eCH-0168 Architecture technique et processus SuisseTrustIAM

Titre	Architecture technique et processus SuisseTrustIAM
Code	eCH-0168
Type	Norme
Stade	Expérimental
Version	1.0
Statut	Approuvé
Validation	2014-11-26
Date de publication	2015-01-06
Remplace	--
Annexes	Aucune
Dépendances	eCH-0107, eCH-0167 et eCH-0169
Langues	Allemand (original), français (traduction)
Auteur(s)	Groupe spécialisé IAM Annett Laube-Rosenpflanzer, HESB annett.laube@HESB.ch Gerhard Hassenstein, HESB, gerhard.hassenstein@HESB.ch Stefan Agosti, HESB, stefan.agosti@HESB.ch Hans Häni, HESB, hans.haeni@HESB.ch Marcel Vinzens, Adnovum, marcel.vinzens@adnovum.ch Urs Pfenninger, Zurich, urs.pfenninger@zuerich.ch Daniel Leiser, Atos AG, daniel.leiser@atos.net
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 permet d'échanger, de manière simple, des identités numériques par delà les limites des entreprises afin de faciliter les processus administratifs. SuisseTrustIAM est une infrastructure de transmission générique, sur laquelle peuvent être représentées les Identity Federations et les solutions IAM.

Ce document propose une description technique mais technologiquement neutre de l'architecture de la plateforme SuisseTrustIAM. Il s'agit concrètement de modéliser et d'expliquer les protocoles de communication, le modèle de données et les processus administratifs de l'infrastructure de transmission SuisseTrustIAM.

Une série d'autres documents a été élaborée dans le cadre de la spécification de SuisseTrustIAM. Ce document vient, d'une part, compléter eCH-0167, Concept cadre de SuisseTrustIAM' et est, d'autre part, référencé dans eCH-0169 ‚Architecture administrative de SuisseTrustIAM.

Sommaire

Statut du document

Approuvé: le Comité d'experts a ***approuvé*** le présent document, lui conférant force normative pour le domaine d'application défini et dans les limites de validité fixées.

Notation

Les mots clés *DOIT*, *NE DOIT PAS, REQUIS*, *DEVRAIT*, *NE DEVRAIT PAS*, *RECOMMANDÉ*, *PEUT* et *FACULTATIF* dans ce document doivent être interprétés selon les descriptions fournies dans IETF RFC 2119 [1].

1 Introduction

Remarque linguistique: dans un souci de meilleure lisibilité, les désignations de personne seront utilisées uniquement sous la forme masculine ou féminine. Ces formulations couvrent ainsi automatiquement l'autre genre de manière implicite.

1.1 Classement

Les concepts pour les solutions IAM fédérées et les ressources supplémentaires reposent sur la norme eCH-0107 [2]. Les concepts sont des descriptions concrètes de la forme que doit prendre une proposition de solution IAM et contiennent des sous-cadres et architectures devant être pris en compte lors de la mise en œuvre. Par ailleurs, des ressources, qui mettent des informations complémentaires à disposition et qui sont pertinentes pour plus d'un concept, sont proposées pour les concepts. Les modèles de qualité et de maturité représentés sont des exemples de ressources et ne sont pas définitifs.

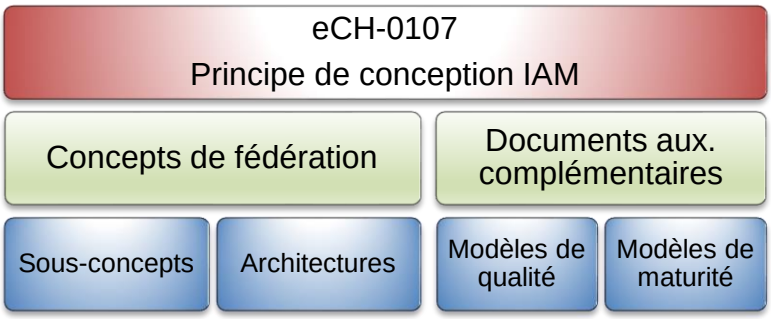


Figure 1: classement de la norme eCH-0168

La présente norme eCH-0168 s'inscrit en tant que proposition d'architecture IAM dans la hiérarchie des documents de solutions IAM fédérées et s'appuie par conséquent sur les documents déjà publiés eCH-0107 [2] et le concept cadre SuisseTrustIAM eCH-0167 [3]. En outre, renvoi est fait aux documents eCH-0170 [4] et eCH-0171 [5] qui définissent les modèles de qualité pour les identités électroniques et la confirmation des attributs.

1.2 But du document

Les structures de données et les processus modélisés dans ce document ainsi que les protocoles utilisés devraient fournir des informations nécessaires à la mise en œuvre des fonctions d'un Hub STIAM et de leurs interactions avec les composants périphériques Relying Party (destinataire STIAM), Identity Provider et Attribute Authority (expéditeur STIAM).

1.3 Structure du document

Le présent document décrit l'architecture de la plateforme SuisseTrustIAM du point de vue technique. Après les définitions terminologiques au chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.** la structure fondamentale du modèle d'Identity Federation de SuisseTrustIAM est expliquée dans une première partie principale [chapitre 3]. Ce chapitre traite également plus en détail de certaines propriétés du modèle et explique les fonctions spécifiques. Le chapitre 4 regroupe les exigences découlant du modèle d'Identity Federation et les descriptions de fonctions récapitulatives pour les différents composants (Hub STIAM, expédi-

teur STIAM, IdP STIAM et destinataire STIAM). Ensuite [chapitres 5 et 6] les protocoles utilisés dans le système SuisseTrustIAM pour la durée d'exécution et de définition sont illustrés et décrits sous forme détaillée. Les processus administratifs et le modèle de données du Hub STIAM sont illustrés dans une troisième partie [chapitre 7].

1.4 Délimitation

Ce document a pour priorité principale de décrire l'architecture de l'infrastructure centrale de transmission et de ses interfaces: le document définit les exigences imposées au système global et les différents composants (Hub STIAM, expéditeur STIAM, IdP STIAM et destinataire STIAM). Les protocoles concernant la durée d'exécution et de définition sont en outre décrits de manière détaillée mais indépendamment de la technologie.

La mise en œuvre des concepts décrits, ainsi que les spécifications concrètes, relatives à la technologie, des interfaces et les fonctions de l'expéditeur et du destinataire STIAM font l'objet d'un traitement distinct dans un document séparé (Best Practice)[1].

Ce document vient compléter le Concept cadre de SuisseTrustIAM eCH-0167 [3]. Il précise les concepts, qui y sont présentés, dans le but de jeter les bases d'une mise en œuvre.

L'idée fondamentale du STIAM est de fournir une structure de transmission des informations entre organisations. Les concepts peuvent également être utilisés pour la mise en place d'une Identity Federation interne à l'organisation, mais doivent alors être adaptés aux exigences spéciales de cette organisation et complétés en conséquence.

[1] Il n'existe pas encore de désignations précises pour les documents de Best Practice prévus par l'association eCH.

2 Terminologie

Bon nombre des termes employés dans ce document ont déjà été décrits dans les documents eCH-0107 [2] et eCH-0167 [3]. C'est la raison pour laquelle l'idée d'une définition terminologique détaillée a été abandonnée. Ce chapitre fournit toutefois une explication de quelques termes, qui ne sont pas traités ou traités seulement en marge dans les deux documents évoqués.

2.1 Attribute Assertion

Une Attribute Assertion est la confirmation d'un attribut par une autorité d'attributs (voir eCH-0107 [2]). L'Attribute Assertion peut être une Attribute Assertion SAML 2.0, mais également reposer sur une autre technologie.

2.2 Attribute Aggregation

Le terme Attribute Aggregation est décrit de façon plus précise par N. Klingenstein dans «Attribute Aggregation and Federated Identity» [6]. Ce que l'on entend par là, c'est le processus consistant à demander les attributs se rapportant à une identité numérique connue auprès de plusieurs sources en vue de les compiler.

2.3 Domaine STIAM

Un groupe limité de bénéficiaires et de fournisseurs d'informations, partageant un certain jeu d'attributs et une politique (Policy) commune, peut être considéré comme un domaine. La sémantique et la syntaxe de ces attributs sont stipulées par les participants du groupe. A titre d'exemple, il devrait être possible de constituer, à l'intérieur de SuisseTrustIAM, une sous-fédération n'échange qu'en interne ses identités et attributs connus.

2.4 Discovery Service (WAYF - Where Are You From)

Le Discovery Service est compétent pour guider l'utilisateur vers un Identity Provider de son choix à des fins d'authentification.

2.5 Composant destinataire

Le composant destinataire réalise une interface STIAM normalisée pour un Relying Party, qui n'est pas directement compatible avec les protocoles STIAM (cf. Figure 2).

2.6 GUID

Une GUID est l'identité unique d'un sujet, enregistrée sur le Hub STIAM, à laquelle renvoie la LinkedID dans son Link Table (tableau des liens).

2.7 Identity Linking

L'Identity Linking est l'opération par laquelle une LinkedID est associée à une identité numérique unique d'un sujet. Les informations nécessaires à cette fin sont enregistrées dans un Link Table.

2.8 Identity Provider/ autorité d'attributs (IdP/AA)

Dans le contexte SuisseTrustIAM, des entreprises et des organisations peuvent, en tant que fournisseurs d'informations, mettre à disposition un composant IdP/AA, qui agit comme un IdP, mais peut également fournir des informations sous forme d'attributs concernant une identité qu'il connaît. Les exigences imposées à un tel IdP/AA et à ses fonctions sont décrites plus précisément dans les documents SuisseTrustIAM (cf. également IdP STIAM, expéditeur STIAM et Figure 2).

2.9 Linking Protocole

L'utilisateur peut associer les IdP ou les AA dans le Link Table de son Account (compte). Pour obtenir l'identificateur correct en tant qu'entrée dans le Link Table, l'utilisateur doit s'authentifier auprès du service d'authentification concerné. Il est ainsi possible d'échanger un identificateur unique entre le Hub STIAM et l'IdP ou l'AA.

2.10 Métadonnées (Metadata)

Dans SuisseTrustIAM, les métadonnées pour les composants STIAM inscrits sont enregistrées au niveau central dans la base de données Hub STIAM, dans le cadre de la gestion de l'organisation et des composants. Les métadonnées décrivent les composants des organisations et des Provider inscrits avec leurs points terminaux de Federation Service, les certificats et les attributs demandés ou mis à disposition.

2.11 OpenID Connect

OpenID Connect 1.0 (OIDC) [7] définit une couche d'identité simple sur la base d'OAuth 2.0 (RFC 6749), qui peut également être utilisée par les appareils mobiles. OIDC utilise le protocole de base OAuth tant pour l'authentification que pour le contrôle d'accès. Les Security Tokens utilisés sont les Web Tokens JSON [8].

2.12 RP (Relying Party, fournisseurs de solution, bénéficiaires d'informations)

Les entreprises et les organisations peuvent se présenter comme des bénéficiaires d'informations (portail Web avec accès contrôlé à une ressource). Dans le cadre de ce rôle, elles ont besoin d'informations concernant un utilisateur souhaitant un accès, afin de lui autoriser ou de lui refuser l'utilisation de la ressource.

2.13 SAML 2.0

SAML (Security Assertion Markup Language) permet d'échanger des informations concernant l'authentification et les attributs à des fins d'autorisation, entre plusieurs participants et de façon normalisée. La norme SAML [9] décrit la syntaxe et les règles pour demander, créer et échanger des SAML Assertions.

2.14 Profils SAML 2.0 Web Browser SSO

Les profils regroupent des cas d'application spéciaux de SAML. Le profil SAML 2.0 Web Browser SSO (single-sign-on) [10] décrit les scénarios d'authentification basés sur le Web, y compris l'Identity Federation, pour les navigateurs.

2.15 Protocole SAML

En introduisant SAML, OASIS a défini non seulement le SAML Token, mais aussi un protocole et des Bindings, qui spécifient la transmission des Tokens. SAML est notamment compatible avec HTTP-POST et HTTP-Redirect en tant que Request Response Schema. Hormis SAML, il existe d'autres protocoles compatibles avec les Tokens SAML. WS-Federation et WS-Trust (cf. chapitre 2.25 et 2.26) en sont deux exemples.

2.16 SAML Token

Un SAML Token comprend, sous forme normalisée, des informations d'identité confirmées concernant un sujet. Le point central d'un SAML Token est l'Assertion. Celle-ci stipule à qui appartient le Token, quelle est sa durée de validité, qui l'a délivrée puis les informations d'identité du sujet et les éventuels attributs qui y sont associés.

2.17 Composant expéditeur

Le composant Expéditeur réalise une interface STIAM normalisée pour la connexion au Hub STIAM (cf. Figure 2), d'une autorité d'attributs, qui ne sont pas directement compatibles avec les protocoles STIAM.

2.18 Security Token

Un Security Token comprend des informations d'identité confirmées concernant un sujet, sous une forme normalisée (Authentication Statement, Authentication Assertion). Un Relying Party vérifie et valide ces informations avant de prendre une décision concernant l'accès.

2.19 STIAM Certificate Service Provider (STIAM-CSP)

Un STIAM-CSP est un CSP, qui est accepté par la Community STIAM.

2.20 Destinataire STIAM

Le destinataire STIAM a recours aux services du Hub STIAM pour pouvoir authentifier un utilisateur et se procurer d'autres informations à son sujet, qui pourront ensuite être utilisées afin de commander l'accès. Le destinataire STIAM définit comment l'utilisateur devrait être authentifié et quels attributs sont nécessaires et dans quelle qualité, afin d'autoriser l'accès à l'une de ses ressources protégées. Le destinataire STIAM obtient du Hub STIAM les informations demandées sous forme de Security Token. Le destinataire STIAM est un Relying Party, un portail par exemple.

2.21 Hub STIAM (Broker, intermédiaire)

Véritable cœur de la plateforme SuisseTrustIAM, le Hub STIAM remplit deux fonctions. Premièrement, il propose les services administratifs Trust et eIdentity pour la durée de définition, les utilisateurs et les organisations pouvant s'inscrire sur le Hub STIAM. Deuxièmement, il agit en tant qu'intermédiaire (Broker) entre les entités pour la durée d'exécution.

Les tâches administratives sur le Hub STIAM peuvent être réparties grossièrement entre les processus et les fonctions suivantes (cf. à ce sujet les processus administratifs au chapitre 7):

- *User Management:* les utilisateurs peuvent ouvrir un compte utilisateur (User Account) sur le Hub STIAM et le gérer. A titre alternatif, il est également possible pour le System Administrator d'une organisation de créer des User Accounts pour un (ou plusieurs) utilisateur(s) ou machine(s).
- *Organisation Management:* une organisation est initialement ouverte par l'exploitant SuisseTrustIAM dans la base de données. A cet égard, un collaborateur de l'organisation (dans le rôle d'un responsable d'organisation) est habilité à administrer certaines propriétés de l'organisation et à créer et à habiliter des administrateurs système supplémentaires. Il est ainsi possible de séparer et de déléguer les tâches administratives de l'organisation (cf. à ce sujet la définition des rôles et processus dans eCH-0169 Architecture administrative SuisseTrustIAM [11]).
- *Component Management:* l'objectif de l'administration centrale sur le Hub STIAM est de permettre au responsable système de gérer, de manière simple et autonome, les composants STIAM. Celui-ci peut ajouter et administrer de manière autonome les différents composants pour SuisseTrustIAM. Pour ces composants, il faut saisir et configurer certains paramètres, qui sont nécessaires pour leur rôle à l'intérieur de la plateforme STIAM.
- *Attribut Management:* l'exploitant SuisseTrustIAM gère une liste d'attributs, qui peuvent être utilisés dans la Community SuisseTrustIAM.

2.22 IdP STIAM

Dans STIAM, un Identity Provider a pour fonction d'authentifier un sujet. Un IdP STIAM implémente une interface STIAM standardisée avec le Hub STIAM (cf. Figure 2).

