la plateforme STIAM, peut jouer un ou plusieurs rôles dans ce système global. Elle peut soit se cantonner au simple rôle de consommateur d'informations, soit assumer également le rôle de fournisseur d'informations.

3.1 Délimitation Broker, plateforme, Community STIAM

Dans ce concept, les termes Broker STIAM, plateforme STIAM et Community STIAM sont utilisés comme suit:

Broker STIAM
Le Broker STIAM englobe les services de base, qui constituent l'infrastructure de transmission centrale de la plateforme STIAM (voir chapitre 5.1).

Plateforme STIAM
La plateforme STIAM englobe le Broker STIAM ainsi que tous les composants supplémentaires spécifiques STIAM (émetteur STIAM, destinataire STIAM, CSP STIAM), qui permettent d'exploiter la solution fonctionnelle.

Community STIAM
La Community STIAM se compose de tous les participants, qui interagissent avec la plateforme STIAM et tiennent compte des spécifications homogènes.

4 Architecture cadre

4.1 Principes d'architecture

Les principes d'architecture s'entendent comme des 'best practice'.

- MUST: le Broker STIAM connaît les autorités d'authentification et d'attributs associées et joue ainsi un rôle de transmission d'authentification et d'attributs pour une Relying Party (destinataire STIAM).
- MUST: le Broker STIAM œuvre à la transmission d'eIdentities avec leurs attributs. Il tient un User Identifier Repository (UIR STIAM) afin de mettre à disposition des identificateurs et des liens vers des autorités d'authentification externes.
- MUST: la plateforme STIAM enregistre exclusivement des données impératives pour l'exploitation et l'assistance.
- MUST: les données, qu'un sujet a lui-même entrées sur la plateforme, sont enregistrées dans un User Data Repository séparé de manière logique par le Broker STIAM.
- MUST: la plateforme STIAM garantit le respect de la vie privée des sujets.
- MUST: les autorités d'attributs sont connectées via un émetteur STIAM standardisé.
- MUST: la Relying Party (destinataire STIAM) communique uniquement avec le Broker STIAM. Il n'y a aucune communication directe entre le destinataire STIAM et les autres composants (autorité d'authentification & d'attributs d'autres domaines ou émetteurs STIAM).
- SHOULD: l'infrastructure SuisseID peut être intégrée par la plateforme STIAM, tant comme autorité d'authentification que comme autorité d'attributs.
- SHOULD: l'intégration d'un destinataire STIAM et émetteur STIAM est simple à configurer.
- SHOULD: les attributs et authentifications transmis par le Broker STIAM présentent des valeurs de qualité standardisées. Le destinataire STIAM peut évaluer ces valeurs de qualité.
- SHOULD: les composants à l'intérieur de la plateforme STIAM se font confiance.
- MUST: le Broker STIAM authentifie le destinataire STIAM et l'émetteur STIAM.
- SHOULD: la plateforme STIAM mise sur des protocoles de norme existants et peut, si nécessaire, procéder à leur extension sous forme standardisée.
- SHOULD: les composants STIAM sont multiutilisateurs.

5 Vue d'ensemble des composants

Ce chapitre décrit les composants utilisés dans le concept cadre STIAM.

5.1 Broker TIAM

Le Broker TIAM est l'infrastructure de transmission centrale entre les Relying Parties, les sujets, les autorités d'attributs en tant que fournisseurs de données et les autorités d'authentification d'autres domaines. Il se compose de l'Identity and Attribute Bus, RLM STIAM, MDR STIAM, IdP STIAM et tient l'User Identifier Repository avec les données d'identificateur et l'User Credential Repository avec les données de Credentials. En cas de besoin, toutes les autres données sont mises à disposition par les autorités d'attributs (AA) enregistrées.

5.1.1 Identity and Attribute Bus

L'Identity and Attribute Bus contrôle les méthodes internes d'authentification et échange, si nécessaire, les procédures d'authentification avec les autorités d'authentification externes. L'Identity and Attribute Bus met à disposition des interfaces vers les autorités d'authentification (ex. MobileID, SuisseID) via des PlugIns. Il est ainsi possible d'effectuer des requêtes auprès des Extended SuisseID IdP's et SuisseID Claim Assertion Services (CAS).

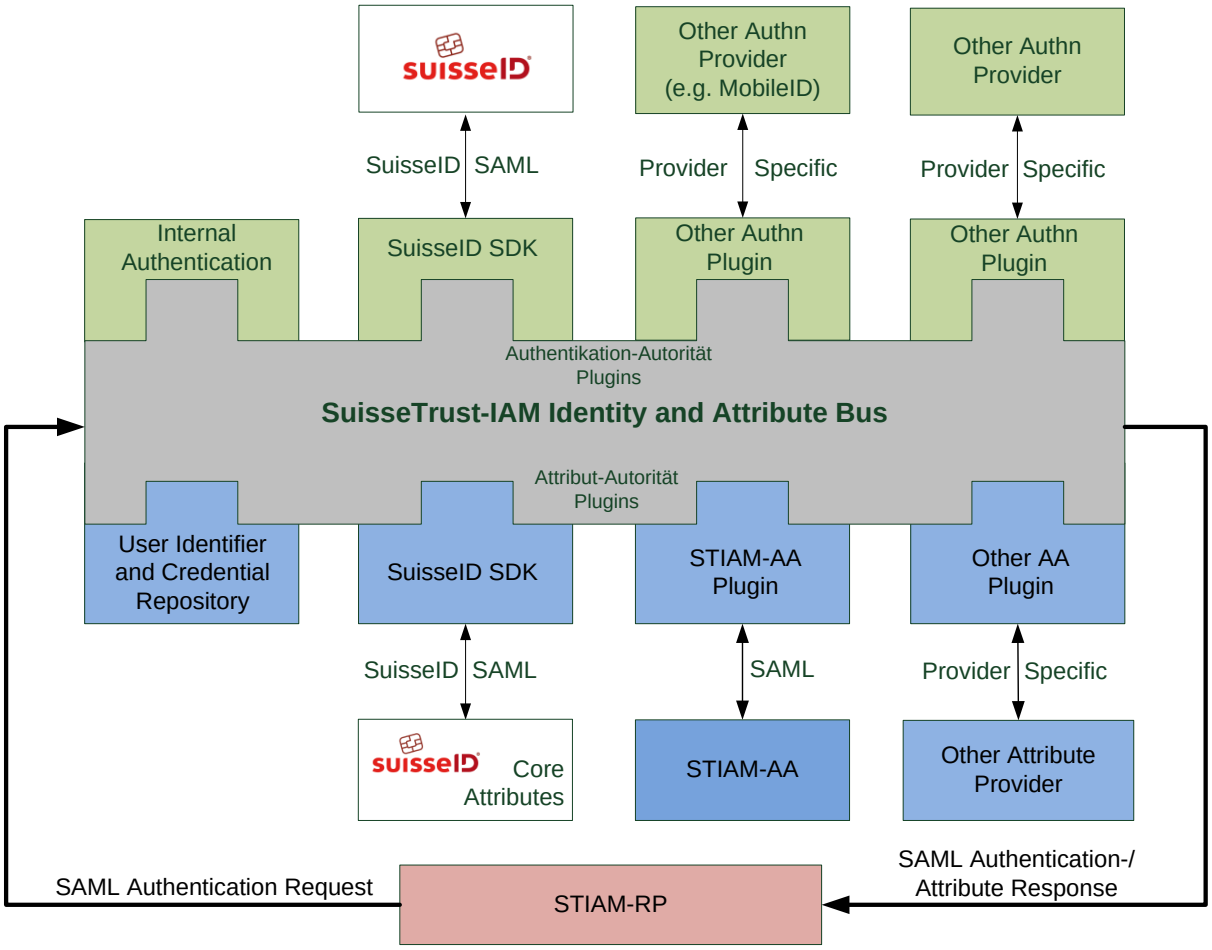

Figure 4 Identity and Attribute Bus STIAM

5.1.2 IdP STIAM (Identity Provider)

Les sujets sont authentifiés au moyen de l'IdP STIAM (Identity Provider). L'authentification s'effectue soit localement via le UCR STIAM, soit via une autorité d'authentification externe. Pour l'authentification externe, l'IdP STIAM utilise le Plugin IdP correspondant de l'Identity and Attribute Bus.