2.23 Composants STIAM

L'expéditeur STIAM (autorité d'attributs), le destinataire STIAM (Relying Party), l'IdP STIAM, le Hub STIAM et les CSP STIAM font partie des composants STIAM. Les composants STIAM possèdent une interface standardisée, qui leur permet de communiquer les uns avec les autres et de se faire mutuellement confiance.

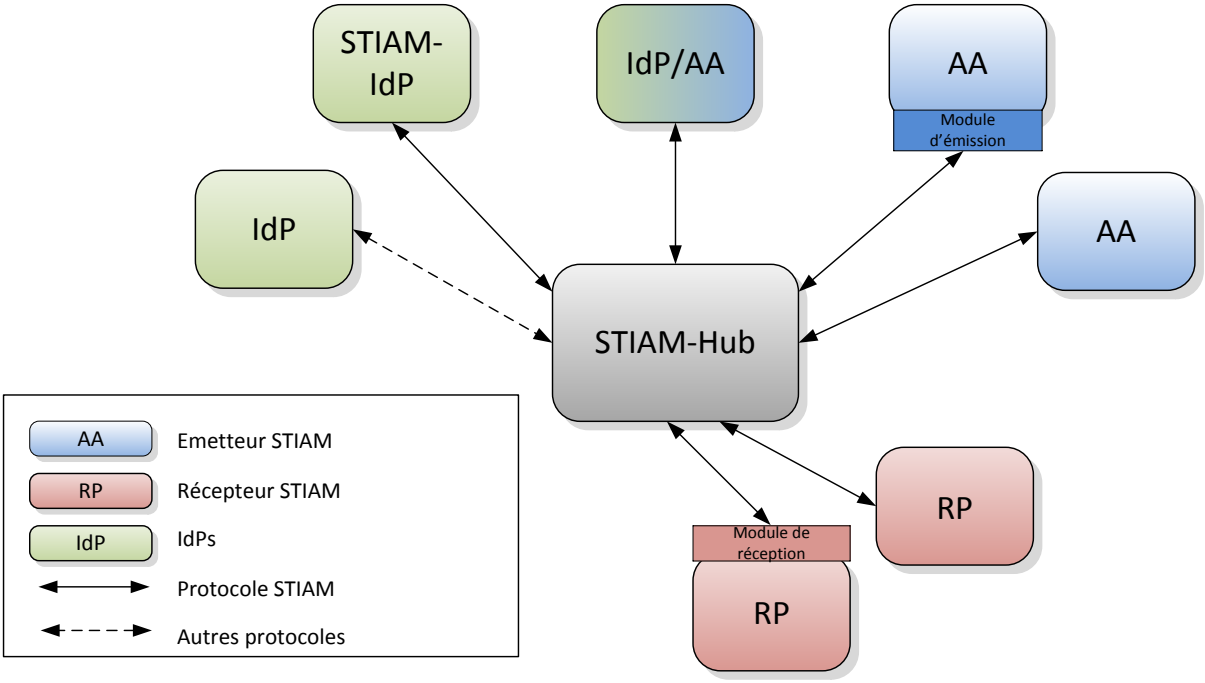


Figure 2: composants STIAM

2.24 Expéditeur STIAM

L'expéditeur STIAM est une autorité d'attributs (des répertoires ou des registres en règle générale), qui met les attributs à la disposition de la Community STIAM sous forme normalisée.

L'expéditeur STIAM a une interface standardisée avec le Hub STIAM (cf. Figure 2).

2.25 WS-Federation

WS-Federation dans la version actuelle 1.2 [12] [13] fait également partie de la spécification WS* et ajoute à WS-Trust la possibilité d'échanger aussi des Security Tokens via différents domaines, la norme étant compatible avec plusieurs Identity Providers. On peut utiliser le format de Token SAML comme Security Tokens (jetons de sécurité) tant pour WS-Trust que pour WS-Federation.

2.26 WS-Trust

Le Web Service Trust (WS-Trust) [14] spécifié par OASIS, dans la version actuelle 1.4, fait partie de la spécification WS*, qui met à disposition un Framework (cadre) pour l'échange sûr de messages Web Service. Bei WS-Trust, il s'agit d'une norme, qui favorise l'interopérabilité des Security Tokens par la définition d'un protocole pour les exigences et les réponses. Ce protocole permet à un Consumer (consommateur ex. un Web Service Client), de demander l'échange d'un Security Token particulier auprès d'un émetteur reconnu, le Security Token Service (STS), et de le transmettre à un Relying Party.

3 Modèle d'Identity Federation SuisseTrustIAM

3.1 Concept SuisseTrustIAM

Le but d'un Hub (plateforme) STIAM est de connecter fournisseurs et consommateurs d'informations de manière simple et, dans le même temps, de les anonymiser mutuellement. Dans un environnement d'Identity Federation classique, l'Identity Provider, en tant que fournisseur d'informations, et les Relying Parties, en tant que consommateurs d'informations, sont en relation directe. Dans ce modèle, le Hub STIAM agit vis-à-vis des consommateurs d'informations comme un Broker (intermédiaire) d'informations sécurisées concernant une identité numérique. En outre, il anonymise vis-à-vis des participants des deux niveaux, les protocoles discutés, l'échange d'informations nécessaires entre les participants et la structure incontournable des relations de confiance. L'interopérabilité des différents participants peut ainsi être simplifiée, en particulier lorsque le nombre de participants est élevé.

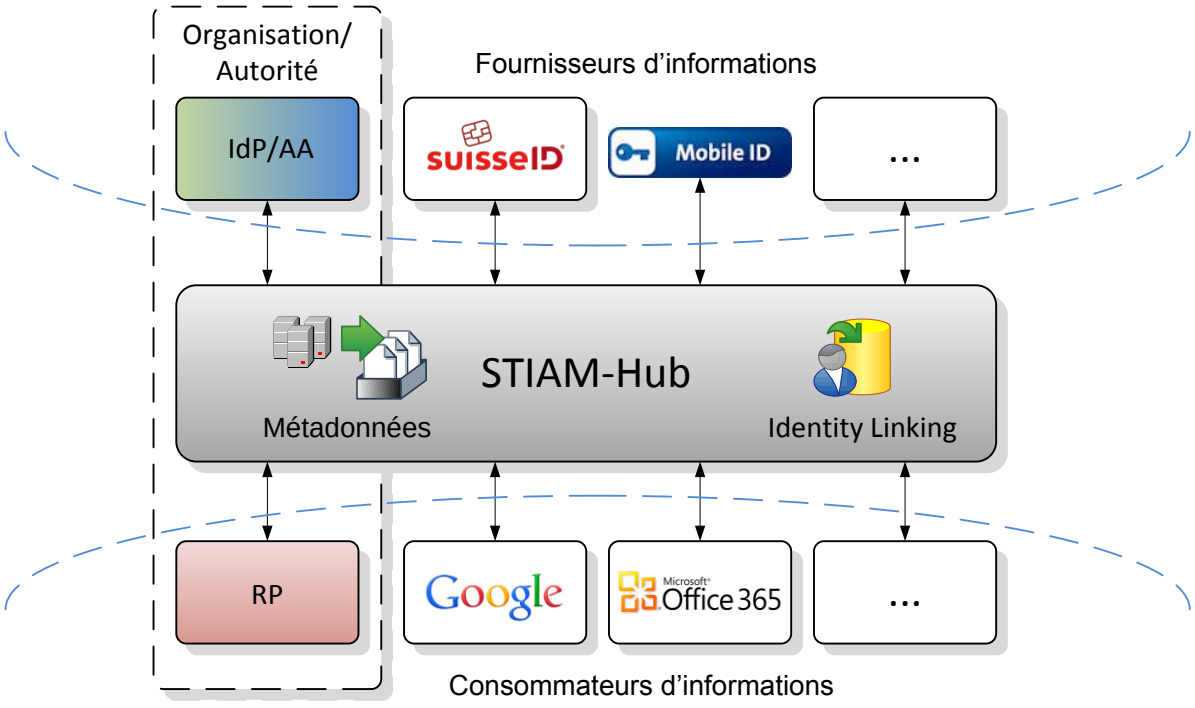


Figure 3: Hub STIAM et services

En tant que client de cette infrastructure, une organisation (autorité, entreprises) peut intégrer ses propres applications comme Relying Parties (RP), afin de faire authentifier par l'un des fournisseurs d'informations connectés, les utilisateurs y accédant. A l'inverse, cette organisation peut être elle-même fournisseur (IdP/AA) d'identités numériques et d'informations d'attributs pour ses propres consommateurs ou d'autres consommateurs. Cependant, il est également possible d'intégrer des solutions Cloud existantes, telles que Google-Mail ou MS-Office 365, en tant que consommateurs d'informations. Afin de permettre l'administration des services des participants connectés et de faire connaître mutuellement, le Hub STIAM gère une base de métadonnées (Metadata) des systèmes affiliés. Pour pouvoir compiler les informations souhaitées d'un sujet, le Hub STIAM a besoin pour chaque sujet d'un type de

Link Table (Identity Linking) lui permettant de classer les identités numériques disponibles de façon décentralisée auprès des fournisseurs d'informations.

3.2 Modèle de Hub STIAM

Différents concepts d'Identity Federation ont déjà été présentés dans la norme eCH-0107 Principes de conception pour l'administration des identités et de l'accès. Le présent chapitre traite, de manière approfondie et illustrée, des modèles pertinents pour SuisseTrustIAM. La plateforme SuisseTrustIAM consiste en un modèle *Hub-,n'-Spoke*[2] (modèle Hub STIAM). Ce modèle repose sur un Hub STIAM central, auquel toutes les parties impliquées font confiance.

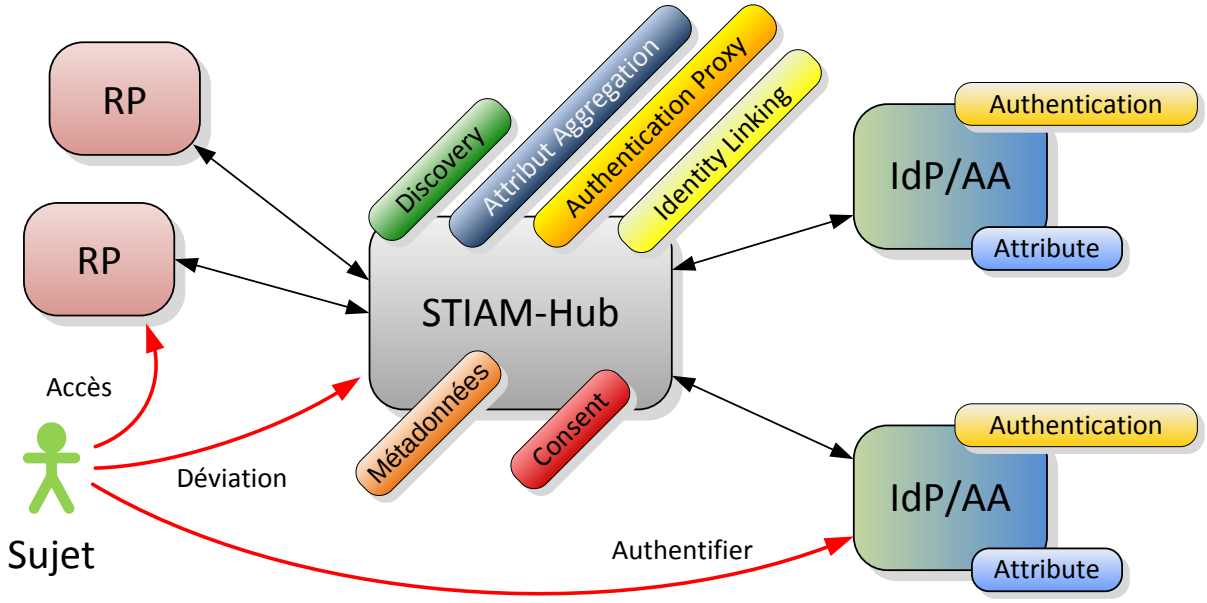


Figure 4: modèle de Hub STIAM

Dans la Figure 4, les flèches noires marquent les relations de communication entre les différents composants.

Les flèches rouges illustrent les interactions du sujet:

- Accès: le sujet souhaite accéder à une ressource protégée d'un Relying Party.
- Déviation: le Relying Party ordonne une déviation du sujet vers le Hub STIAM, où l'Identity Provider est sélectionné à l'aide du service Discovery.
- Authentifier: le Hub STIAM guide le sujet vers l'Identity Provider sélectionné, où le sujet peut à présent s'authentifier.

Comme le montre la Figure 4, le Hub STIAM peut se charger de différents services à l'intérieur de l'Identity Federation et les exercer au niveau central:

Discovery: le Hub STIAM est compétent pour guider l'utilisateur (sujet) vers un Identity Provider de son choix à des fins d'authentification. Il indique au sujet une sélection d'Identity

[2] Nabe & Speiche

Providers potentiels, ou le guide directement vers l'unique IdP possible à des fins d'authentification.

Authentication Proxy: en règle générale, le Hub STIAM n'authentifie pas lui-même un sujet. Il agit plutôt comme un intermédiaire d'authentification (Proxy), en se comportant comme un Relying Party à l'égard de l'IdP authentifiant et en lançant une requête en ce sens sous son propre nom.

Attribute Aggregation: une fois l'authentification effectuée auprès d'un Identity Provider, le Hub STIAM doit être en mesure d'associer à l'identité du sujet, des informations supplémentaires (Attribute) demandées par un Relying Party, provenant des fournisseurs d'attributs possibles, et de renvoyer au RP requérant.

Metadata: le Hub STIAM gère et fait office d'intermédiaire pour toutes les informations nécessaires entre les composants et établit ainsi les relations de confiance entre ceux-ci. Les métadonnées tenues à jour par le Hub au niveau central contiennent les informations de tous les IdP/AA et de tous les RP. Ces métadonnées sont signées numériquement par le Hub STIAM et représentent ainsi une troisième instance digne de confiance (Trusted Third Party).

Consent: avant que la garantie d'une authentification (*Authentication Statement*) ou un jeu d'attributs puissent être transmis à un Relying Party, l'utilisateur doit approuver la transmission.

Identity Linking[3]*:* quand un Relying Party exige – pour l'accès à une ressource dont il a le contrôle – des attributs de différentes sources, tant le Hub STIAM que cette source d'informations (autorité d'attributs) doivent offrir une possibilité de savoir pour quel utilisateur, qu'il connaît localement, il doit fournir un attribut. Tous les services fournissant des informations et le Hub STIAM doivent disposer d'un ou de plusieurs identificateurs, par le(s)quel(s) ils peuvent classer sans ambigüité l'identité numérique du sujet. Dans le cadre du User Management (gestion des utilisateurs), le Hub STIAM doit gérer un Link Table, dans lequel un utilisateur peut enregistrer ses identificateurs au niveau central.

La liste des services centralisés n'est pas préalablement prescrite dans le modèle Hub STIAM. L'exercice des différents services peut également rester réparti. Il est ainsi tout à fait envisageable que le consentement (Consent) à la validation de l'authentification ou des attributs reste du ressort de l'IdP/AA.

3.3 Procédé pour la transmission des identités et d'attributs

La plus importante différence avec un modèle classique d'Identity Federation (Cross Domain ou modèle full-meshed) réside dans le fait que le RP et l'IdP/AA ne communiquent plus directement, mais mène la communication exclusivement via le Hub STIAM pour la durée d'exécution.

Il en résulte que celui-ci doit, en remplacement du Relying Party, amorcer l'authentification du sujet auprès d'une IdP et se charger de l'agrégation des informations demandées. Selon

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

ce scénario, différents IdP/AA peuvent être les sources compétentes pour l'authentification et pour les attributs d'utilisateur.

C'est à ce modèle que correspond SuisseTrustIAM, car si un sujet peut être authentifié par un Identity Provider de son choix, les informations sur les attributs en revanche peuvent provenir d'autres sources.

En fonction du nombre de fournisseurs d'attributs impliqués dans une requête et de leur relation avec l'Identity Provider authentifiant, le Hub STIAM peut choisir différents procédés pour l'Attribute Aggregation. Il existe en principe deux procédés dont le déroulement diffère et qui sont présentés dans la suite du document.