5.1.3 UIR STIAM (User Identifier Repository)

Chaque sujet dispose, sur la plateforme STIAM, d'un compte (Account) unique avec un GUID (Global Unique Identifier). Ce GUID est couplé au User Identifier Repository, dans lequel sont gérées les définitions d'identificateur externes pour les ressources AA. Ceci permet

au sujet d'associer à son compte, via le Broker STIAM, des données émanant d'une autorité d'attributs. L'identification enregistrée dans l'UIR STIAM est l'identificateur, qui est transmis au Broker par un émetteur STIAM au cours du processus de validation du sujet.

Méta-attribut	Identificateur	AA
<Autorisation d'avocat>	1234.5678.8910.1112	Registre des avocats URI
<Droit de vote>	234.234-324	Registre des électeurs Winterthur URI
<Appartenance à une entreprise>	67889054123	Haute école spécialisée bernoise AA URI
<Nom>	STIAM-0001-0002-0003-0004	UDR STIAM URI

Tableau 1 exemple UIR STIAM

5.1.4 STIAM-UCR (User Credential Repository)

L'User Credential Repository, qui contient pour chaque sujet les identificateurs des Credentials et leur source, est également couplé au GUID. Ceci permet à l'IdP STIAM d'authentifier le sujet en interne ou de le faire authentifier en externe.

Type de Credential	Identificateur	Autorité d'authentification source
<MobileID>	1234.5678.8910.1112	MobileID URI
<internal U/PW>	peter.muster	Internal
<BFH-ID>	mustepet	Haute école spécialisée bernoise AuthnA URI
<SuisseID>	0001-0002-0003-0004	CoreIdP URI

Tableau 2 exemple STIAM-UCR

5.1.5 MDR STIAM (Metadata Registry)

Les métadonnées sont des documents XML spéciaux, qui contiennent toutes les informations nécessaires des entités (consommateurs d'informations, fournisseurs d'informations). Ces métadonnées permettent, d'un point de vue technique, que des relations de confiance s'établissent entre ces entités à l'intérieur de la Community. Le MDR STIAM est un service de renseignement central, qui administre et met à disposition les métadonnées de la Community pour la plateforme STIAM.

5.1.6 RLM STIAM (Reporting, Logging et Monitoring)

Le RLM STIAM sert à tenir un journal de et à surveiller toutes les opérations, que le Broker STIAM doit transmettre, au sens de la conformité requise.

5.2 Relying Party (RP)

La Relying Party ou partie de confiance propose une prestation de service sous forme de service Web, qui met en œuvre les contrôles d'accès via SuisseTrustIAM.

5.2.1 Destinataire STIAM

La ressource proposée par la Relying Party communique avec le Broker STIAM via le destinataire STIAM. La Relying Party définit quels attributs sont nécessaires et dans quelle qualité afin de permettre un accès à une ressource protégée. Pour utiliser la ressource, un sujet doit s'authentifier auprès du Broker STIAM et fournir au destinataire STIAM les attributs exigés par la Relying Party dans la qualité correspondante.

5.3 Autorité d'attributs (AA)

Une autorité d'attributs est une organisation ou un registre, qui met à disposition les attributs pour la Community STIAM en tant que fournisseur d'informations.

5.3.1 Emetteur STIAM

Un répertoire est connecté à la plateforme STIAM via un émetteur STIAM. L'émetteur STIAM est conçu comme module de communication, qui met en œuvre la communication SAML standardisée entre l'autorité d'attributs et le Broker STIAM. Il est doté d'une structure aussi simple que possible et peut se procurer des attributs auprès de différentes sources de données (LDAP, SQL etc.).

5.4 UDR STIAM (User Data Repository)

L'User Data Repository STIAM est la mémoire spécifique des attributs d'un sujet. Y sont gérés l'ensemble des attributs spécifiques à un sujet, qui ne sont pas mis à disposition par une autorité d'attributs externe. L'User Data Repository STIAM gère les attributs fournis par le sujet lui même, tel que le ferait une autorité d'attributs. Le sujet gère ses données directement via un service conçu comme un destinataire STIAM. Les données ne font pas partie de la plateforme STIAM et doivent être séparées de la plateforme STIAM de manière logique. La séparation d'UDR STIAM et d'UIR STIAM a pour vocation d'empêcher ou de compliquer le profilage et la traçabilité des données par le Broker STIAM et d'accroître la protection des données spécifiques au sujet.

5.5 CSP STIAM (Certification Service Provider)

Le CSP STIAM représente le Trust-Anchor et le Certificate Issuer pour l'ensemble de la plateforme STIAM. Chaque membre de la plateforme STIAM fait implicitement confiance à ces composants.

6 Métadonnées et Circle of Trust

Un Circle of Trust (COT) regroupe un certain nombre de Relying Parties, d'autorités d'attributs et au moins un Identity-Provider. Dans un COT, ces composants se font confiance à différents niveaux. Pour établir un COT, il faut saisir certaines informations pour ce Provider sous forme de métadonnées d'entité et les publier de telle sorte que chacun des membres du COT puisse contrôler l'authenticité et l'intégrité de ces informations.

6.1 Rôle des MDR STIAM

Au sein de la Community STIAM, chaque membre (fournisseur d'informations, infrastructure de transmission et consommateur d'informations) joue un rôle précis. Les informations nécessaires à cette fonction sont conservées dans les métadonnées d'entité. Celles-ci contiennent notamment des renseignements concernant:

- l'adresse et le nom de l'entité,
- les configurations des points finaux de l'entité (URL),
- les certificats Public Key pour le contrôle des messages à signature numérique (Assertion) d'une entité.

Dans des environnements plus vastes et plus complexes, l'administration de ces métadonnées d'entité est effectuée de manière centrale au moyen d'un service dédié. C'est à cet effet que le présent concept prévoit le service MDR STIAM. Ce service administre et signe de façon centralisée les métadonnées d'entité des membres et les publie sous forme de fichier de métadonnées de Community. De cette manière, les membres de la Community peuvent trouver et vérifier des informations concernant d'autres entités.

Le MDR STIAM propose un répertoire central de toutes les informations nécessaires des Broker STIAM, émetteur STIAM et destinataire STIAM. Ce fichier est à nouveau signé par le MDR STIAM de manière périodique ou après toute modification. Pour la signature, le MDR STIAM utilise un certificat délivré par le CSP STIAM, qui est reconnu digne de confiance par tous les composants dans l'environnement STIAM.