3.3.1 Proxying

Le Proxying consiste pour un composant à l'origine d'une requête (le Hub STIAM dans notre cas) à envoyer une requête séquentielle via plusieurs destinations. La dernière destination dans la chaîne est l'Identity Provider authentifiant. Une fois le sujet authentifié, chaque IdP/AA (proxy d'authentification) intermédiaire va ajouter les attributs relevant de sa compétence. Le procédé implique cependant que tous les fournisseurs d'informations impliqués connaissent les identificateurs (UID) de l'IDP/AA authentifiant pour chacun des sujets possibles. Ce procédé convient donc tout particulièrement aux scénarios suivants:

- Le Hub STIAM agit lui-même en tant que fournisseur d'attributs unique dans la chaîne entre le RP et l'IdP/AA authentifiant.
- L'Identity Provider authentifiant et les fournisseurs d'attributs impliqués partagent un identificateur déjà convenu et échangé au préalable.
- La chaîne des fournisseurs d'attributs impliqués est relativement courte et se compose de serveurs robustes et d'une grande disponibilité.

Pour parvenir à cet identificateur, le fournisseur d'attributs peut le faire saisir par l'utilisateur lui-même ou le faire confirmer électroniquement par l'IdP/AA dans le cadre d'un processus d'enregistrement.

L'intégration d'un SuisseID Claim Assertion Service (CAS) constitue un bon exemple d'Attribute Aggregation avec Proxying dans le SuisseTrustIAM, l'IdP/AA authentifiant(e) devant être dans ce cas l'IdP SuisseID.

La Figure 5 représente la façon dont tous les fournisseurs d'informations impliqués doivent disposer, de manière décentralisée, du même identificateur (UID) d'un sujet, afin que chacun des composants impliqués puisse classer sans ambigüité l'identité numérique du sujet. Les identificateurs locaux peuvent être enregistrés dans les bases de données d'utilisateur (User DB). Les UID de l'IdP/AA authentifiant avec les identificateurs locaux peuvent être classés via un Mapping Table.

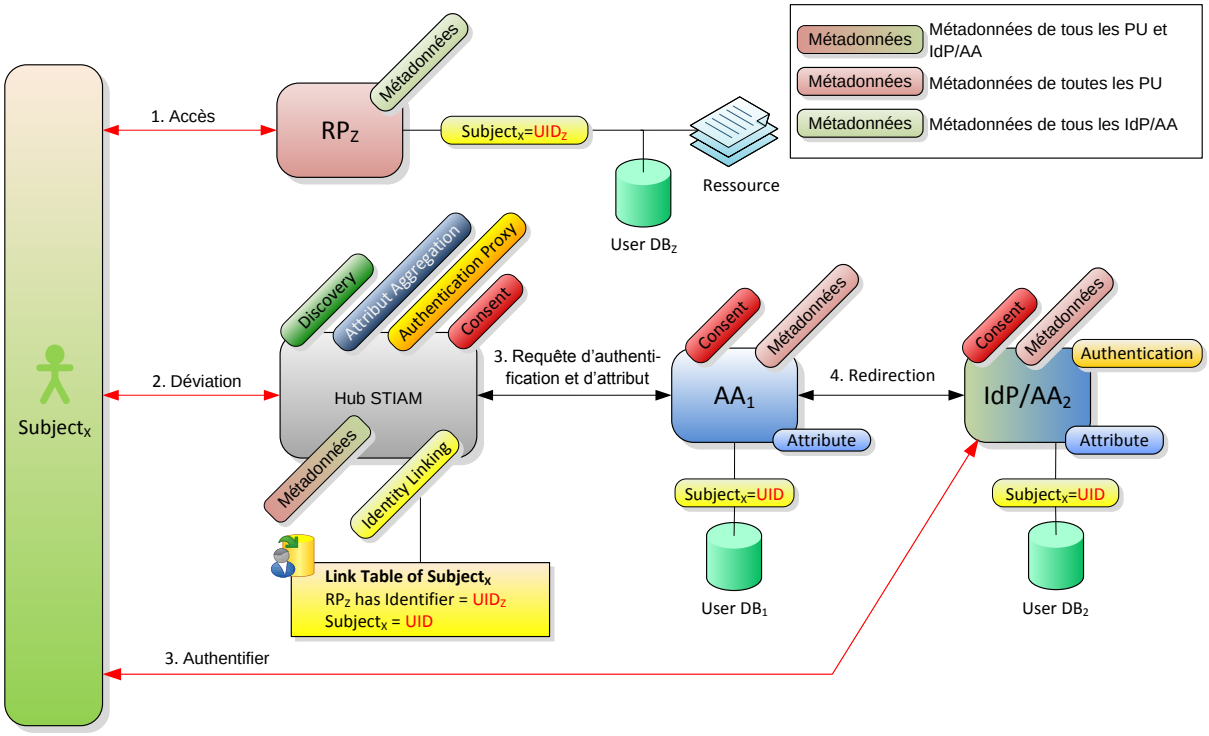


Figure 5: transmission d'identité et d'attributs par Proxying

Dans ce scénario, un utilisateur ($Subject_X$) accède à un Relying Party (RP_Z). Le Relying Party redirige l'utilisateur vers le Hub STIAM. Ce dernier peut déduire des métadonnées du RP que l'on a besoin des attributs d'AA_1, mais que l'utilisateur doit s'authentifier auprès de l'IdP/AA_2. Le Hub crée un chemin de proxy avec l'AA_1 comme première destination et l'IdP/AA_2 comme serveur authentifiant (2ème destination). Il dévie vers l'AA_1, l'utilisateur avec cette information concernant le chemin. Celle-ci reconnaît au moyen du chemin de proxy qu'il doit tout d'abord rediriger l'utilisateur vers l'IdP/AA_2. L'IdP/AA_2 authentifie l'utilisateur, joint les attributs mis à disposition par lui-même et le renvoie à l'AA_1. Sa réponse contient l'UID de l'utilisateur, de sorte que l'AA_1 reconnaisse à présent l'identité de l'utilisateur et puisse maintenant ajouter également ses attributs. Il renvoie l'information désormais complète au Hub, qui contrôle l'authentification effectuée et les différents attributs et les renvoie au RP dans une Assertion propre en tant que confirmation.

3.3.2 Transmission d'identité aux AA

Lorsqu'une même requête contient plusieurs fournisseurs d'attributs indépendants, ils ne disposent en règle générale pas d'identificateur communément connu. C'est là qu'intervient le Link Table du Hub STIAM, dans lequel les identificateurs des fournisseurs d'attributs sont à présent enregistrés de façon décentralisée pour chaque sujet. Ceci permet au Hub STIAM, une fois effectuée l'authentification des utilisateurs auprès d'un Identity Provider, de se procurer les attributs qui font encore défaut en adressant une requête directe aux fournisseurs d'attributs. A cette fin, il envoie au préalable une unsolicited[4] Authentication-Response aux fournisseurs d'attributs (cf. à ce sujet le rapport sur SuisseTrustIAM PoC [15] d'ATOS).

[4] unsolicited message: message non sollicité

Comme le montre la Figure 6, le Linking Service permet à l'utilisateur de gérer de façon centralisée et dans un tableau, les identificateurs pour les sources compétentes. Grâce à ce Link Table, il est possible, au terme d'une authentification réussie, d'effectuer des demandes d'attributs dans un ordre indéterminé directement auprès des sources compétentes.

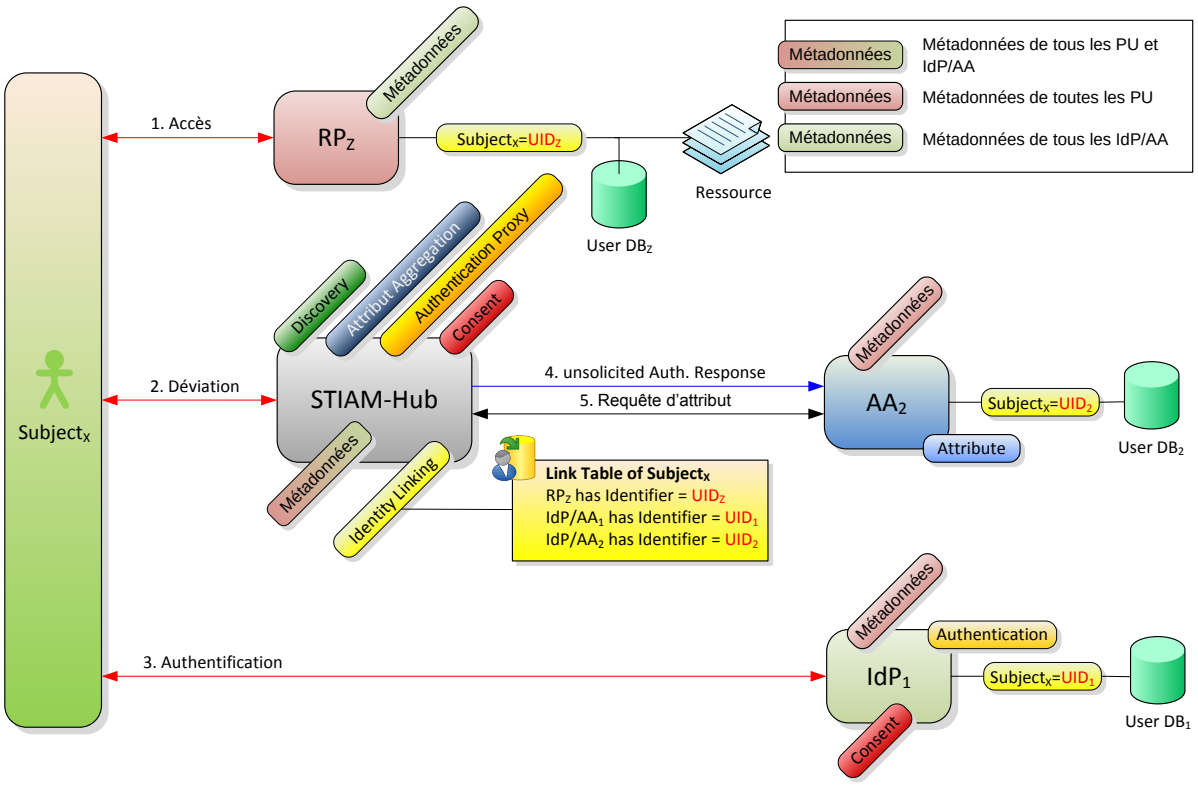


Figure 6: transmission d'identités et d'attributs au moyen de solicited Messages

Dans ce scénario, un utilisateur accède à un Relying Party (RP_z). Le Relying Party redirige l'utilisateur vers le Hub STIAM. Le Hub peut déduire des métadonnées du RP que l'on a besoin des attributs de AA_2, mais que l'utilisateur doit s'authentifier auprès de l'IdP/AA_1. Le Hub redirige tout d'abord l'utilisateur vers l'IdP_1 afin qu'il s'y authentifie. Une fois l'authentification effectuée, le Hub STIAM connaît l'utilisateur et peut en déduire l'identificateur pour l'AA_2 au moyen du Link Table. Il commence par envoyer une ‚unsolicited' Authentication Response avec l'UID_2 à l'AA_2 (en bleu sur la Figure 6). Il peut ensuite déposer une requête directe pour un jeu particulier d'attributs auprès de l'AA_2. L'AA_2 vérifie la requête du Hub et répond avec l'Attribute Assertion souhaitée. Le Hub, qui a contrôlé l'authentification effectuée et a vérifié lui-même les différents attributs, crée sa propre Assertion et la renvoie au RP.

3.4 Validation des informations sur les identités et les attributs

Dans le modèle SuisseTrustIAM, le Hub STIAM transmet des informations sur les identités et les attributs (Security Tokens, Attribute Assertions), qui sont émises, infalsifiables, par les sources compétentes par rapport au Relying Party. En fonction de l'exigence du Relying Party, cela peut être effectué selon deux modes différents.

3.4.1 Identity Proxying Mode (IP Mode)

Le Hub STIAM reçoit, pour la durée d'exécution, les Security Tokens et Assertions émis par l'Identity Provider en charge de l'authentification respectivement par les fournisseurs d'attributs et les valide lui-même. A partir de ceux-ci, il génère un nouveau Token (ou une Assertion) provenant de lui et portant une signature numérique, et le transmet au Relying Party. Dans ce cas de figure, le Relying Party ne peut valider que les Assertions du Hub STIAM. Le Relying Party doit donc faire pleinement confiance aux affirmations du Hub STIAM.

3.4.2 Identity Relaying Mode (IR Mode)

Le Hub STIAM reçoit, pour la durée d'exécution, les Security Tokens et Assertions émis par l'Identity Provider en charge de l'authentification respectivement par les fournisseurs d'attributs, mais ne les valide pas. Il produit une réponse pour le Relying Party, qui contient l'original de tous les Tokens et Assertions demandés, et les envoie au Relying Party. Le RP commence par valider l'authenticité du Hub STIAM, puis celle des Tokens et Assertions intégrés dans le message. Sous ce mode, le Relying Party peut vérifier directement les affirmations des sources émettrices et ne doit donc pas se fier qu'au seul Hub STIAM. Pour se procurer les informations nécessaires (certificats) à la validation des Tokens et Assertions, le Relying Party doit se reporter aux métadonnées.

3.5 Security Token et protocoles STIAM

En tant que Broker, le Hub STIAM SuisseTrustIAM est en mesure de générer des Security Tokens sous une forme standardisée et de les transmettre au Relying Party en tant qu'informations d'authentification et d'autorisation. Ces Security Tokens et Attribute Assertions peuvent être émis de différentes manières. A cet égard, il existe des normes applicables, telles que SAML 2.0 ou WS-Trust resp. WS-Federation pour n'en citer que quelques-unes.

Le tableau suivant répertorie les protocoles pouvant être utilisés par les entités SuisseTrustIAM:

Protocole	Destinataire STIAM	Hub STIAM	Expéditeur STIAM	IdP STIAM	Remarque
SAML 2.0 Web Browser SSO-Profile avec HTTP POST Binding	DEVRAIT	DOIT	DEVRAIT	DEVRAIT	• Pour la communication axée sur l'utilisateur
WS-Trust avec SAML-Token comme Security Token	PEUT	DOIT	PEUT	PEUT	• Pour la communication de service à service • Les Security Tokens

Protocole	Destinataire STIAM	Hub STIAM	Expéditeur STIAM	IdP STIAM	Remarque
					émis par le Hub STIAM sont SAML 2.0 Assertions comme ceux du Web Frontend • Un IdP/AA Suisse-TrustIAM devrait être compatible WS-Trust, quand il doit authentifier des Web Services.
OpenID Connect	peut	PEUT	peut	peut	Avec tokens JSON Web
Autres protocoles (ex. Mobile ID, OpenID, etc.)	peut	PEUT	peut	peut	Le Hub STIAM sera à l'avenir compatible également avec des protocoles supplémentaires, afin de pouvoir intégrer d'autres Identity Providers commerciaux.

Tableau 1: protocoles STIAM

Comme le montre le tableau ci-dessus, SAML 2.0 et WS-Trust sont les principaux protocoles utilisés dans SuisseTrustIAM. Mais il devrait être également possible d'intégrer d'autres protocoles dans l'infrastructure SuisseTrustIAM – en particulier par rapport aux Authentication Providers commerciaux. Grâce à la fonction de proxy d'authentification du Hub STIAM, il est également possible d'intégrer facilement d'autres technologies et de les anonymiser par rapport aux Relying Parties. Dans son rapport «SAML Proxying and Attribute Services» [15]. ATOS a mis en évidence le fait qu'avec un Hub STIAM, l'intégration de Google en tant qu'Identity Provider avec les technologies OAuth 2.0 [16] [17] et OpenID Connect (OIDC) [7] était très simple à mettre en œuvre.

D'un autre côté, il est également possible de connecter des Relying Parties incompatibles SAML. Là encore, il existe, avec OIDC, WS-Trust etc., d'autres technologies, qui pourront être intégrées à l'avenir.