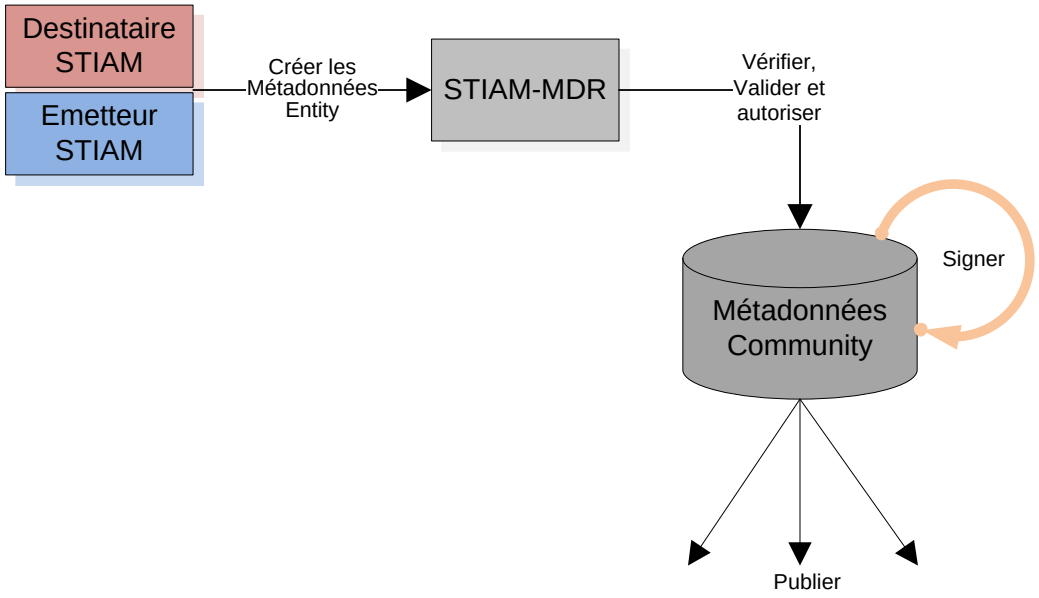

Figure 5 Fonction MDR STIAM

Pour s'enregistrer sur la plateforme STIAM, le responsable d'une organisation doit créer les métadonnées d'entité de son émetteur STIAM ou destinataire STIAM (ceci peut être réalisé au niveau local ou directement via une application Web sur le MDR). Ces données font ensuite l'objet de contrôles dans le cadre d'un processus d'enregistrement concernant la syntaxe, le contenu et l'autorisation.

- Concernant l'émetteur STIAM, les attributs qui doivent être proposés par les fournisseurs de données, sont indiqués en supplément dans les métadonnées d'entité. Le contrôle des attributs indiqués et leur classement par qualité ont lieu au moment de la définition dans le cadre du processus d'enregistrement.
- Concernant le destinataire STIAM, les attributs qui sont requis pour l'autorisation d'accès, sont indiqués en supplément dans les métadonnées d'entité. Là encore, les renseignements doivent être contrôlés dans le cadre du processus d'enregistrement en s'appuyant sur les directives applicables.

Une fois la vérification effectuée avec succès, les métadonnées d'entité du nouveau membre sont intégrées aux métadonnées de la Community par le MDR. Celles-ci sont ensuite signées et publiées.

6.2 Circle of Trust et CSP STIAM

Comme cela a été décrit au chapitre précédent, les membres de la plateforme STIAM se font confiance dans le cadre d'un Circle of Trust. Les relations de confiance entre les composants STIAM reposent sur des certificats X.509, qui sont utilisés pour différentes applications.

- Les certificats SSL sont utilisés afin de garantir la communication entre le serveur Web et les services Web;
- Les certificats, pour signer ou coder les Assertions SAML par exemple;
- Les certificats pour signer les métadonnées de la Community.

Ces certificats doivent être délivrés par un Certification Service Provider (CSP), auquel tous les composants STIAM de la plateforme font confiance.

7 Scénario

Les scenarii suivants présupposent que le destinataire STIAM et l'émetteur STIAM se soient enregistrés au préalable auprès du Broker STIAM, c'est-à-dire du MDR STIAM (voir 5.1.5).

Le fournisseur d'informations (émetteur STIAM) est défini sur la base des exigences de qualité d'attributs de l'acquéreur d'informations (destinataire STIAM). Cette méthode d'identification est quant à elle définie par l'exigence de qualité imposée à l'authentification du sujet (qualité d'authentification) des fournisseurs d'informations (émetteurs STIAM) concernés.

Scénario de base

Dans tous les scénarios, un sujet appelle un service d'une Relying Party et est redirigé vers le Broker STIAM. Les attributs demandés sont compilés et transmis par le Broker STIAM à l'intention du destinataire STIAM. A cet égard, l'authentification et l'Attribut-Assertion peuvent prendre plusieurs formes.

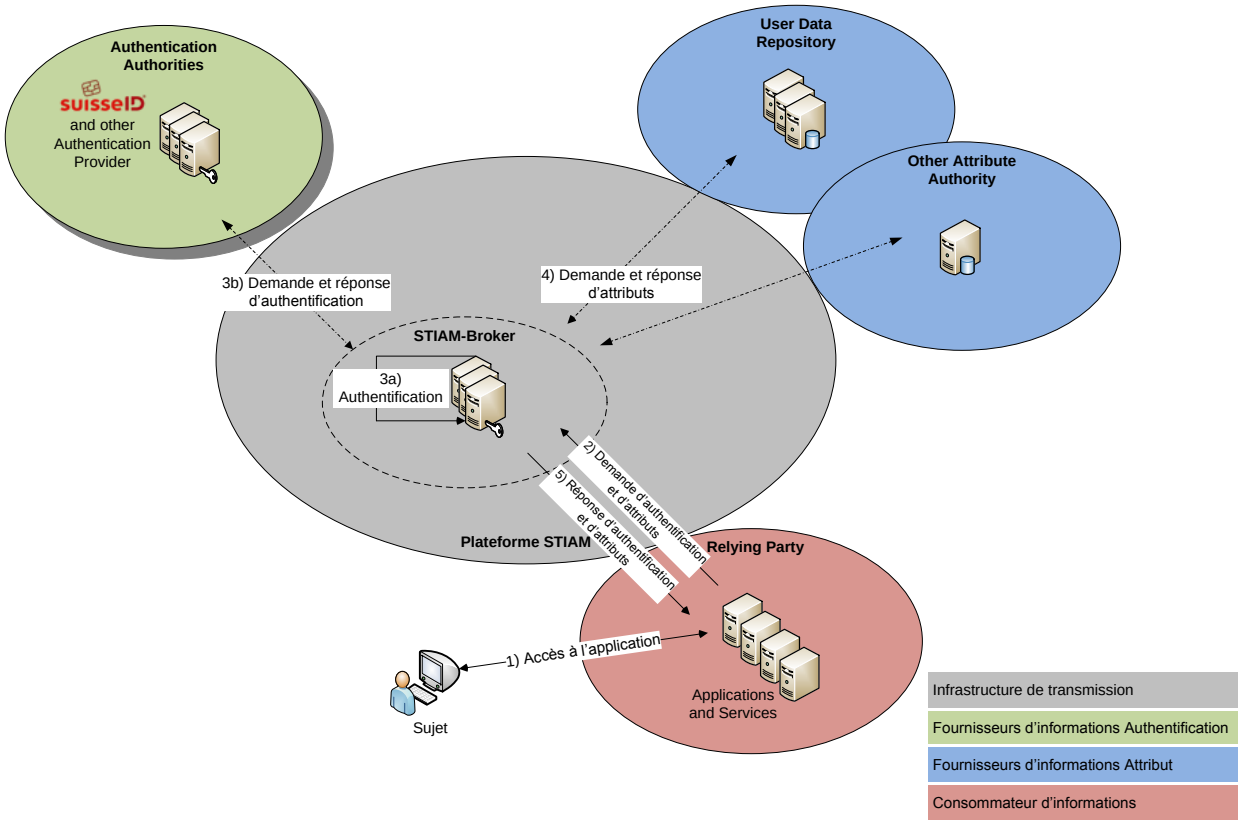

Figure 6 Scénario

8 Modèle de qualité

Dans le contexte de SuisseTrustIAM, deux qualités revêtent une importance particulière. Il s'agit d'une part de la qualité d'un sujet identifié (qualité d'authentification) et d'autre part de la qualité des Attribut-Assertions (qualité d'attributs) relative au sujet. Les qualités d'authentification et d'attributs peuvent présenter des valeurs différentes.