3.6 Relation de confiance entre les composants

Tous les acteurs impliqués (Identity Provider, autorité d'attributs, Relying Party et Hub STIAM) doivent se faire mutuellement confiance. Les relations de confiance sont établies à deux niveaux:

- Le canal de communication entre le Hub STIAM et l'IdP/AA respectivement entre le Hub STIAM et le Relying Party est crypté par 2-way SSL/TLS et authentifié. Ceci implique le déploiement de certificats de serveur dignes de confiance pour tous les services impliqués.
- Les contenus de tous les messages transmis (Request ou Assertion) depuis et vers le Hub STIAM doivent être infalsifiables (signature numérique).
- Les certificats nécessaires à cette fin doivent être émis par un Certificate Service Provider (CSP) digne de confiance.

3.7 Session Handling

Les informations sur les identités et les attributs transmis par le Hub STIAM au Relying Party sont recueillies dans les plus brefs délais auprès des sources compétentes et contrôlées soit par le Hub STIAM lui-même, soit par le consommateur. Ce faisant, le Hub STIAM n'enregistre par principe aucune information d'identité. Les exceptions suivantes peuvent toutefois être constatées:

- Le Hub STIAM peut enregistrer temporairement des informations sur les identités et les attributs d'un sujet pour la durée d'exécution à des fins d'agrégation pour la durée d'une requête.
- Une fois l'authentification d'un sujet effectuée, le Hub STIAM peut enregistrer l',Authentication State' dans un cookie de session correspondant, sous réserve que le Relying Party à l'origine de la requête y consente[5].
- Le Hub STIAM peut enregistrer, sous forme cryptée, des ,informations agrégées sur les attributs' dans un cookie de session[6].

3.8 Confidentialité des contenus des attributs

Les informations sur les identités et les attributs relatifs à un sujet sont obtenues auprès de diverses sources et transmises par le Hub STIAM. Dans ces attributs peuvent figurer des données contenant des informations sensibles. C'est la raison pour laquelle il doit être possible de rendre ces informations accessibles uniquement au Relying Party à l'origine de la requête. Les fonctions suivantes sont mises à disposition en option dans SuisseTrust-IAM:

- Un fournisseur d'informations peut crypter le contenu d'un attribut pour un Relying Party.
- Pour obtenir les informations nécessaires au cryptage des informations sur les attributs, le fournisseur d'informations doit se reporter aux métadonnées.

3.9 Anonymisation des identités

[5] [5] Le Relying Party peut prescrire une option pour l'authentification du sujet dès le moment de la définition dans ses métadonnées ou à chaque fois pour la durée d'exécution dans le cadre d'une requête.

[6] La validité de l'information d'attribut enregistrée ne doit pas dépasser la validité max. de l'attribut et celle de la Security Session.

L'Identity Linking anonymise de manière implicite les identités numériques entre les fournisseurs d'informations SuisseTrust-IAM (IdP et AA), car chaque lien (Link) dispose de son propre identificateur. Seul un acteur ayant accès au Link Table peut relier les identités entre elles.

Exception: lorsque l'on a recours au Proxying (tel que décrit au chapitre 3.3.1), tous les services impliqués sont informés par le même identificateur.

Les choses sont différentes entre le Hub STIAM et le Relying Party. Le Hub STIAM doit renvoyer un identificateur dans sa réponse par rapport au Relying Party. En fonction de l'exigence fixée (protection de la sphère privée en particulier), le Hub STIAM peut renvoyer différents types d'identificateurs par rapport à un Relying Party (cf. à ce sujet UID_Z dans les Figure 5 et Figure 6).

Identificateur	Description	Utilisation
Distributed ID	Le Hub STIAM renvoie toujours le même identificateur d'un sujet dans ses réponses à tous les Relying Parties à l'origine d'une requête. L'identificateur utilisé en commun peut également être échangé via d'autres canaux en amont (Out-of-Band[7] Linking).	Une Distributed ID permet à un Relying Party de créer localement une identité numérique lors de la première connexion ou d'établir une connexion avec une identité existante (Identity-Mapping). L'identificateur étant connu via plusieurs Relying Parties, les attributs obtenus peuvent facilement être corrélés Out-of-Band.
Persistent ID	Pour chaque Relying Party à l'origine d'une requête, l'Identity Provider (respectivement le Hub STIAM) renvoie toujours dans ses réponses, un identificateur particulier et inchangé, d'un sujet. Un identificateur persistant cache la véritable identité d'un sujet au Relying Party à l'origine de la requête.	Une ID persistante permet également à un Relying Party de créer localement une identité numérique lors de la première connexion ou d'établir une connexion avec une identité existante (Identity-Mapping). L'identificateur étant destiné uniquement à un Relying Party, il est bien plus difficile corréler directement les activités des utilisateurs entre les différents Relying Parties..
Transient ID	Les identificateurs transitoires ont le même objectif que les identificateurs persistants, mais dans ce cas précis,	Le Relying Party ne peut plus relier l'identité d'un sujet entre deux sessions distinctes à partir

[7] Über einen anderen (zweiten) Kanal übermittelt

Identificateur	Description	Utilisation
	le Hub STIAM renvoie au Relying Party un identificateur aléatoire pour chaque Login Session d'un sujet.	de l'identificateur obtenu. Les autorisations d'accès reposent sur des informations sur les attributs.
Requested ID	Dans son Authentication Request, le Relying Party peut, pour la durée d'exécution, indiquer un identificateur dont il a connaissance. La réponse du Hub STIAM doit se rapporter à cet identificateur, afin que le Relying Party soit en mesure d'associer les informations d'identité obtenues avec les données locales concernant l'utilisateur.	Un Relying Party dépose une requête auprès du Hub STIAM portant sur des attributs supplémentaires concernant un sujet déjà authentifié. L'identificateur utilisé doit être connu des deux partis.

Tableau 2: types d'identificateurs

Il est à noter qu'indépendamment des types d'identificateurs figurant dans le Tableau 2, il est toujours possible d'établir des liens pour les identités, lorsque l'IdP/AA et le RP disposent chacun de suffisamment d'attributs identifiants concernant un sujet et que ceux-ci sont transférés pour la durée d'exécution.

Dans sa réponse, le Hub STIAM émet pour chaque sujet et chaque RP une *Persistent ID* ou une *Transient ID*.

3.10 Traçabilité de processus

Les processus exécutés pour la durée de définition comme pour la durée d'exécution doivent être consignés et conservés à des fins de traçabilité pour une période prescrite par la législation. L'enregistrement et la conservation de tous les processus de communication et leur affectation unique à un sujet sont volontairement requis. Pour connaître l'endroit où sont enregistrées et conservées des informations précises, se reporter au chapitre 5.6. Les différentes donnés doivent être enregistrée de manière centralisée, car les composants périphériques (AA, IdP et RP) n'ont à leur disposition que les informations dont ils ont besoin. Il n'est donc pas possible de se faire une idée globale du processus sur la durée d'exécution.

L'exploitant d'un Hub STIAM doit pouvoir s'acquitter de son obligation de conservation des informations dans les protocoles dans le respect de la règlementation suisse en matière de protection des données.

3.11 Catégorisation des attributs

Partant du concept cadre, la plateforme SuisseTrustIAM doit être compatible avec les scénarios d'application suivants pour la durée d'exécution:

- Un utilisateur, particulier et citoyen, devrait pouvoir utiliser le Hub STIAM pour obtenir la confirmation de l'identité numérique et, en option, l'agrégation des informations personnelles par le Hub STIAM.
- Les utilisateurs ou services (Machine Accounts ou comptes machines) d'une entreprise devraient pouvoir accéder, à l'aide du Hub STIAM, aux services hors de leur propre organisation, afin de disposer d'accès en ligne autorisés au nom de cette entreprise.

Dans les deux cas, le Hub STIAM transmet des informations d'identité sous forme d'attributs, mais les emplois prévus sont forts différents. L'on a d'un côté des informations personnelles, dont la divulgation à un Relying Party requiert le consentement préalable impératif de l'utilisateur concerné, et de l'autre, des renseignements spécifiques à l'entreprise, comme l'appartenance à l'entreprise et un justificatif de fonction, pour lesquels aucun accord explicite de l'utilisateur ne s'impose.

Dans son rapport d'état des lieux des technologies, Overlap of Identity Technologies' [18] Google a inventé le terme d',Identity Camps'. Pour résumer, Google établit une distinction entre les deux catégories Enterprise-IAM et Internet-IAM Camp. Ces deux Camps se différencient en premier lieu par la question de l'appartenance des données d'identité et du consentement requis lors de la livraison.

- *Enterprise-IAM:* les ressources et en particulier les données d'identité (HansMuster@Répertoireorganisation) sont la propriété de l'organisation. Celle-ci statue donc sur la transmission des données dans le respect des lois et contrats en vigueur. Dans le cadre de cette décision, le rôle de l'employé («Hans Muster») est secondaire. En fonction des informations à transmettre, ni l'autorisation de l'utilisateur (consent) et ni une communication axée sur ce dernier (user-centric) ne sont nécessaires.
- *Internet-IAM:* les ressources et en particulier les données d'identité (HansMuster@Facebook) sont la propriété de l'individu. Lui seul doit pouvoir décider de la transmission des informations. Contrairement à la catégorie Enterprise-IAM, les exigences relatives à l'autorisation de l'utilisateur et la communication axée sur lui sont ici incontournables.

Les deux scénarios sont appliqués à de maintes reprises dans les infrastructures parallèles et pas sur une plateforme commune. Dans un environnement où les scénarios tant Enterprise-IAM que Internet-IAM devraient être couverts, il doit être possible de commander le mode de publication d'un attribut.

Autorisation de divulgation d'informations personnelles

- L'utilisateur doit avoir la possibilité de valider des confirmations d'authentification et des attributs personnels envers le Relying Party à l'origine d'une requête.
- La forme d'autorisation de divulgation devrait pouvoir être sélectionnée par l'utilisateur:
    - L'utilisateur reconfirme à chaque fois la publication de confirmations d'authentification et d'attributs personnels pour chaque Relying Party à l'origine d'une requête.

- L'utilisateur peut donner une seule fois son accord pour la publication d'une confirmation d'authentification et d'un jeu d'attributs pour chaque Relying Party à l'origine d'une requête. Les informations demandées sont ensuite automatiquement transmises par le Hub STIAM au RP, jusqu'à ce que le jeu d'attributs change ou que l'utilisateur exige de donner à nouveau son consentement.

Autorisation de divulgation des attributs dans le cas d'une organisation

- Les confirmations d'authentification et les attributs d'un sujet dans le contexte d'une organisation peuvent être transmis à un Relying Party sans le consentement du sujet. Ils décrivent et autorisent le sujet en lien avec son activité dans l'organisation.
- La publication des informations concernant les employés (respectivement Machine Accounts) doit pouvoir être restreinte à certains Relying Parties par une organisation respectivement un IdP/AA. Dans le cadre de SuisseTrustIAM, ceci devrait permettre de rendre des identités et attributs, présentant une sémantique spéciale, accessibles uniquement à certains domaines.

3.12 Administration des attributs

Les attributs doivent pouvoir être référencés sans ambigüité dans SuisseTrustIAM par tous les composants impliqués. La/les définition/s (dénomination, syntaxe, type) est/sont enregistrées et gérées de manière centralisée sur le Hub STIAM. Les processus relatifs à la qualification et à l'administration des attributs ne font pas partie de cette documentation et sont spécifiés dans un document séparé.

4 Exigences

4.1 Infrastructure de transmission SuisseTrustIAM

Le Tableau 3 récapitule les exigences résultant du chapitre 3 et du concept cadre de SuisseTrustIAM [3] imposées à l'infrastructure de transmission SuisseTrustIAM.

N°	Désignation	Description
A1	Identité du sujet	La détermination de l'identité d'un sujet est prouvée sans ambigüité et revêt une qualité définie.
A2	Classement des attributs	Les attributs peuvent toujours être affectés - indépendamment de leur qualité – à une identité numérique précise.
A3	Coordination des identificateurs[8]	Les identificateurs d'un sujet peuvent être référencés sans ambigüité pour toutes les entités périphériques (Identity Provider, Relying Party et autorité d'attributs) par rapport à une identité numérique locale.
A4	Authenticité d'un attribut	Il est possible de vérifier qui a émis un attribut et quand celui-ci a été émis.
A5	Catégorisation des attributs	Concernant les informations d'identité, il faut faire la distinction entre les contenus personnels et les contenus liés aux entreprises.
A6	Protection de la sphère privée	L'utilisateur a la possibilité de contrôler la publication des attributs.
A7	Limitation de la publication	Il est possible de délimiter la visibilité et la publication d'un attribut à un cercle déterminé de consommateurs (Relying Parties).
A8	Fiabilité d'un attribut	Indépendamment de l'origine, on peut contrôler la fiabilité d'un attribut précis. Un attribut dispose par conséquent d'une valeur de qualité, qui fournit des renseignements concernant le contrôle effectué concernant le contenu.
A9	Mise sur liste noire d'attributs et de fournisseurs d'attributs	Afin de pouvoir établir des relations de confiance vérifiables concernant la qualité des attributs, il est nécessaire de disposer de procédés permettant de bloquer un attribut respectivement un fournisseur d'attributs.
A10	Etablissement de relations de confiance	Tous les partis impliqués (Identity Provider, autorité d'attributs, Relying Party et Hub STIAM) ont la possibilité de vérifier la communication avec leur partenaire et les contenus

[8] L'anonymisation de l'identité figurant sous A15 n'est pas en contradiction avec A3, car il s'agit dans ce cas, non pas d'une identité globale, mais d'identités pouvant être référencées au niveau local.

N°	Désignation	Description
		de messages de manière fiable.
A11	Confidentialité du contenu des attributs	On s'assure que les contenus de messages peuvent être transmis de façon confidentielle.[9]
A12	Renseignement minimal	On s'assure qu'un parti à l'origine d'une requête peut demander et obtenir uniquement les informations (enregistrées) qui lui sont nécessaires.[10]
A13	Compétence de la source	On s'assure qu'un fournisseur d'attributs peut émettre uniquement des informations d'identité pour lesquelles il est compétent.[10]
A14	Traçabilité	La traçabilité d'un processus d'émission d'authentifications et d'attributs pour une durée déterminée est possible.
A15	Anonymisation d'identités	L'identité d'un sujet est anonymisée pour les partis impliqués (voir à ce sujet la note de base de page 8 page 29).
A16	Syntaxe d'attribut	La syntaxe d'un attribut est définie sans ambigüité pour tous les partis impliqués.
A17	Sémantique d'attribut	La sémantique d'un attribut est définie sans ambigüité pour tous les partis impliqués.
A18	Administration	Les organisations ont la possibilité d'administrer, de manière simple et autonome, leurs employés, services proposés et ressources.
A19	Step-up Authentication	Un degré d'authentification accru exigé par un consommateur d'informations au cours d'une session entraîne une authentification renouvelée du sujet.
A20	Vérification de l'authentification	Un fournisseur d'attributs a la possibilité de vérifier lui-même l'authentification effectuée pour un sujet.
A21	Single Logout	Un sujet peut, via le Relying Party (respectivement via son application), obtenir la fermeture par le Hub STIAM des sessions en cours sur d'autres RP.
A22	Login Session Handling	Un sujet reste authentifié sur le Hub STIAM une fois l'authentification effectuée par un IdP. Une demande d'attributs supplémentaires (par un autre Relying Party éga-

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

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

N°	Désignation	Description
		lement) est possible sans authentification renouvelée du sujet, tant que cette demande ultérieure ne nécessite pas un niveau d'authentification (Authentication Level) supérieur. Si la requête d'un RP exige un Authentication Level supérieur, A19 entre en jeu.