8.1 Exigences

- MUST: la Relying Party définit auprès du Broker STIAM la valeur de qualité de l'authentification d'un sujet.
- MUST: la Relying Party définit auprès du Broker STIAM la valeur de qualité d'un attribut exigé.
- SHOULD: le Broker STIAM peut transférer à la Relying Party la valeur de qualité effective d'un attribut dans la Attribute Response.
- MUST: les Attribute Assertions sont signées par l'émetteur STIAM.
- SHOULD: la Relying Party peut elle-même vérifier l'autorité d'attributs d'une Attribute Assertion.
- SHOULD: l'ensemble du modèle de qualités STIAM s'appuie sur la norme ISO29115 QAA.
- MUST: la qualité d'authentification dans SuisseTrustIAM est définie de façon analogue à la norme ISO29115.
- MUST: les valeurs de qualité se situent entre 1 et 4. Level 4 est la plus haute qualité possible, Level 1 à l'inverse, la plus faible.

9 Considérations de sécurité

La protection des données dans STIAM s'appuie sur les développements actuels des projets européens[1].

9.1 Protection des données par des moyens techniques

Concernant le respect des directives relatives à la protection des données, le concept STIAM suit le principe selon lequel «la protection des données est, dans la mesure du possible, mise en œuvre par des moyens techniques et des règles d'organisation et complétée par des moyens légaux chaque fois que cela est nécessaire».

Un IAM ne permet jamais l'anonymisation totale des sujets. C'est la raison pour laquelle la plateforme STIAM met l'accent sur la «pseudonymisation».

- MUST: la plateforme STIAM restreint le traitement des données relatives aux personnes à un minimum nécessaire.
- SHOULD: la plateforme STIAM renonce à l'utilisation d'identificateurs évocateurs.
- SHOULD: la plateforme STIAM a recours à des pseudonymes comme identificateurs.
- SHOULD: la plateforme STIAM renonce aux identificateurs uniques.
- MUST: la plateforme STIAM empêche ou complique l'établissement de liens entre identificateurs, utilisations prévues et données relatives aux personnes.
- MUST: la plateforme STIAM supprime les liens ou corrélations existants entre eIdentity et identificateur, qui ne sont pas ou plus nécessaires au traitement des données.
- MUST: la plateforme STIAM restreint l'identifiabilité des sujets à un minimum nécessaire.[2]
- MUST: la plateforme STIAM enregistre les données relatives aux personnes, séparées de façon logique.

9.2 Codage des Assertions

Le concept STIAM prévoit également en option le codage direct des attributs dans l'Assertion enchevêtrée. Cela permet un échange confidentiel de valeurs d'attributs entre autorité d'attributs et Relying Party. Mais cela a pour conséquence que l'émetteur STIAM ne peut soumettre au sujet pour validation, les valeurs des attributs requis, qu'avant le codage.

9.3 Centrage sur l'utilisateur et interactions des sujets

La plateforme STIAM a la possibilité de servir de plaque de tournante pour des données relatives à l'identité et d'autres informations d'ordre privé se rapportant à un sujet. D'un autre côté, il doit également être possible d'échanger, via le même service, des informations re-

[1] En particulier 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) et TDL (Trust in Digital Life (2012) Architecture serving complex Identity Infrastructures).

[2] Cf. TURBINE, 47.

présentant le sujet dans sa relation avec une entreprise, une organisation ou une fonction publique.

9.3.1 Sujets physiques

Dans le premier cas, les informations demandées (en particulier les données relatives à l'identité) appartiennent à l'individu (ex. hans.muster@facebook.com). Dès lors, celui-ci doit également pouvoir décider lui-même de leur transmission (écran Attribut Stop) et la communication s'effectue exclusivement centrée sur l'utilisateur, via le navigateur de ce dernier.

Dans le deuxième cas, il est question de données relatives à l'identité, mais qui appartiennent (en règle générale) à une organisation, avec laquelle l'utilisateur est en relation (ex. hans.muster@unternehmen.ch). L'organisation décide, dans le cadre de la législation et des contrats en vigueur, de transmettre ou non ces données à un tiers. Dans le cadre de cette décision, le collaborateur n'a pas à donner son consentement en tant qu'individu. C'est la raison pour laquelle la communication centrée sur l'utilisateur n'est pas non plus nécessaire. Ceci permet une communication directe entre Relying Party et Broker.

9.3.2 Sujets de service

La plateforme STIAM s'adresse également aux services. Les sujets de service se distinguent en particulier sur la durée. Les sujets techniques sont principalement utilisés afin d'exécuter des opérations de processus optimisées. C'est la raison pour laquelle il apparaît peu judicieux à cet égard d'opter pour des opérations de communication centrées sur l'utilisateur. Tous les processus d'enregistrement sont toutefois assurés par les sujets physiques à titre de représentation.

La plateforme STIAM doit tenir compte de tous les scenarii et les standardiser. Pour la communication directe, non centrée sur l'utilisateur, des concepts supplémentaires font l'objet d'évaluations en dehors de ce concept cadre. La spécification ‚Backend attributs Exchange' (BAE)[3] de l'US Federal ‚Identity, Credential and Access Management' (ICAM) constitue une approche prometteuse en la matière.

[3] voir: 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 Exclusion de responsabilité – droits de tiers

Les normes élaborées par l'Association **eCH** et mises gratuitement à la disposition des utilisateurs, ainsi que les normes de tiers adoptées, ont seulement valeur de recommandations. L'Association **eCH** ne peut en aucun cas être tenue pour responsable des décisions ou mesures prises par un utilisateur sur la base des documents qu'elle met à disposition. L'utilisateur est tenu d'étudier attentivement les documents avant de les mettre en application et au besoin de procéder aux consultations appropriées. Les normes **eCH** ne remplacent en aucun cas les consultations techniques, organisationnelles ou juridiques appropriées dans un cas concret.

Les documents, méthodes, normes, procédés ou produits référencés dans les normes **eCH** peuvent le cas échéant être protégés par des dispositions légales sur les marques, les droits d'auteur ou les brevets. L'obtention des autorisations nécessaires auprès des personnes ou organisations détentrices des droits relève de la seule responsabilité de l'utilisateur.

Bien que l'Association **eCH** mette tout en œuvre pour assurer la qualité des normes qu'elle publie, elle ne peut fournir aucune assurance ou garantie quant à l'absence d'erreur, l'actualité, l'exhaustivité et l'exactitude des documents et informations mis à disposition. La teneur des normes **eCH** peut être modifiée à tout moment sans préavis.

Toute responsabilité relative à des dommages que l'utilisateur pourrait subir par suite de l'utilisation des normes **eCH** est exclue dans les limites des réglementations applicables.

11 Droits d’auteur

Tout auteur de normes **eCH** en conserve la propriété intellectuelle. Il s’engage toutefois à mettre gratuitement, et pour autant que ce soit possible, la propriété intellectuelle en question ou ses droits à une propriété intellectuelle de tiers à la disposition des groupes de spécialistes respectifs ainsi qu’à l’association **eCH**, pour une utilisation et un développement sans restriction dans le cadre des buts de l’association.

Les normes élaborées par les groupes de spécialistes peuvent, moyennant mention des auteurs **eCH** respectifs, être utilisées, développées et déployées gratuitement et sans restriction.

Les normes **eCH** sont complètement documentées et libres de toutes restrictions relevant du droit des brevets ou de droits de licence. La documentation correspondante peut être obtenue gratuitement.

Les présentes dispositions s’appliquent exclusivement aux normes élaborées par **eCH**, non aux normes ou produits de tiers auxquels il est fait référence dans les normes **eCH**. Les normes incluront les références appropriées aux droits de tiers.

Annexe A – Références & bibliographie

[eCH-0107] Groupe spécialisé eCH IAM. eCH-0107 Principes de conception pour la gestion de l'identité et de l'accès (IAM). Version 2.0.

Annexe B – Collaboration & vérification

Review Hans Häni, Canton Thurgovie, B2.06

Enno Hoffmann, Atos

Steff Schnetzler, iWeb

Patrick Graber, Swisscom

Konrad Walser, Haute école spécialisée bernoise

Andreas Spichiger, Haute école spécialisée bernoise

Daniel Leiser, Atos

Annett Laube-Rosenpflanzer, Haute école spécialisée bernoise

Annexe C – Abréviations

AA	Autorité d'attributs
AuthnA	Autorité d'authentification
BAE	Backend Attribute Exchange
CAS	Claim Assertion Service
COT	Circle of Trust
CSP	Certification Service Provider
QAA	Quality of Authentication Assurance Levels
IAM	Identity et 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

Annexe D – Glossaire

Terme	Définition
Assertion	Voir *Authentication Assertion* ou *Attribute Assertion* [eCH-0107]
Attribute	Image sémantique d'une propriété attribuée à un sujet, qui décrit ce dernier plus en détail. L'identificateur et les Credentials sont également des attributs. [eCH-0107] Chaque attribut est décrit dans un schéma (méta-attribut) et présente une valeur d'attributs.
Attribute Assertion	Confirmation d'un *attribut* par une *Attribute Authority*. Correspond à une Attribute Assertion SAML 2.0 [eCH-0107].
Autorité d'attributs (AA)	Une autorité d'attributs est un registre ou autre *répertoire* avec un *Attribute Service* pour gérer les attributs et un *Attribute Assertion Service* pour délivrer des *Attribute Assertions*. [eCH-0107] Fournisseur d'informations qui met à disposition des attributs pour la Community STIAM via une interface définie (émetteur STIAM).
Attribute Broker	Voir Broker STIAM
Attribute-Based Access Control (ABAC)	Concept d'octroi dynamique de droits d'accès reposant sur les attributs du sujet.
Auditing	a) Vérification de la conformité à la Policy. b) Liste de toutes les actions et décisions prises pour garantir la traçabilité. [eCH-0107]
Authentication Authority	Une *entité* technique (service), qui propose l'authentification comme prestation de service et délivre des *Authentication Assertions* pour les *sujets* [eCH-0107].
Autorité d'authentification (AuthnA)	Une AuthnA met à disposition un *Authentication Service*, auprès duquel le *sujet* peut s'authentifier. L'Authentication Service utilise des Credentials qui sont délivrés par un *Credential Service*. Le Credential Service peut être une partie intégrante de l'AuthnA. Les IdPs (selon SAML), OpenID Provider et MobilID Provider sont des exemples d'autorités d'authentification. [eCH-0107]
Authentication Proxy	Si l'AuthnA(1) est dans l'incapacité d'authentifier un utilisateur, elle peut dans certaines circonstances agir comme Authentication Proxy, en envoyant elle-même sa propre Authentication Request à une autre AuthnA. L'AuthnA(1) peut utiliser la réponse de l'AuthnA(2) pour créer sa propre réponse. La fonction d'Authentication Proxy est décrite et définie en détails dans la norme SAMLv2, mais elle y est désignée par le terme Identification Proxy.
Authentification	Opération de vérification d'une prétendue *identité numérique*. [eCH-0107]

Authentification	Justificatif de l'*identité numérique* propre à un sujet. [eCH-0107]
Caractéristique d'identification	La caractéristique d'authentification peut reposer sur une connaissance (mot de passe, PIN), sur la possession (certificat, clé privée) ou sur une propriété (caractéristique biométrique ex. voix, empreinte d'iris, empreinte digitale) ou sur une combinaison de ces caractéristiques. [eCH-0107]
Backend Attribute Exchange (BAE)	Demande d'attributs en arrière-plan, habituellement par une machine. Un utilisateur n'est pas directement impliqué dans la requête d'attributs, celle-ci a lieu sans son accord explicite.
Autorisation	a) Administration: définition des règles d'accès et des droits d'accès à une *eRessource*. b) Sur la durée: contrôle de l'autorisation d'accès d'un *sujet* authentifié à une *ressource* et affectation des accès sur la durée. On établit à cet égard une distinction entre *autorisation grossière et précise*. [eCH-0107]
Utilisateur	Sujet humain [eCH-0107]
Gestion d'identité centrée sur l'utilisateur	Permet à l'utilisateur de choisir des Credentials et attributs spécifiques pour le traitement dans les demandes d'authentification et d'attributs et lui donne ainsi le contrôle de sa propre identité numérique. Cela ne signifie pas que l'utilisateur doit autoriser encore une fois de manière explicite chaque transaction, mais que les données sont toujours transmises lors de l'administration de l'identité de l'utilisateur et sont directement liées à son identité numérique.
Autorisation	Droit d'un sujet à utiliser des ressources précises [eCH-0107]
Traitement	Toute opération avec les données, indépendamment des moyens appliqués et des procédés mis en œuvre, en particulier la fourniture, la conservation, l'utilisation, la transformation, la divulgation, l'archivage ou la destruction (en bref: création, lecture, modification, suppression, transfert) de données.
Certification Authority (CA)	Organisme qui, dans le cadre d'un environnement électronique, confirme des données et délivre à des certificats numériques à cet effet. Synonyme: Certification Service Providers (CSP) [eCH-0107]
Certification Service Provider (CSP)	Voir Certification Authority (CA) [eCH-0107]
Circle of Trust (CoT)	Un certain nombre de RP, AA et au moins une AuthnA, dont les composants techniques et d'organisation se font confiance à différents niveaux.
Claim	Le terme Claim n'a pas été explicitement employé dans ce document, en raison de l'existence de plusieurs significations parfois contradictoires. Il est donc recommandé d'éviter ce terme. [eCH-0107]
Claim Assertion Service (CAS)	Le Claim Assertion Service est une *Attribute Authority* particulière. Il a pour mission de permettre à l'utilisateur de confirmer des propriétés lui ayant été attribuées par une organisation ou un registre. [eCH-0107]
Client	Dispositif technique (application, navigateur Web etc.), au moyen duquel le sujet accède à la ressource.
Métadonnées de la Community	Compilation signée de métadonnées d'entité des membres d'une Community STIAM.