Tableau 3 : exigences imposées à l'infrastructure de transmission SuisseTrustIAM

4.2 Destinataire STIAM

Les destinataires STIAM (Relying Party) définissent pour chaque ressource les règles précises concernant le degré d'authentification des utilisateurs et la qualité d'un attribut demandé dans ses métadonnées. Ils peuvent donc valider les réponses reçues du Hub STIAM conformément à leurs propres directives:

Fonction	Description
RP-01	Le destinataire STIAM DOIT déléguer l'authentification du sujet au Hub STIAM en tant qu'instance digne de confiance.
RP-02	Le destinataire STIAM PEUT présélectionner un Identity Provider particulier pour la période de définition.
RP-03	Le destinataire STIAM DOIT prescrire le niveau de qualité de l'identité (QAA-Level) en fonction de la ressource à contrôler.
RP-04	Le destinataire STIAM PEUT lui-même valider le Security Token émis par un Identity Provider, lorsque le Hub STIAM est compatible avec l'Identity Relaying Mode (HUB-LZ-11).
RP-05	Le destinataire STIAM PEUT déléguer la vérification des Attribute Assertions au Hub STIAM en tant qu'instance digne de confiance.
RP-06	Le destinataire STIAM PEUT prescrire le niveau de qualité d'un attribut qui lui est nécessaire pour la période de définition.
RP-07	Le destinataire STIAM DOIT être compatible avec l'un des protocoles de communication STIAM décrits au chapitre 3.5 et compatible avec le Hub STIAM.
RP-08	Le destinataire STIAM PEUT lui-même valider les Attribute Assertions délivrés par une autorité d'attributs compétente, lorsque le Hub STIAM est compatible avec l'Identity Relaying Mode (HUB-LZ-11).
RP-09	Le destinataire STIAM DEVRAIT être compatible avec les SSO Sessions, lorsque Single Logout (SLO) doit être supporté (cf. chapitre 5.5).
RP-10	Si le destinataire STIAM demande un attribut crypté à un expéditeur STIAM, qui supporte le cryptage (AA-LZ-02), il DOIT également être mesure de le traiter correctement.

4.3 IdP STIAM

Dans SuisseTrustIAM, un IdP STIAM a pour fonction d'authentifier un sujet. Il peut s'agir d'un IdP commercial ou d'un IdP/AA d'une organisation affiliée à SuisseTrustIAM. Les moyens d'authentification et les Credentials par lesquels l'IdP authentifie le sujet ne sont pas couverts par la normalisation SuisseTrustIAM. Afin que l'enregistrement et l'authentification d'un sujet puissent être contrôlés de manière transparente pour toutes les entités de la plate-forme SuisseTrustIAM, les Identity Providers doivent fournir certaines informations concernant la qualité de l'identification de l'utilisateur effectuée et la méthode d'authentification conformément au modèle de qualité de la norme eCH eCH-0170 [4].

Fonction	Description
IDP-01	L'IdP STIAM DOIT être compatible avec l'un des protocoles de communication décrits au chapitre 3.5 et proposés par le Hub STIAM.
IDP-02	L'IdP STIAM DOIT renvoyer les informations d'authentification demandés par un Relying Party, sous une forme infalsifiable (signature numérique).
IDP-03	L'IdP STIAM DOIT renvoyer un identificateur qu'il connaît – unique pour chaque sujet – en tant que partie de son Authentication Statement.
IDP-04	L'IdP STIAM DEVRAIT indiquer le niveau de qualité de l'identification de l'utilisateur et la méthode d'authentification sous forme normalisée, en tant que partie de son Authentication Statement (justificatif).
IDP-05	L'IdP STIAM DOIT être compatible avec le protocole de Linking pour l'enregistrement par l'utilisateur (cf. Chapitre 6.1).
IDP-06	L'IdP STIAM DOIT toujours utiliser une Persistent ID vis à vis du Hub STIAM.

4.4 Expéditeur STIAM

L'expéditeur STIAM (autorité d'attributs) émet des attributs après réception d'une requête pour un sujet particulier. Une autorité d'attributs émet uniquement des attributs pour lesquels elle est la source compétente. Dans le cadre de cette fonction, elle doit respecter certaines règles, mais a également la possibilité de lier les conditions à l'émission d'un attribut.

Fonctions pour la durée d'exécution:

Funktion	Beschreibung

Funktion	Beschreibung
AA-LZ-01	L'expéditeur STIAM PEUT lui même valider le Security Token délivré par l'Identity Provider, lorsque le Hub STIAM est compatible avec l'Identity Relaying Mode (HUB-LZ-11).
AA-LZ-02	L'expéditeur STIAM PEUT crypté l'attribut demandé avec son contenu pour un destinataire particulier.
AA-LZ-03	L'expéditeur STIAM DOIT disposer d'un identificateur unique par sujet vis à vis du Hub STIAM.
AA-LZ-04	L'expéditeur STIAM DOIT interpréter l'identité fournie par le Hub STIAM du Relying Party à l'origine de la requête et la représenter sur l'identité utilisée en interne.
AA-LZ-05	L'expéditeur STIAM DOIT être compatible avec l'un des procédés de transmission des identités et des attributs (Proxying chapitre 3.3.1, Transmission d'identité chapitre 3.3.2).
AA-LZ-06	L'expéditeur STIAM DOIT renvoyer les informations d'attribut demandées par le Hub STIAM sous forme infalsifiable (avec signature numérique).
AA-LZ-07	L'expéditeur STIAM DOIT être compatible avec l'un des protocoles de communication décrits au chapitre 3.5 et proposé par le Hub.
AA-LZ-08	L'expéditeur STIAM DOIT pouvoir contrôler si le Hub STIAM est en droit de solliciter les attributs demandés.
AA-LZ-09	L'expéditeur STIAM PEUT permettre un «User Consent» indépendant du Hub STIAM[11].
AA-LZ-10	L'expéditeur STIAM DOIT être compatible avec le Linking Protocole pour l'inscription par l'utilisateur (cf. chapitre 6.1).
AA-LZ-11	L'expéditeur STIAM DOIT interpréter les attributs sollicités par le Hub STIAM et les représenter sur les attributs utilisés en internes.
AA-LZ-12	L'expéditeur STIAM DOIT gérer les identités, pour lesquels il met à disposition des attributs et dont ils gère les attributs.
AA-LZ-13	L'expéditeur STIAM DEVRAIT mettre une fonctionnalité pour inclure/exclure les identités qu'il gère à la disposition de l'Identity-Federation (User Filtering).

Fonctions pour la période de définition:

[11] Dans un souci de convivialité, il ne faudrait demander le consentement de l'utilisateur qu'une seule fois, dans la mesure du possible.

Les fonctionnalités suivantes font partie de l'administration de l'expéditeur STIAM et sont stipulées pour la période de définition (voir chapitre 7.5.4.4).

Fonction	Description
AA-DZ-01	L'expéditeur STIAM DOIT indiquer un niveau de qualité pour l'identification du sujet (QAA-Level de (eCH)) pour l'émission d'un attribut particulier).
AA-DZ-02	L'expéditeur STIAM PEUT prescrire un Identity Provider particulier pour l'émission d'un attribut.
AA-DZ-03	L'expéditeur STIAM PEUT lui-même demander encore une fois l'authentification du sujet.
AA-DZ-04	L'expéditeur STIAM DOIT indiquer un niveau de qualité selon eCH-0171 [5] pour un attribut qu'il met à disposition.
AA-DZ-05	L'expéditeur STIAM PEUT restreindre l'utilisation d'un attribut à un cercle précis de fournisseurs de solutions (domaine).

4.5 Hub STIAM

Le Hub STIAM dans SuisseTrustIAM couvre plusieurs fonctions des services d'affaires IAM. Il agit en tant que *Hub STIAM* pour la durée d'exécution et sert d'intermédiaire entre les entités. Pendant la durée de définition, il occupe la fonction de *Trust & eIdentity Service*, dans lequel des sujets et des organisations peuvent s'inscrire sur le Hub STIAM.

Les *Trust & eIdentity Services* sont des processus administratifs dans le cadre de la gestion des utilisateurs et des organisations et ne sont que brièvement abordés dans la présente description des fonctions. Pour une description plus détaillée des fonctions, se reporter à l'architecture administrative de SuisseTrustIAM eCH-0169 [19].

Fonctions pour la durée d'exécution:

Fonction	Description
HUB-LZ-01	Le Hub STIAM DOIT disposer d'un Discovery Service central.
HUB-LZ-02	Le Hub STIAM DOIT donner au sujet la possibilité de choisir parmi une liste d'Identity Providers possibles, en fonction du niveau QAA requis.
HUB-LZ-03	Le Hub STIAM DOIT être compatible avec l'un des protocoles de communication décrits au chapitre 3.5.
HUB-LZ-04	Le Hub STIAM DOIT, pour la durée d'exécution, se charger de la fonction de proxy d'authentification pour les Relying Parties à l'origine de requêtes.
HUB-LZ-05	Le Hub STIAM DOIT contrôler l'authenticité des Attribute Assertions.
HUB-LZ-06	Le Hub STIAM DOIT, pour la durée d'exécution, se charger de la fonction d'Attribut Aggregator pour les Relying Parties à l'origine de requêtes.
HUB-LZ-07	Le Hub STIAM DEVRAIT être compatible avec le Proxying en tant que pro-

Fonction	Description
	cédé de transmission d'identités et d'attributs (cf. chapitre 3.3.1).
HUB-LZ-08	Le Hub STIAM DOIT être compatible avec la transmission d'identité comme procédé de transmission d'identités et d'attributs (cf. chapitre 3.3.2**)**.
HUB-LZ-09	Le Hub STIAM DOIT renvoyer les informations demandées par un Relying Party concernant les authentifications et les attributs sous une forme infalsifiable (signature numérique).
HUB-LZ-10	Le Hub STIAM DOIT être compatible avec l'Identity Proxy Mode décrit au chapitre 3.4.1.
HUB-LZ-11	Le Hub STIAM DEVRAIT être compatible avec l'Identity Relaying Mode décrit au chapitre 3.4.2.
HUB-LZ-12	Le Hub STIAM DOIT proposer la possibilité, dans le cadre de la transmission des attributs, d'obtenir le consentement du sujet (User Consent) concernant la publication de différents attributs.[12]
HUB-LZ-13	Le Hub STIAM DOIT, en tant que proxy d'authentification, gérer son propre Session Handling pour les utilisateurs authentifiés.
HUB-LZ-14	Le Hub STIAM DOIT être en position de transférer l'identité du Relying Party à l'origine de la requête à l'autorité d'attributs.
HUB-LZ-15	Le Hub STIAM DEVRAIT être compatible avec les identificateurs anonymisés spécifiques au RP (Persistent ID).
HUB-LZ-16	Le Hub STIAM DOIT être compatible avec les identificateurs aléatoires anonymisés (Transient ID).
HUB-LZ-17	Le Hub STIAM DOIT consigner toutes les opérations de communication dans le cadre de la transmission des authentifications et des attributs.
HUB-LZ-18	Le Hub STIAM DOIT gérer ses identités.

Fonctions pour la période de définition:

Fonction	Description
HUB-DEF-01	Le Hub STIAM DOIT mettre à disposition un Linking Service pour l'administration der sujets .
HUB-DEF-02	Le Hub STIAM DOIT mettre à disposition un service pour l'administration des organisations et de leurs entités.

[12] Lors de la définition des attributs proposés (chapitre 7.5.4.4), il est déterminé si un User Consent est nécessaire pour un attribut ou si le Hub STIAM ou l'émetteur STIAM se le procurent.

Fonction	Description
HUB-DEF-03	Le Hub STIAM DOIT agréger les entités enregistrées d'une organisation sous forme de métadonnées.
HUB-DEF-04	Le Hub STIAM DOIT publier les métadonnées agrégées sous forme infalsifiable.
HUB-DEF-05	Le Hub STIAM DOIT mettre à disposition un service pour l'administration des attributs.
HUB-DEF-06	Le Hub STIAM DOIT consigner tous les processus administratifs pour l'administration des organisations et des sujets.

5 Protocole pour la durée d'exécution

5.1 Agrégation d'authentifications et d'attributs

Ce chapitre décrit plus en détail les procédés d'agrégation d'authentifications et d'attributs utilisés dans SuisseTrustIAM. Comme cela a déjà été évoqué au chapitre 3.3, on distingue deux procédés possibles. A la place du processus d'agrégation d'authentifications et d'attributs, le procédé direct est représenté de manière détaillé et décrit au moyen de la transmission d'identité (cf. chapitre 3.3.2) dans les pages qui suivent.

Dans ce procédé, le Hub STIAM (15) transmet à un expéditeur STIAM (autorité d'attributs) l'identité du sujet, en amont de la requête d'attribut qui suit immédiatement (16). Cette approche de solution permet d'effectuer une requête parallèle d'attributs auprès d'autorités d'attributs avec différents identificateurs. La Figure 7 illustre le procédé dans son intégralité dans un diagramme de séquence.

L'utilisateur (sujet) accède avec son navigateur à une application (Resource) d'un destinataire STIAM (Relying Party). L'accès à la ressource est commandé par un contrôle d'accès. Le sujet est redirigé vers le Hub STIAM à des fins d'authentification et de confirmation des attributs. Le Hub STIAM fait authentifier le sujet par un IdP correspondant et se procure les attributs demandés auprès des sources compétentes. Le Hub STIAM agrège tant les *Authentication Statements* que les attributs *Statements* en une *Assertion* propre et les renvoie au Relying Party (destinataire STIAM).

Aucune représentation détaillée du deuxième procédé par Proxying (cf. chapitre 3.3.1) n'est proposée dans ces pages, car le SAML-Proxying est spécifié de façon précise dans la norme SAML-Core [20] et peut donc être appliqué en conséquence à d'autres protocoles.

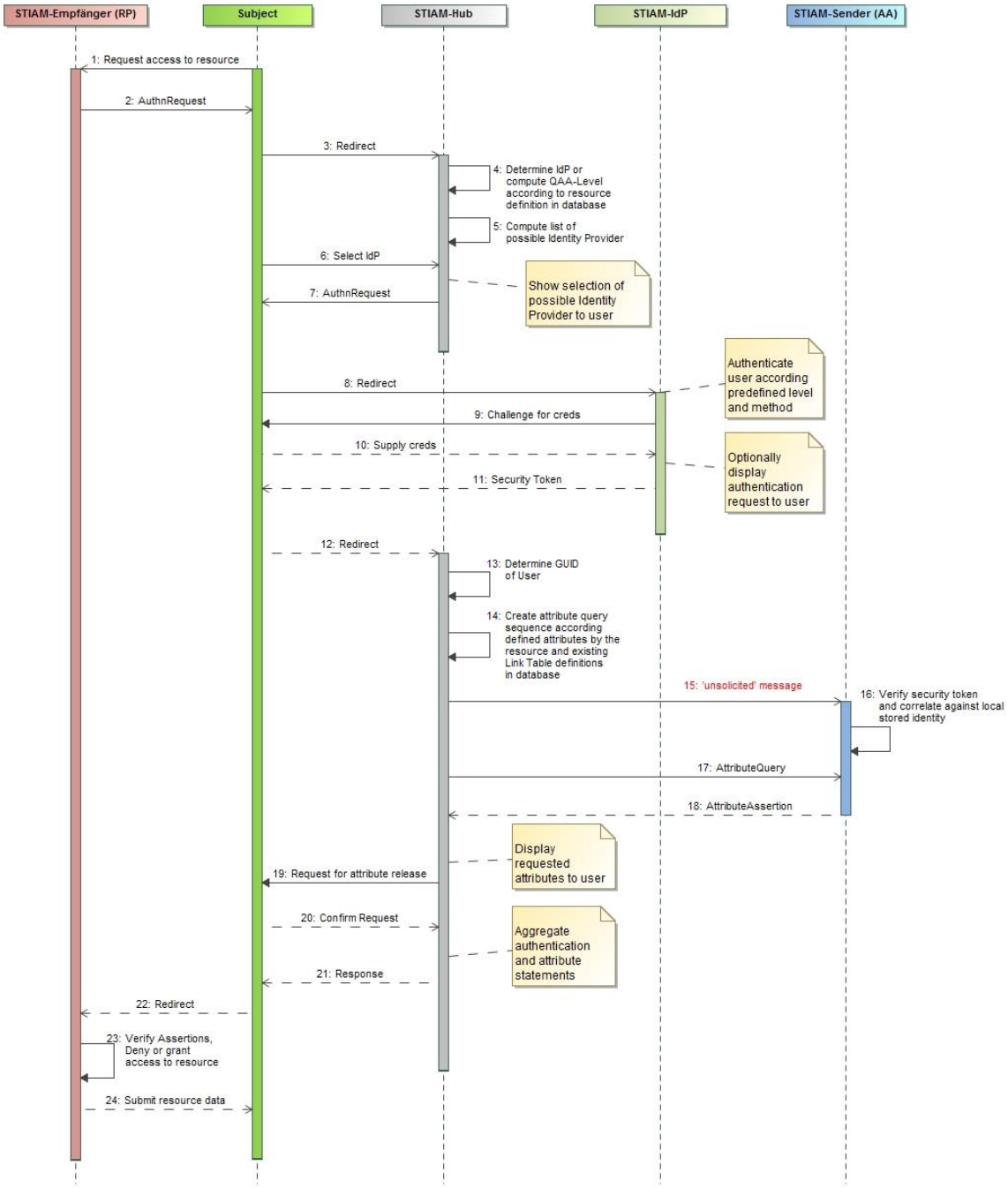


Figure 7: procédé direct d'agrégation des attributs

Description de la Figure 7:

Etape	Remarque
2	• Le destinataire STIAM (RP) envoie au navigateur de l'utilisateur, une *Authentication Request* portant une signature numérique, avec des renseignements concernant la ressource à laquelle l'utilisateur veut accéder.
3	• Le navigateur redirige l'*Authentication Request* vers le Hub STIAM (Redirect).
4	• Le Hub STIAM identifie le destinataire STIAM (RP-ID) et la ressource

Etape	Remarque
	souhaitée (RES-ID) à partir des informations de son *Authentication Request* dans sa base de données. • Le Hub STIAM doit vérifier la signature du destinataire STIAM (RP).
5	• A partir de la *Resource Definition,* le Hub STIAM constitue dans sa base de données une liste des services d'authentification possibles (IdP). A cet égard, les scénarios suivants sont possibles en fonction de la *Resource Definition*: a) La ressource a prescrit un (ou plusieurs) IdP (*IdP-ID*). Sur son site Web, le Hub STIAM indique à l'utilisateur les IdP prédéfinis et proposés au choix. b) La ressource a défini un (ou plusieurs) attribut(s) proposé(s) (*Attr-ID*). A partir de l'*Attr-ID,* le Hub STIAM détermine le QAA-Level qui y est exigé. A partir du QAA-Level le plus élevé de tous les attributs demandés, le Hub STIAM établit pour l'utilisateur une liste des IdP entrant en ligne de compte [pour la requête auprès d'autorités d'attributs correspondantes]. A titre facultatif, un ou plusieurs IdP (*IdP-ID*) peuvent également être prescrits directement dans l'*Attr-ID*. Dans ce cas de figure, le Hub procède comme au point a). c) La ressource a prescrit un niveau d'authentification souhaité (QAA-Level). A partir de cette valeur, le Hub STIAM établit une liste des IdP entrant en ligne de compte et la soumet à l'utilisateur afin qu'il puisse choisir. • Le Hub STIAM recherche dans sa base de données les autorités d'attributs (*AA-ID*), qui peuvent mettre à disposition un attribut demandé. Les QAA-Levels respectivement les IdP déterminés auparavant sont contrôlés par rapport aux exigences des autorités d'attributs en matière de QAA-Level. Si le Hub STIAM reconnaît un fournisseur d'attributs qui, pour la livraison d'un attribut particulier, exige un QAA-Level plus élevé que ce qui a été établi auparavant, le Hub STIAM doit alors adapter le QAA-Level et corriger la liste des IdP possibles en conséquence.
6	• A partir des services d'authentification au choix (évalués au point 5), l'utilisateur choisit un IdP.
7	• Le Hub STIAM crée une *Authentication Request* à l'intention de l'IdP sélectionné et le renvoie au navigateur.
8	• Le navigateur redirige l'*Authentication Request* vers le service d'authentification de l'IdP sélectionné.
9	• L'IdP somme l'utilisateur de s'authentifier (nom d'utilisateur/mot de passe, à base PKI, etc.)
10	• L'utilisateur s'authentifie par rapport à l'IdP.
11	• L'IdP authentifie l'utilisateur et lui renvoie un Security Token portant une signature numérique. • A titre facultatif, l'IdP peut obtenir le consentement de l'utilisateur pour

Etape	Remarque
	livrer le Security Token au Hub STIAM à l'origine de la requête.
12	• Le navigateur redirige le Security Token de l'IdP vers le Hub STIAM.
13	• A partir d'informations provenant du Security Token, le Hub STIAM peut déterminer le GUID des utilisateurs dans le Link Table dans l'User Identifier Repository (UIR). Si l'identificateur provenant du Security Token est associé à plus d'un GUID, le Hub STIAM doit alors présenter à l'utilisateur des Accounts (comptes) concordants pour lui permettre de faire son choix.[13]
14	• Le Hub STIAM établit une *Attribute Query Sequence*[14] en fonction des attributs dans la ressource. Ce faisant, il doit tenir compte des critères suivants: a) La ressource a défini un (ou plusieurs) attributs proposés (*Attr-ID*). A à partir de l'*Attr-ID,* le Hub STIAM détermine l'*AA-ID* et vérifie si l'utilisateur dispose d'un AA-Link correspondant dans son Link Table. b) La ressource a défini un (ou plusieurs) attributs avec une qualité d'attribut (*Attr-Quality*). Le Hub STIAM recherche dans la base de données des autorités d'attributs (*AA-ID*), qui peuvent mettre à disposition l'attribut dans la qualité exigée, et vérifie si l'utilisateur dispose bien, dans son Link Table, d'un AA-Link correspondant. c) La ressource a seulement défini un (ou plusieurs) attributs (*OID*). Le Hub STIAM recherche dans la base de données des autorités d'attributs (*AA-ID*), qui proposent l'attribut, et vérifie si l'utilisateur dispose bien dans son Link Table du AA-Link correspondant. • Dans l'hypothèse où l'utilisateur ne dispose pas d'un AA-Link nécessaire et que l'attribut indiqué dans la Resource Definition est désigné comme *required*, le Hub STIAM doit envoyer à l'utilisateur un message d'erreur correspondant. • Si l'utilisateur a défini plusieurs AA-Links pour un attribut, le Hub STIAM doit alors indiquer à l'utilisateur les autorités d'attributs entrant en considération afin qu'il puisse choisir.
15	• Le Hub STIAM envoie un message non sollicité et portant une signature numérique (*unsolicited message*) directement[15] à l'expéditeur STIAM (AA).

[13] Ill devrait être possible pour un utilisateur d'avoir plusieurs Accounts SuisseTrustIAM et d'utiliser le même identificateur pour ces Accounts (ex. pour deux Accounts, un même SuisseID avec un n° SuisseID comme identificateur).

[14] Attribute Query Sequence: la liste des AA, qui sont fournisseurs des attributs de la qualité exigée.

Etape	Remarque
	• Ce message contient un Security Token (*Authentication Statement*) ainsi qu'un *AA-Identifier* signé[16] par l'autorité d'attributs.
16	• L'expéditeur STIAM (AA) doit vérifier le Security Token obtenu du Hub STIAM et l'associer avec l'*AA-Identifier* du sujet défini dans sa base de données. • L'autorité d'attributs doit vérifier sa signature apposée sur l'*Identifier AA*.[17]
17	• Le Hub STIAM envoie une *Attribute Request* au Attribute Assertion Service de l'expéditeur STIAM (AA). • Cette Request contient les attributs demandés et l'*AA-Identifier* envoyé lors de l'étape 15.
18	• L'expéditeur STIAM (AA) établit une *Attribut Assertion*, qui comprend les valeurs de l'attribut, et y appose sa signature numérique.
19	• Le Hub STIAM se procure, auprès de l'utilisateur, l'autorisation de transmission (*user consent*) au destinataire STIAM, pour les attributs demandés (individuellement ou globalement).[18]
20	• L'utilisateur confirme l'autorisation de divulgation des attributs.
21	• Le Hub STIAM crée une *Assertion* portant une signature numérique, composée des *Authentication Assertions* et des *Attribute Assertions,* et la renvoie comme *Response* au navigateur.
22	• Le navigateur redirige la *Response* au destinataire STIAM (RP).
23	• Le destinataire STIAM doit vérifier la signature de la *Response* et peut utiliser la réponse du Hub STIAM pour la décision concernant l'accès à la ressource.
24	• Le destinataire STIAM refuse ou accorde l'accès à la ressource au moyen des contenus d'attributs et de la Policy définie localement.

5.2 Communication reposant sur le Service-to-Service

[15] En option, ce message peut aussi passer par le navigateur de l'utilisateur. Toutefois, le chemin axé sur l'utilisateur ne s'impose que lorsque l'Attribut Authority veut exiger elle-même le consentement pour la publication des attributs de l'utilisateur.

[16] L'Attribut Authority signe l'identificateur dans le protocole de Linking (voire chapitre 7.1).

[17] L'Attribut Authority peut ainsi exclure les identificateurs falsifiés.

[18] Il est également possible que l'AA obtienne l'autorisation de l'utilisateur pour ses attributs. Pour cela, la communication concernant la demande d'attribut (étape 16 et 17) entre le Hub STIAM et l'émetteur doit être redirigée via le navigateur de l'utilisateur. Toutefois, l'autorisation centrale au niveau du Hub STIAM reste le mode le plus convivial pour l'utilisateur.

Le type de Security Token et les protocoles utilisés dans SuisseTrustIAM ont déjà été évoqués au chapitre 3.5. Outre la communication basée sur SAML 2.0 et axée sur l'utilisateur, des services Web tels que *Requestor* devraient également pouvoir être intégrés. Pour cela, le Hub STIAM doit être compatible, côté Relying Party, avec les fonctionnalités WS* selon WS-Trust [14] respectivement WS-Federation [12].

Le type de Token émis est également utilisé pour les services Web SAML Assertions, comme il l'est pour la communication axée sur l'utilisateur.

Le procédé d'intégration de WS-Trust avec la fonction Hub STIAM se déroule de la manière décrite au chapitre **Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.**. . Le Hub STIAM agit en tant que Security Token Service (STS), intermédiaire de la ressource (RP). L'IdP/AA est le STS du Requestor, auprès duquel le service Web doit s'authentifier. Le protocole peut être mis en œuvre de plusieurs manières pour la durée d'exécution. Les scénarios possibles ne sont pas traités plus en détail dans le cadre de cette architecture technique.

5.3 Validation d'informations sur les identités et les attributs

Pour la durée de définition, tant un Relying Party qu'une autorité d'attributs avec l'option *Verify Assertion* peuvent signaler au Hub STIAM qu'ils souhaitent valider eux-mêmes les originaux des Security Tokens et Attribute Assertions émis. Avec pour conséquence que le Hub STIAM doit insérer dans sa *Response* générée le(s) Assertion(s) et Token(s) agrégé(s) dans leur forme originale avec la signature originale de l'instance émettrice (comparaisons à ce sujet voir chapitre 3.4.2).

5.4 Confidentialité des attributs

Comme cela a été présenté au chapitre 3.8, l'infrastructure SuisseTrustIAM doit proposer la possibilité de crypter les informations des utilisateurs entre l'autorité d'attributs et le Relying Party à l'origine de la requête. Ces deux composants ne communiquant que via le Hub STIAM, l'identité du RP ne peut être transmise directement à l'expéditeur STIAM. Mais celui-ci a besoin de cette identité afin de trouver la ‚public key' dans les métadonnées, pour pouvoir crypter les Attribute Assertion pour le Relying Party à l'origine de la requête.

Le Hub STIAM doit par conséquent transmettre l'identité du RP en tant que partie de l'Authentication Request respectivement de la requête d'attribut.

5.5 Single Logout (SLO)

Single Logout (SLO) permet à un utilisateur dans un domaine STIAM de mettre un terme en un ‚clic' à toutes les sessions en cours. Dans le cadre de SuisseTrustIAM, cette fonctionnalité est un service supplémentaire important, car un utilisateur peut, via le Hub STIAM, créer facilement plusieurs sessions pour différents destinataires STIAM (RP). Le SLO l'aide alors à fermer ces sessions de manière propre et simple.

Pour que le SLO fonctionne, le Hub STIAM et le destinataire STIAM doivent avoir une SSO Session pour chaque utilisateur. La Figure 8 expose le procédé de manière grossière: un utilisateur termine une session avec le RP_1. Ce dernier envoie une *LogoutRequest* correspon-

dante au Hub STIAM, qui la valide et, sur la base du *NameID* et du *SessionIndex,* fait fermer toutes les sessions en cours avec d'autres RP et faisant partie de cet index .

L'utilisateur doit être informé qu'il se trouve sur un site Web dans une SSO Session et qu'une déconnexion entraîne la fermeture de toutes les sessions encore en cours.

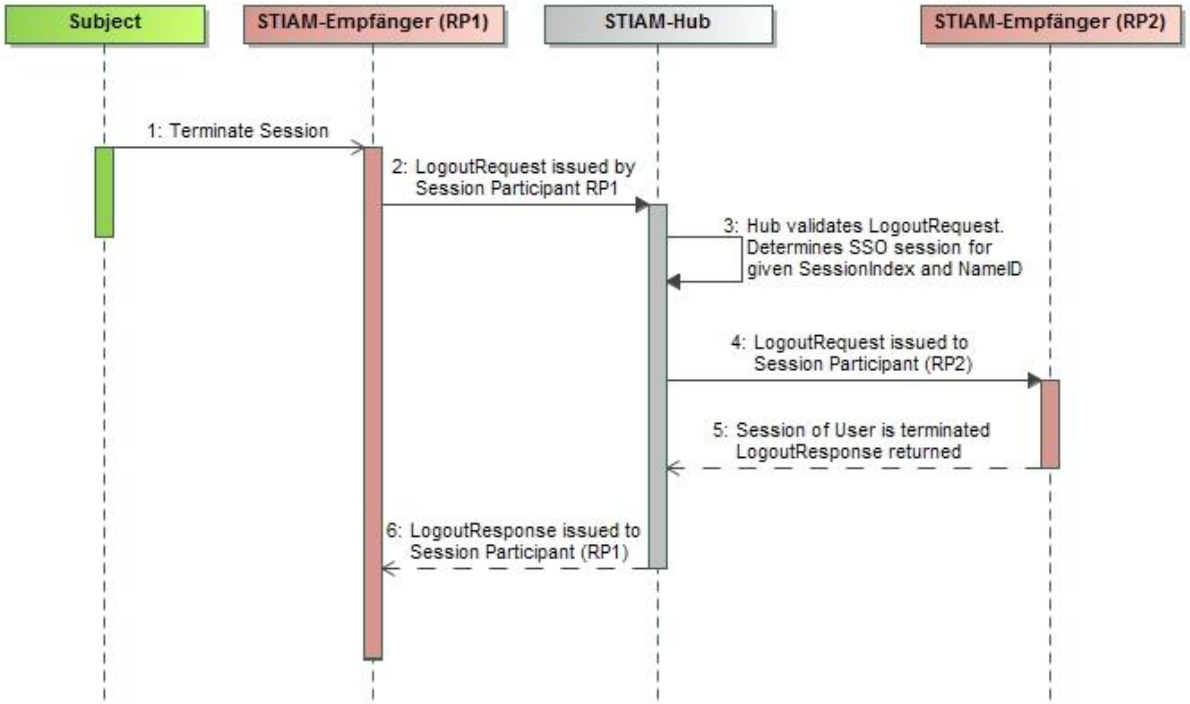


Figure 8: procédé Single Logout

5.6 Reporting, Logging et Monitoring

L'une des exigences de l'infrastructure SuisseTrustIAM est la possibilité de pouvoir tracer la transmission des authentifications et des attributs sur une période donnée. En fonction de l'endroit ou de l'ampleur selon laquelle les données de communication doivent être enregistrées, différentes approches sont possibles.