Credential	Justificatif confirmant l'*identité* d'un sujet. Dans le contexte IAM, on utilise pour confirmer une identité numérique une identification d'utilisateur (identificateur) en lien avec une (ou plusieurs) caractéristique(s) d'authentification. Synonyme: justificatif d'identité [eCH-0107]
Fournisseur de données	Voir AA
Identité numérique / Digital Identity / eIdentity	Représentation d'un sujet. Une identité numérique (eIdentity) a un identificateur (nom unique), le plus souvent avec un certain nombre d'attributs supplémentaires, qui peuvent être affectés de manière unique à un sujet à l'intérieur d'un espace de noms. Un même sujet peut avoir plusieurs identités numériques. [eCH-0107]
Certificat numérique	Données structurées, qui confirment le propriétaire ainsi que d'autres propriétés d'une clé publique (également certificat ou certificat Public Key). [eCH-0107]
Domaines	Organisation ou communauté administrative / technique ayant une *Policy* commune. [eCH-0107]
Métadonnées d'entité	Métadonnées d'une AA ou d'une RP pour la définition du rôle d'une entité au sein de la Community STIAM.
Globally Unique Identifier GUID	Numérotation unique affectée à un sujet, générée lors de l'enregistrement de ce dernier sur la plateforme STIAM. Associe les entrées d'un sujet dans UIR STIAM et UCR STIAM.
Identificateur	Chaîne de caractères, qui désigne de manière unique une *eIdentity* à l'intérieur d'un *espace de noms*. Fait partie des Credentials. [eCH-0107]
Identité	L'identité correspond à l'ensemble des propriétés qui caractérisent un sujet et le différencient des autres en tant qu'individu. Dans le contexte IAM, on utilise principalement l'*identité* numérique d'un sujet (voir *identité numérique*). [eCH-0107]
Entité	Elément actif d'un système IT, ex. un processus automatisé ou un certain nombre de processus, un système partiel, une personne ou un groupe de personnes aux fonctionnalités définies. [eCH-0107] Organisation avec un rôle défini rôle au sein d'une Community STIAM.
Fonction	Propriété, qui attribue à un sujet des tâches, des compétences et une responsabilité au sein d'une organisation. Un même sujet peut avoir plusieurs fonctions (cf. rôle). [eCH-0107]
Identity Provider (IdP)	*Entité*, qui administre et délivre les *identités numériques*. Un IdP met à disposition un *Authentication Service* et le plus souvent également un *Attribute Assertion Service*. [eCH-0107]
Administration des identités et des accès / Identity & Access Management (IAM)	Tous les processus et systèmes permettant au sujet d'accéder aux ressources, dont il a besoin compte tenu de sa fonction au sein de l'organisation. [eCH-0107]
Consommateur d'informations	Voir RP
Fournisseur	Voir AA

Personne morale	Personne morale au sens du CO (entreprises, autorités, associations etc.).
Fournisseurs de solutions	Voir RP
Acquéreur de solutions	Voir Sujet
Méta-attribut	Composant du schéma des attributs, spécification de l'attribut.
Métadonnées	Un moyen de permettre la confiance et l'interopérabilité technique entre les composants SAML. Peuvent également être utilisées pour échanger des informations d'attributs. [eCH-0107]
Espace de noms	Domaine d'utilisation (ex. une entreprise, un Etat, une communauté spécialisée, une communauté linguistique), pour lequel est définie la signification d'une chaîne de signes (ex. identificateur). [eCH-0107]
Personne physique	Personne physique au sens du CO.
Organisation	Unité organisationnelle (entreprise, association, service officiel…) [eCH-0107]
Policy	Règles et prescriptions stipulées par écrit et devant être respectées. [eCH-0107]
Quality Authentication Assurance (QAA)	Qualité de l'authentification d'une identité numérique selon la norme ISO 29115:2013.
Registre	Répertoires dans la langue d'administration, comme le registre des habitants, le registre des avocats, le registre d'état civil, le registre du commerce etc. Ils sont généralement tenus par les services officiels (autorités). [eCH-0107]
Registration Authority	Instance facultative au sein d'une Public Key Infrastructure (PKI). Elle travaille en étroite collaboration avec la CA et est garante de la sûreté de saisie des détails personnels nécessaires. Elle contrôle l'identité, envoie la demande à la CA.
Relying Party (RP)	La Relying Party utilise les services d'affaires d'IAM et traite les informations des prestataires de services IAM afin de protéger ses ressources. Elle a besoin de plus amples renseignements concernant un sujet pour évaluer l'autorisation d'un accès à une ressource. [eCH-0107]
Ressource	Service ou données auxquels peut accéder un *sujet*, lorsqu'il s'est authentifié et que cela a été autorisé sur la base des attributs nécessaires. [eCH-0107]
Responsable des ressources	Organisme responsable des *ressources* administrées par la *Relying Party* (ex.: responsable d'application, responsable de service, propriétaires de données). [eCH-0107]
Role based Access Control (RBAC)	Procédure de commande et de contrôle des accès aux fichiers ou aux services (français: contrôle d'accès basé sur le rôle).

Rôle / Role	a) *Organisation*, *sujet*: nombre défini de fonctions, qui sont exécutées au sein d'une organisation. Un ou plusieurs rôles peuvent être affectés à un même *sujet*. b) Système, *entité*: tâche et but d'une entité au sein d'une fédération. Un ou plusieurs rôles peuvent être affectés à une même *entité*. [eCH-0107]
Security Assertion Markup Language (SAML)	SAML (Security Assertion Markup Language) a été spécifié afin de permettre un Single Sign-On indépendamment de l'auteur. SAML est un XML Framework, à l'aide duquel des *informations d'authentification et d'autorisation* peuvent être échangées. SAML a été standardisée par un consortium international et dans le cadre de l'OASIS. [eCH-0107]
Security Token	Un paquet de données, que peut être utilisé, afin d'autoriser l'accès à une *ressource*. [eCH-0107]
Security Token Service STS	Infrastructure, qui est en mesure de générer des Security Tokens selon la norme SAML 2.0, de les signer et de les mettre à disposition en tant que service.
Service Level Agreement (SLA)	Désigne un contrat entre le donneur d'ordre et le prestataire de services pour les prestations de services récurrentes. [eCH-0107]
STIAM	SuisseTrust Identity and Access Management
Account STIAM	Minimum constitué par des entrées dans IdP STIAM (adresses E-Mail, mot de passe, moyen d'authentification facultatif de 2ème canal) et UCR STIAM (GUID, identificateur IdP STIAM, Credential facultatif). Est créé lors de l'enregistrement du sujet, doit ensuite être activé par le sujet. Chaque sujet dispose d'au moins un Account STIAM sur la plateforme STIAM.
Broker STIAM	L'infrastructure de transmission centrale entre sujet, RP, AuthnA et AA. Elle se compose d'Identity & Attribute Bus, RLM STIAM, MDR STIAM, IdP STIAM, UIR STIAM et UCR STIAM. Broker au sens de la norme eCH-0107.
Community STIAM	La Community STIAM se compose de tous les participants, qui interagissent avec une plateforme STIAM et tiennent compte d'une spécification homogène (cf. Policy).
Destinataire STIAM	Module de communication, qui met en œuvre la communication SAML standardisée entre la RP et le Broker STIAM.
STIAM Identity et Attribute Bus	Transmet les demandes d'authentification et d'attributs entre le sujet, la RP, l'AuthnA et l'AA. Reçoit les SAML-Requests du destinataire STIAM et les transmet à l'AuthnA et l'AA corrects. Il reçoit ensuite les réponses de l'émetteur STIAM et renvoie les informations en tant que SAML-Response agrégées à la RP correcte.
IdP STIAM	IdP interne d'une plateforme STIAM. Sert à l'enregistrement et l'initialisation d'Accounts STIAM et fournit une authentification qualitativement minimale des sujets.
STIAM-Metadata Repository (MDR STIAM)	Centre de renseignements central de la plateforme STIAM, administre et publie les métadonnées pour la Community STIAM.