Logging central

Une fonction partielle du Hub STIAM est un service de Reporting, Logging & Monitoring (RLM), qui enregistre toutes les opérations de communication pour la durée d'exécution. Ceci soulève des questions de protection des données, car les opérations correspondantes sont conservées de manière centralisée. Le Hub STIAM enregistre, pour une durée déterminée, toutes les activités d'un processus de la durée d'exécution, que déclenche un sujet. En fonction du procédé utilisé pour la transmission des informations d'identité (cf. à ce sujet chapitre 3.4), le Hub STIAM doit enregistrer différentes données le Tableau 4).

Logging sur composants périphériques

Pour des raisons de protection des données, il est recommandé d'enregistrer les informations uniquement aux endroits où elles apparaissent et utilisées, c'est-à-dire chez le destinataire STIAM (RP), l'Identity Provider ou l'expéditeur STIAM (AA). Toutefois, ceci va également à l'encontre de l'anonymisation visée des identités transmises. Le système SuisseTrus-

tIAM - en fonction de qui valide une Assertion – part du principe selon lequel un composant dans un processus de durée d'exécution dispose uniquement d'un jeu déterminé d'informations concernant une identité numérique.

- En règle générale, un destinataire STIAM ne connaît pas toutes les informations d'identité, qui identifient un sujet sans ambigüité. Il ne peut ainsi établir un protocole que pour une partie de l'opération globale.
- L'IdP STIAM connaît pour sa part l'identité, mais pas les attributs, qui sont agrégés à partir d'autres sources par le Hub STIAM.
- En règle générale, un expéditeur STIAM connaît uniquement les attributs et l'identificateur (dont il a connaissance). Seul le Hub STIAM est en possession de toutes les informations et a connaissance de toutes les opérations au cours d'un processus de durée d'exécution.

La matrice suivante pour le comportement de Reporting, de Logging et de Monitoring des différents composants peut être élaborée à partir de ces considérations:

	Hub STIAM	Destinataire STIAM	IdP STIAM	Expéditeur STIAM
Données de connexion	M/L	M/L	M/L	M/L
Informations sur la transmission	R/M/L	-	-	-
Contenus de l'attribut	(R/M/L)[19]	L	-	L
Informations d'authentification	R/M	-	L	-
Informations sur la session du sujet	R/M/L	L	L	L

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

[19] Le Hub STIAM doit consigner les contenus des attributs, quand il opère en Identity Proxy Mode (IP-Mode) et un Attribut ‚auditable' est établi (cf. à ce sujet le chapitre 7.5.4.4 page 60).

6 Protocoles pour la période de définition

6.1 Protocole de Linking

On peut établir une distinction entre deux protocoles de Linking pour la durée de définition. Le protocole IdP-Linking est utilisé entre le Hub STIAM et un IdP STIAM. Il comprend les étapes 3 à 10 du processus présenté par la Figure 9. Le protocole AA-Linking est représenté par la Figure 10. Il est utilisé entre le Hub STIAM et un expéditeur STIAM (AA).

Comparer aussi à ce sujet les descriptions de processus «Administration des IdP/AA-Links» au chapitre 7.3.2.

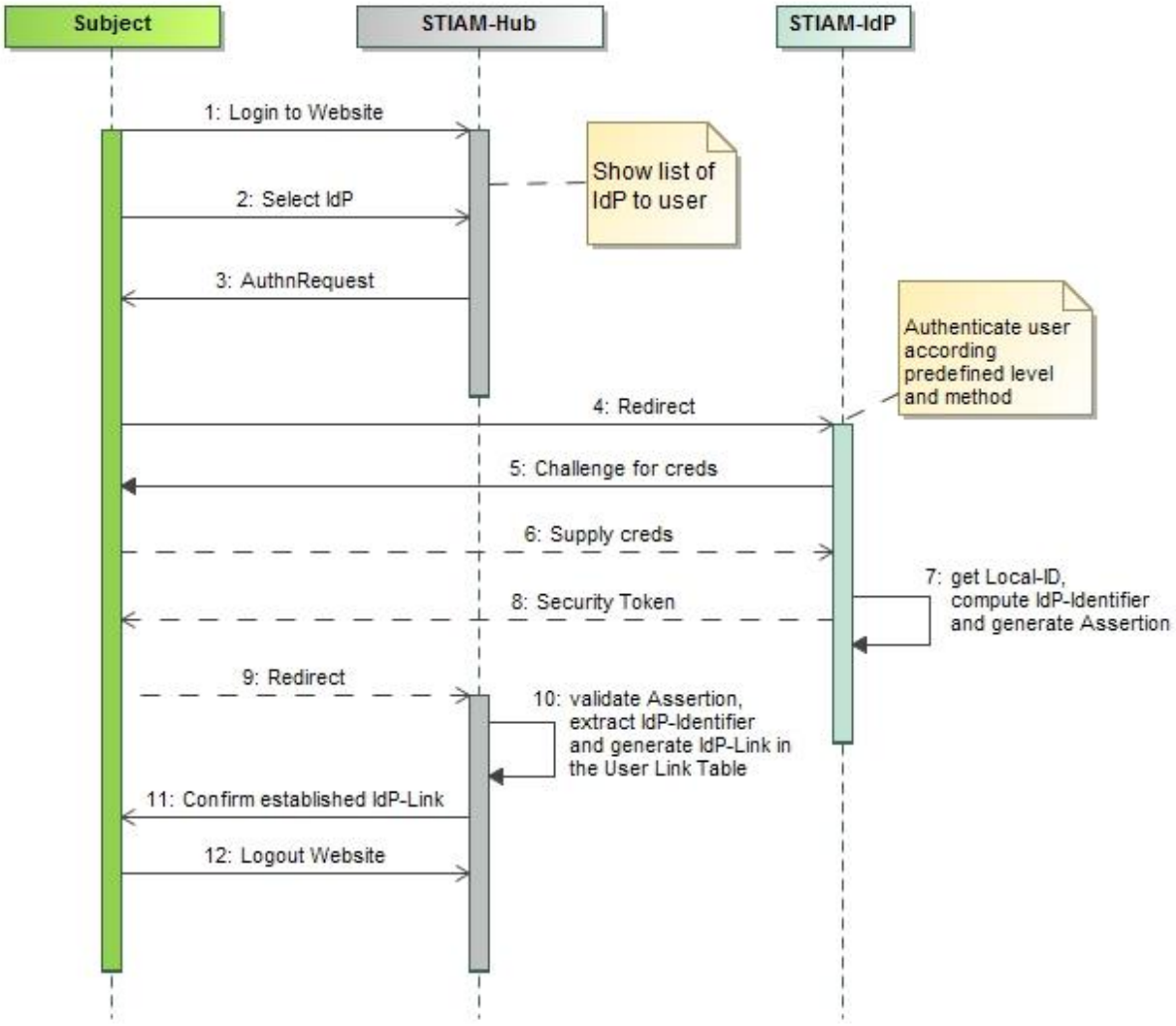


Figure 9: protocole IdP-Linking

Description du protocole IdP-Linking

Le protocole IdP-Linking permet à un utilisateur d'intégrer, de manière interactive, un IdP STIAM à son Link Table. Sur son site Web, le Hub STIAM offre à un utilisateur la possibilité de choisir un IdP possible dans une liste (1-2) et d'établir un lien vers lui. L'utilisateur est redirigé par le Hub STIAM vers l'Authentication Service de l'IdP STIAM (3-4). L'utilisateur est authentifié par ce dernier au moyen de la méthode qu'il connaît et qui a cours localement (5-

6). Dans son Assertion, l'IdP STIAM renvoie au Hub STIAM un identificateur de l'utilisateur signé et calculé par lui (8-9). Le Hub STIAM peut ainsi ajouter l'identificateur obtenu au Link Table de l'utilisateur (10).

Lors de l'élaboration et de l'administration des Identity Links, le Hub doit garantir que l'utilisateur s'authentifie auprès d'un ou de plusieurs IdP soit afin d'atteindre le QAA-Level maximum des identités associées, soit de garantir une sécurité équivalente par le biais d'authentifications multiples avec différents Credentials.[20]

Description du protocole AA-Linking

Le protocole AA-Linking permet à un utilisateur d'intégrer, de manière interactive, un expéditeur STIAM (AA) à son Link Table. Sur son site Web, le Hub STIAM offre à un utilisateur la possibilité de sélectionner un AA possible dans une liste (1-2) et d'établir un lien vers lui. Le Hub STIAM envoie à cette fin une *Authentication Request* à l'expéditeur STIAM (4). L'expéditeur STIAM requiert l'authentification de l'utilisateur et redirige pour cela l'Authentication Request vers un IdP approprié (5-10), via le navigateur de l'utilisateur. L'IdP utilisé peut être une partie de l'AA (IdP interne ou local) ou l'AA peut utiliser un IdP STIAM approprié. L'utilisateur est authentifié par l'IdP sélectionné selon la méthode qu'il connaît et qui a cours localement (7-8). Une fois l'authentification achevée avec succès, l'expéditeur STIAM détermine l'identificateur local de l'utilisateur (11) et le transmet, signé et pourvu d'une estampille, au Hub STIAM, en tant que Security Token via le navigateur de l'utilisateur (12-13). Le Hub STIAM peut ainsi ajouter l'identificateur obtenu au Link Table de l'utilisateur (14).

Lors de l'élaboration et de l'administration des Attribute Links, le Hub doit garantir que l'utilisateur s'authentifie auprès d'un ou de plusieurs IdP, de sorte à atteindre une qualité d'authentification, qui correspond à la qualité maximale des identités associées ou à une combinaison appropriée de plusieurs authentifications multiples avec différents Credentials de sécurité équivalente.

[20] Afin de résoudre le problème de la première élaboration d'Identity Links, le Hub STIAM peut mettre à disposition ce que l'on appelle un Bootstrap-Account, qui dispose d'une authentification simple à 2 facteurs. Cet Account ne peut être utilisé qu'à des fins administratives, mais pas vis-à-vis d'un RP et devrait être désactivé après la création du premier Identity-Link. En cas de problème, ce Bootstrap-Account pourrait être réactivé par le Helpdesk afin de corriger les liens invalides.

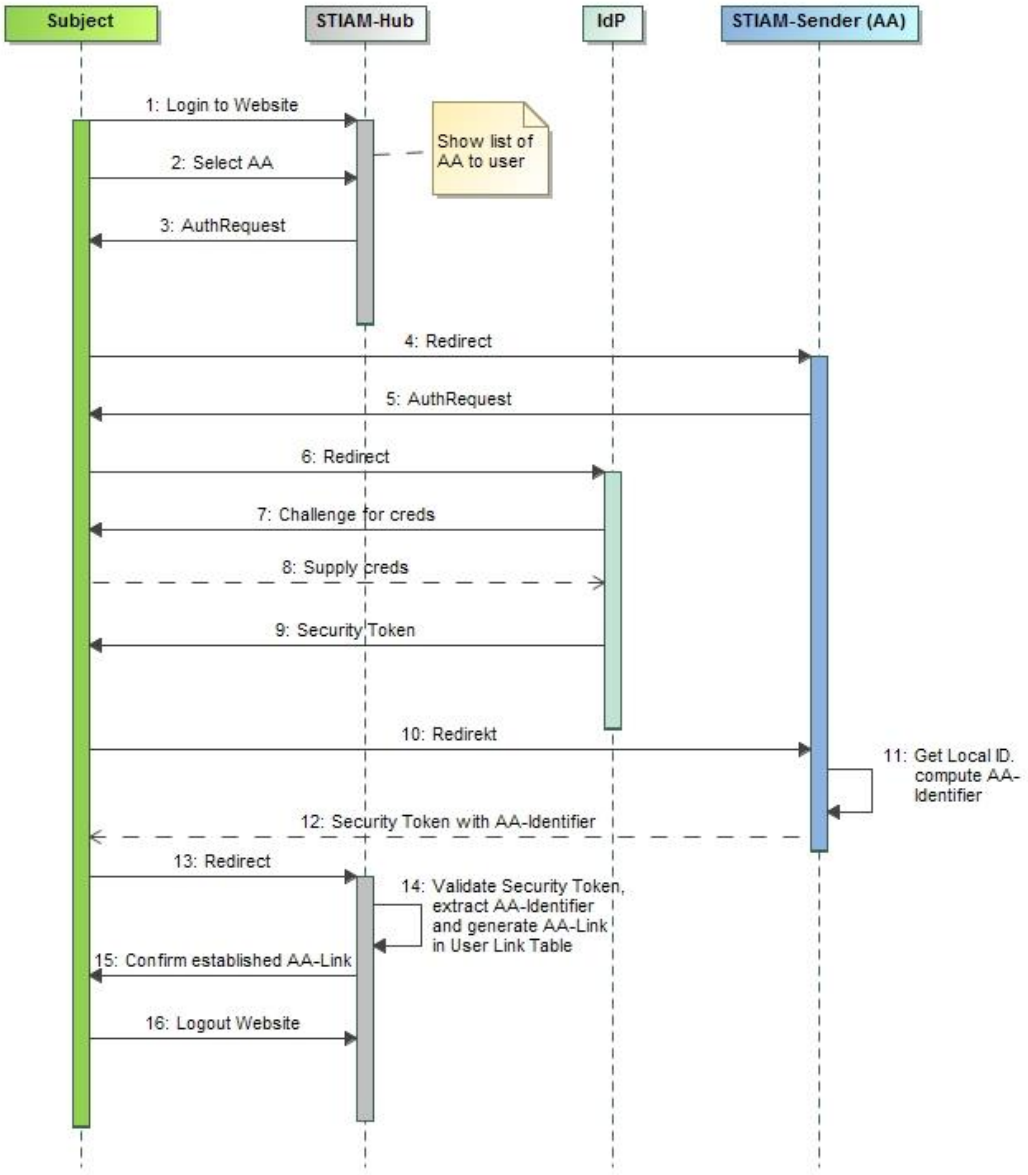


Figure 10: protocole AA-Linking

6.2 Agrégation et répartition des métadonnées

Le responsable de système d'une organisation peut, au moyen du Component Management, ajouter et configurer les composants mis à disposition. Les différentes étapes correspondantes sont présentées en détail dans la description des processus administratifs au chapitre 7 correspondantes sont présentées en détail dans la description des processus administratifs au chapitre 7. Ces informations sont enregistrées dans la base de données du Hub STIAM. Pour une autorité d'attributs, des attributs peuvent être définis avec leurs paramètres, restrictions etc. D'un autre côté, les exigences (attributs, QAA-Level, qualité d'attribut, etc.) peuvent être stipulées – par ressource – pour un Relying Party.

Ces métadonnées doivent être agrégées par le Hub STIAM et mises à la disposition des composants STIAM, une fois pourvues d'une signature numérique. Un IdP/AA reçoit alors

les métadonnées des destinataires STIAM (RP) et inversement, un RP celles des IdP/AA (comparer aussi à ce sujet les métadonnées Eléments dans la Figure 5 et la Figure 6).

Les métadonnées comprenant également les certificats des différents composants STIAM, les relations de confiance nécessaires peuvent également être établies par ce biais.

7 Processus administratifs et modèle de données

Les processus administratifs peuvent être répartis en quatre domaines, que l'on retrouve sur la carte nationale des processus (Figure 12) et dans le modèle de données (Figure 13). Ces domaines reflètent les fonctions principales du Hub STIAM au niveau administratif:

1. *Account Management:* exploitation des données des Accounts des sujets dans l'User Identifier Repository et le Link-Table.
2. *Organisation Management:* administration des données et autorisations de l'organisation. En outre, les personnes responsables d'une organisation y sont gérées avec leurs rôles et privilèges.