Plateforme STIAM	La plateforme STIAM englobe le Broker STIAM ainsi que tous les composants spécifiques STIAM (émetteur STIAM, destinataire STIAM, CSP STIAM), qui permettent d'exploiter la solution fonctionnelle.
RLM STIAM (Reporting-Logging-Monitoring)	Les accès aux ressources sont enregistrés afin de garantir la traçabilité et la vérifiabilité. De manière semblable, le RLM STIAM doit permettre de tenir un journal de et de surveiller toutes les opérations, qui sont transmises par le Broker STIAM.
Emetteur STIAM	Module de communication, qui met en œuvre la communication SAML standardisée entre l'AA et le Broker STIAM.
UCR STIAM (User Credential Repository)	Contient les Credentials des sujets et leur source.
UDR STIAM (Userdata Repository)	Le coffre-fort de données d'un sujet, dans lequel sont administrés tous les attributs qui lui sont spécifiques et qui ne sont pas mis à disposition par une AA externe. Le sujet y saisit lui-même ses attributs. L'UDR STIAM est une forme particulière d'AA. Elle est séparée de manière logique de la plateforme STIAM et communique avec celle-ci via un émetteur STIAM.
UIR STIAM (User Identifier Repository)	Les User Identifier Repository gèrent les définitions d'Identifier externes pour les ressources AA et permettent à la plateforme STIAM de faire ainsi concorder les données concernant un sujet émanant d'une AA et la personne identifiée en interne.
Sujet	Une personne physique, une organisation ou un service, qui accède ou souhaite accéder à une *ressource*. Un sujet est décrit par des *identités numériques*. [eCH-0107]
Trusted Third Party	Instance digne de confiance ex. pour l'administration de clés publiques ou de certificats. [eCH-0107] (Voir aussi MDR STIAM)
Trust-Level	Niveau de confiance convenu entre les participants, qui définit les exigences de sécurité pour les processus et les composants technologiques. [eCH-0107]
UID	Numéro d'identification des entreprises
Entreprise	Voir *Organisation* [eCH-0107]
User	Voir *Utilisateur* [eCH-0107]
infrastructure de transmission	Voir Broker STIAM
Confiance	Relation de confiance formellement définie entre les services responsables, ex. la description formelle des critères qui doivent être remplies, afin que deux organisations, entités, domaines etc. se fassent mutuellement confiance (Trust en anglais).
Répertoire	Collecte systématique d'informations présentant des caractéristiques communes. [eCH-0107]
Accès	Interaction avec une entité en vue de manipuler ou d'utiliser une ou plusieurs de ses ressources. Les accès sont enregistrés dans un souci de garantir la traçabilité et la vérifiabilité. [eCH-0107]
Contrôle d'accès	Surveillance et commande de l'accès aux *ressources*. Le but est de garantir l'intégrité, la confidentialité et la disponibilité des informations. [eCH-0107]

Annexe E – UseCases STIAM

Use case ‚Standard STIAM'

Use case ‚STIAM Standard'

Le destinataire STIAM exige, pour l'accès à une ressource, que le sujet s'identifie au moyen d'un jeu précis d'Attribute Assertions d'un émetteur STIAM.

Le sujet s'authentifie auprès du Broker STIAM selon une méthode d'identification précise (par exemple nom d'utilisateur / mot de passe ou une méthode d'authentification supérieure à deux facteurs) et demande ensuite l'attribut correspondant d'un émetteur STIAM.

Exemple:

Le sujet demande à accéder à un service de construction, dont la connexion présuppose d'appartenir à une société figurant au registre de l'autorité d'attributs interne à l'entreprise.

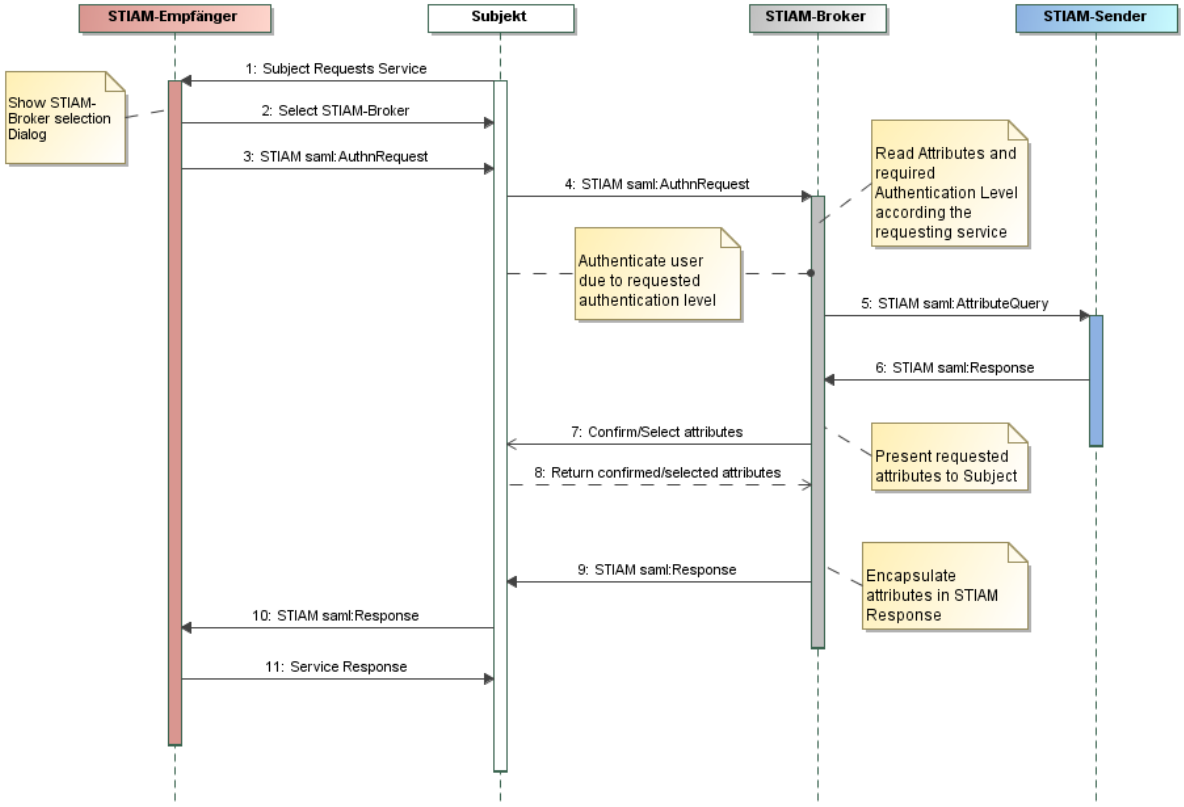

Figure 7 Authentification & Attribute Request STIAM

Use case ‚Demande STIAM combinée'

Pour qu'un sujet puisse accéder à une ressource, le SP STIAM lui impose de s'identifier avec un certain nombre d'Attribute Assertions de plusieurs autorités d'attributs.

Le sujet s'authentifie auprès de l'IdP STIAM par une méthode d'identification interne (par exemple nom d'utilisateur / mot de passe ou une méthode d'authentification supérieure à deux facteurs) et demande ensuite les attributs correspondants de plusieurs émetteurs STIAM. Ceux-ci doivent être agrégés par le Broker STIAM avant la restitution au sujet.

Exemple:

Le sujet demande à accéder à un service de construction étendu, dont la connexion présuppose d'appartenir à une société figurant au registre de l'autorité d'attributs interne à l'entreprise et exige le statut de l'UID correspondant tiré du registre UID.

Use case ‚Autres autorités d'authentification avec requête d'attributs STIAM'

Ce Use case part d'une authentification auprès d'un IdP externe et d'une requête d'attributs auprès d'un émetteur STIAM. L'IdP externe est abordé via un ‚Other-Authn-Plugin'. Le destinataire STIAM fait confiance à l'identification de l'autorité d'authentification externe en raison des critères de qualité définis et garantit les accès d'attributs correspondants. Le Trust naît de la représentation des ‚Other-Authn-Plugin' dans une liste d'autorités d'authentification externes dignes de confiance, qui apparaît sur le Broker STIAM.

Exemple:

Le sujet est authentifié pour l'accès à un portail Web via une autorité externe d'authentification (ex. MobileID).

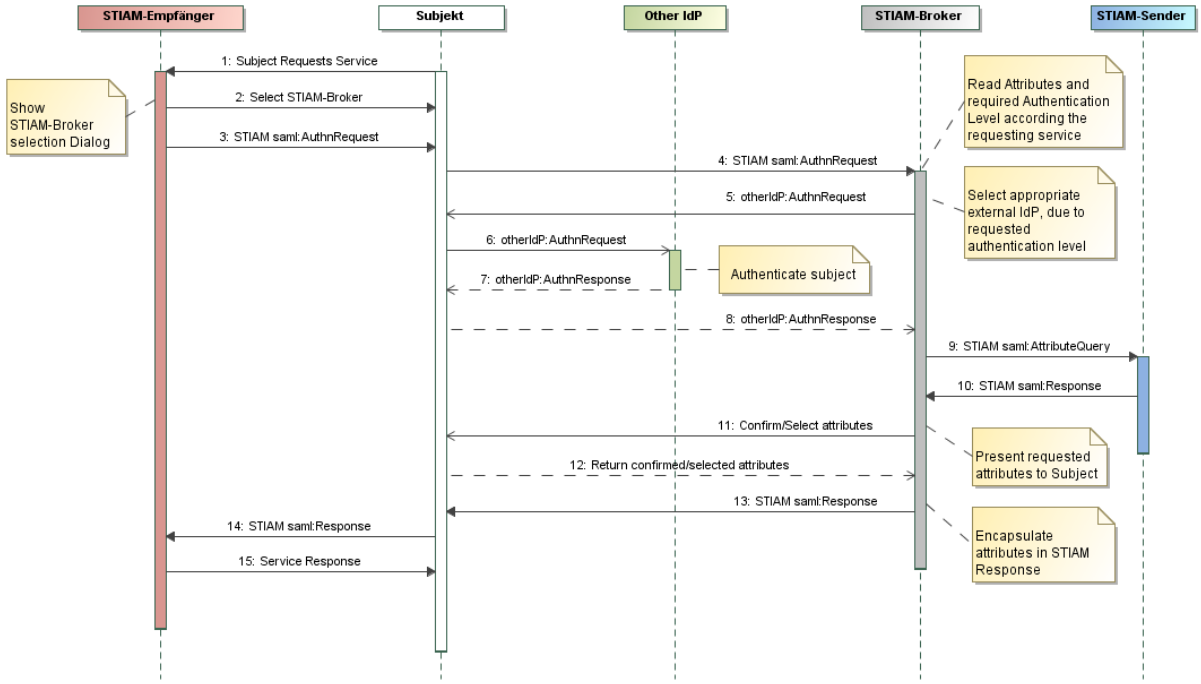

Figure 8 Autre autorité d'authentification avec requête d'attributs STIAM'

Use case ‚Attributs SuisseID Core'

Pour qu'un sujet puisse accéder à une ressource, le SP STIAM exige un attribut du SuisseID-Core Set. Le Broker STIAM transmet la demande directement à l'IdP de SuisseID. Le sujet s'y authentifie. Pour ce Use case particulier, le sujet n'a besoin d'aucun identificateur à l'intérieur de la plateforme STIAM, mais ne peut pas non plus se procurer d'attribut supplémentaire auprès d'une AA issue d'un autre domaine administratif.

Exemple :

Le sujet demande à accéder à une boutique de vins, qui impose de fournir sa date de naissance pour se connecter.

Use case ‚Requête SuisseID CAS'

Ce Use case part d'une demande CAI SuisseID. Il faut pour cela demander un attribut d'un CAS SuisseID. Pour ce faire, il doit y avoir authentification auprès de l'IdP SuisseID, car un CAS SuisseID l'exige par principe. Dans ce cas, les attributs demandés via le Broker STIAM peuvent être fournis et signés par un CAS SuisseID enregistré comme émetteur STIAM, car la spécification CAS SuisseID ne prévoit pas de relation de Trust d'un CAS avec l'environnement IdP SuisseID existant. Ceci permet de rendre accessible à chaque destinataire STIAM et via le Broker STIAM, un service CAS SuisseID (registre des notaires par exemple) avec une certaine qualité et une confiance en résultant via le Broker STIAM.

Exemple:

Le sujet demande à accéder à un service, dont la connexion présuppose une confirmation de notaire que le sujet peut demander auprès du registre des notaires CAS SuisseID.

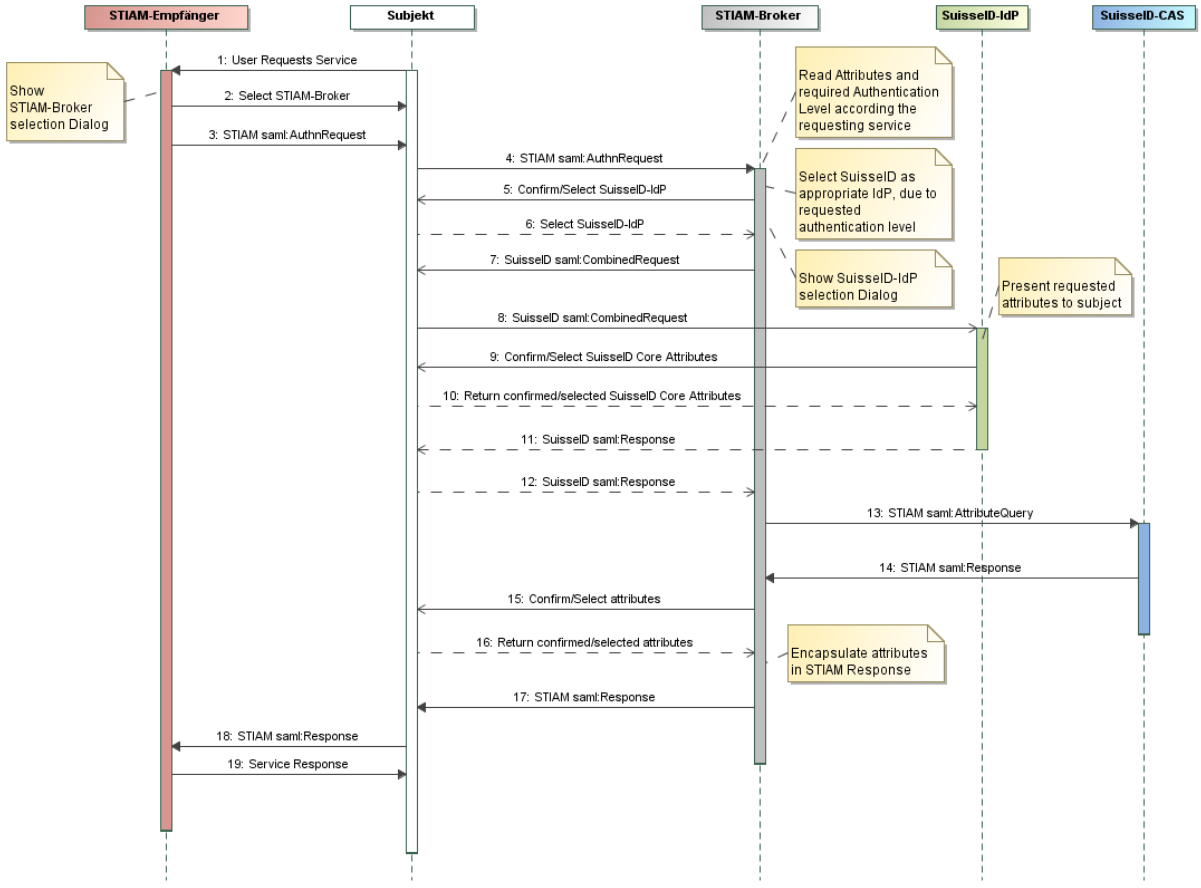

Figure 9 Authentification et requête CAS SuisseID via Broker STIAM