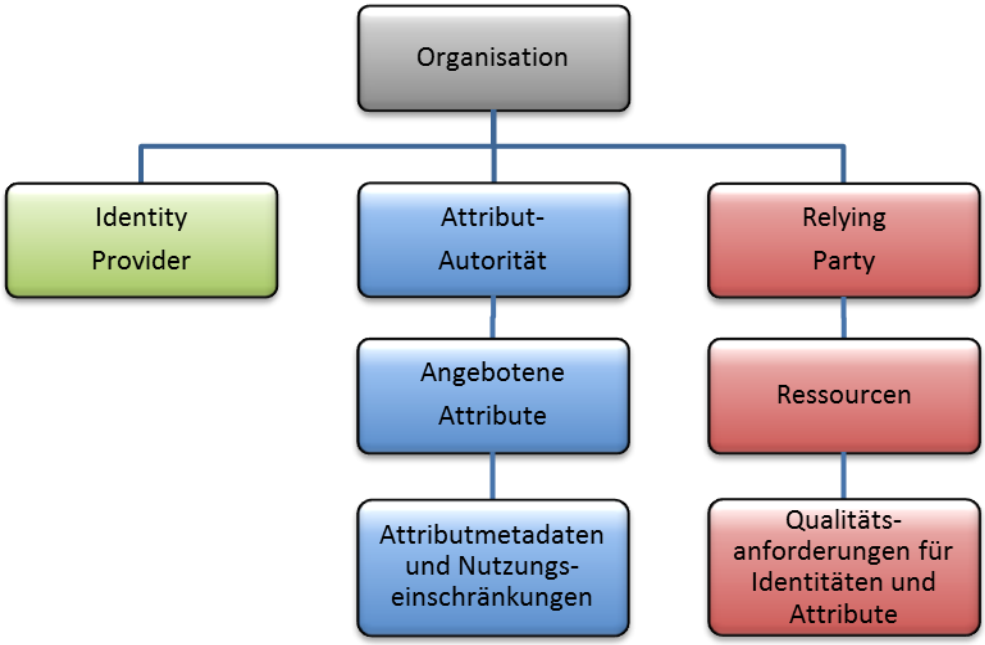


Figure 11: variantes de l'organisation

3. *Component Management:* exploitation des entités SuisseTrustIAM d'une organisation. Une organisation peut enregistrer différentes entités sur la plateforme SuisseTrustIAM.
   Les informations nécessaires concernant ces entités (métadonnées) sont également enregistrées dans la base de données du Hub STIAM. Ces informations sont saisies et mises à jour par l'administrateur système de l'organisation (voir OrgSysAdmin dans le Tableau 5). Une autorité d'attributs peut en outre définir les attributs qu'elle propose sur le Hub STIAM, en saisissant les métadonnées d'attributs correspondantes et leurs restrictions d'utilisation. D'un autre côté, un Relying Party peut, pour chaque ressource contrôlée, stipuler ses exigences (attributs, QAA-Level, qualité d'attribut etc.) dans la base de données.
4. *Attribut Management:* la définition, la mise à jour et la publication des attributs, qui doivent être utilisés au sein de la Community, constituent une autre tâche du Hub

STIAM SuisseTrustIAM. C'est la raison pour laquelle tous les attributs, même centralisés, doivent être définis de telle sorte qu'ils puissent être référencés pour les entités dans les différents processus administratifs.

Les processus pour l'IdP, l'expéditeur et le destinataire STIAM sont également répertoriés dans les processus administratifs, dans la mesure où ils se déroulent en interaction avec le Hub STIAM. Tous les autres processus administratifs internes de ces composants (UserManagement local, User Filtering, Mapping des identités et attributs) ne sont pas traités dans ce document.

Dans les processus exposés ci-après, on distingue, outre l'utilisateur lui-même, au sens d'une personne physique, entre trois rôles spécifiques. Ceux-ci sont répertoriés sommairement et décrit brièvement dans le Tableau 5. Se reporter également au document eCH-0169 ‚Architecture administrative SuisseTrustIAM' pour une description détaillée des rôles ainsi que de leurs tâches, compétences et responsabilités.

Rôle	Description
SuisseTrustIAM System Administrator (STIAM-SysAdmin)	Le STIAM-SysAdmin est un rôle de l'exploitant du Hub STIAM. Il est notamment en charge des tâches administratives dans le cadre de l'Organisation Management lors de la création initiale d'organisations ainsi que de l'enregistrement des informations correspondantes.
Responsable d'organisation (RO)	Le STIAM-SysAdmin doit affecter un RO à chaque organisation. Celui-ci enregistre et tient à jour les informations spécifiques à l'organisation et délègue les tâches administratives en lien avec les différents composants à un ou plusieurs OrgSysAdmin. Le RO remplit par ailleurs une fonction de contrôle à l'égard du OrgSysAdmin.
Administrateur système d'une organisation (OrgSysAdmin)	Le RO compétent affecte à chaque organisation au moins un OrgSysAdmin. Celui-ci remplit différentes tâches dans le cadre du Component Management en lien avec l'administration des composants, ressources et attributs.

Tableau 5: description des rôles à l'intérieur des processus administratifs

7.1 Vue d'ensemble de la carte nationale des processus

Comme cela a déjà été décrit en introduction, la carte nationale des processus administratifs est organisée selon les quatre domaines *Account Management*, *Organisation Management*, *Component Management* et *Attribut Management*, que l'on retrouve également dans le modèle de données. Les différents processus administratifs sont affectés à ces domaines.

Le Trust Management figure également sur la carte nationale des processus en tant que domaine supplémentaire. Celui-ci a été inclus au graphique dans un souci d'exhaustivité. Le Trust Management apparaît d'une part sous forme de processus administratifs partiels dans

les autres domaines principaux et d'autre part, comme une partie intégrante de la Gouvernance. Ainsi la définition des composants, l'agrégation et la distribution digne de confiance des métadonnées, l'établissement d'un service de certification commun comme «ancrage de confiance», ainsi que l'administration centrale des attributs sont autant d'exemples de processus partiels importants du Trust Management.

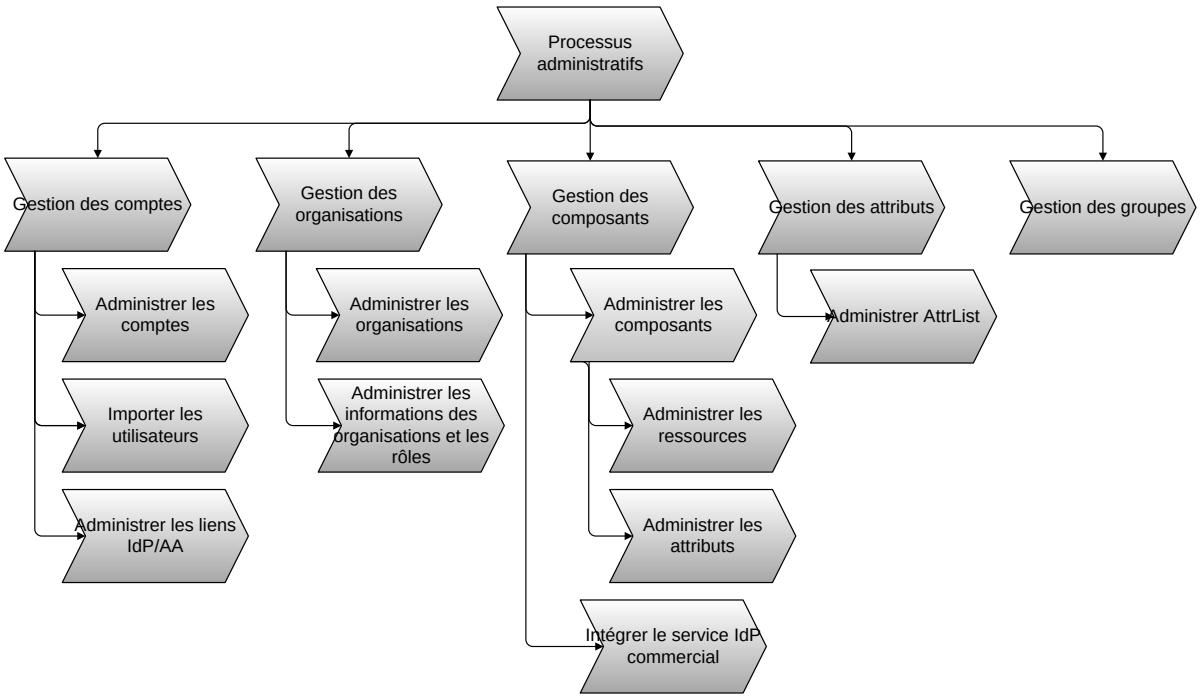


Figure 12: carte nationale des processus administratifs du Hub STIAM

Les différents processus et leur rapport avec le modèle de données sont décrits en détail dans les sous-chapitres suivants. L'attention est attirée sur le fait que deux processus n'apparaissent plus dans la suite de ce document. Il s'agit d'une part du processus «Intégration d'un service IdP commercial» sous Component Management. L'intégration de services IdP commerciaux doit être traitée au cas par cas et ne convient actuellement pas à la description des processus standardisée. Leur mise en œuvre est en outre tributaire des décisions prises au niveau des organismes de pilotage.

Par ailleurs, le processus «Administration de la liste des attributs» dans l'Attribut Management n'est pas non plus abordé de manière explicite. Les concepts et les méthodes relatifs à la définition, l'administration et la détermination de la sémantique d'attributs déterminés sont spécifiés avec plus de précision dans un document complémentaire.

7.2 Modèle de données

Dans les chapitres qui suivent, le modèle de données exposé ici dans son intégralité sera ordonné (réparti) selon les quatre domaines de Management. Les différents processus administratifs et les parties les plus importantes du modèle de données d'un domaine y sont exposés et décrits de manière plus détaillée. Le modèle de données comprend uniquement les objets nécessaires, d'un point de vue conceptuel, et peut donc être encore précisé et élargi.

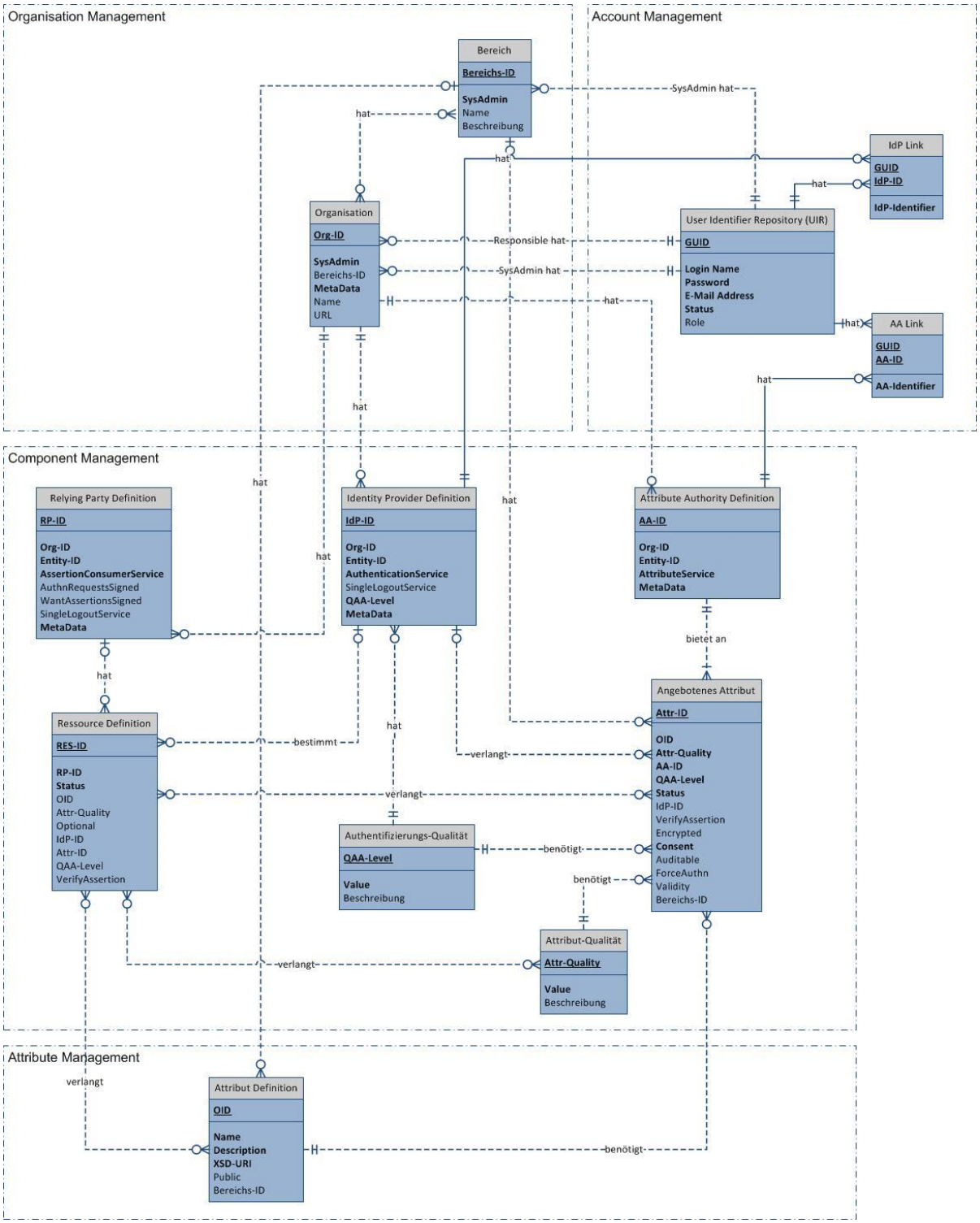


Figure 13: modèle de données SuisseTrustIAM Broker[21]

[21] Dans un souci d'une plus grande clarté, le modèle de données ne comprend délibérément pas de tableau intermédiaire concernant les relations *n:m*. Au lieu de cela, on y a re-présentées et inscrites les connexions directes entre les tableaux.

7.3 Account Management

L'Account Management peut être grossièrement réparti entre l'administration des données des Accounts effectifs et l'administration des Links vers les différents composants. Ceci se reflète tant dans les processus que dans les parties correspondantes qui composent le modèle de données.

7.3.1 Administration des données d'Account

Un utilisateur doit initialement créer un Account sur le Hub STIAM. Dans le cas d'une personne physique, celui-ci peut être créé de manière interactive sur un site Web du Hub STIAM. Il est en outre possible de modifier ses propres données de Account et de supprimer un Account déjà existant.

7.3.1.1 Administration d'Account

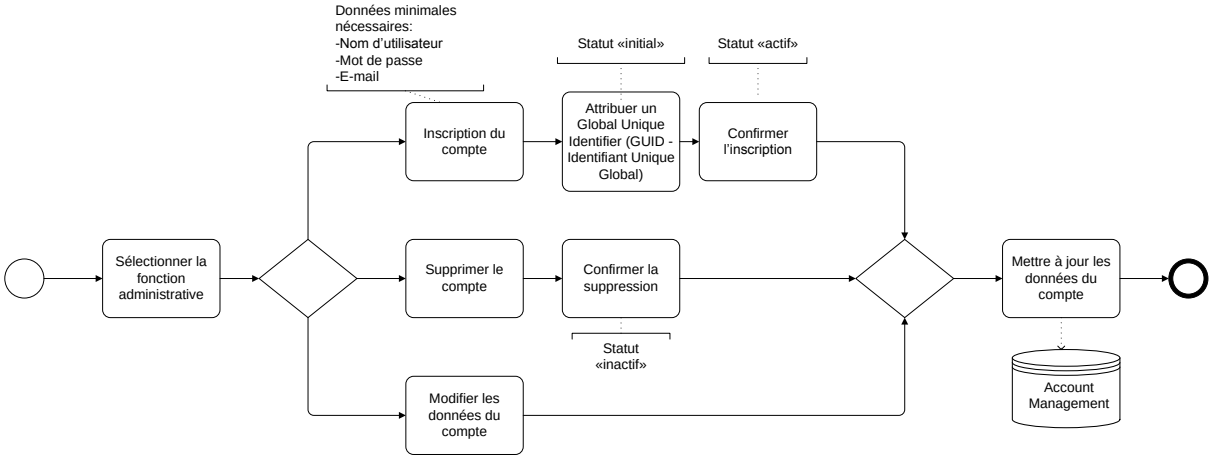


Figure 14: processus d'administration d'un Account

Les exigences minimales nécessaires à l'enregistrement d'un Account sont un identifiant de connexion, un mot de passe ainsi qu'une adresse E-mail active. Le système attribue à chaque utilisateur un Global Unique Identifier (GUID) et règle le statut de l'Account sur «initial». Tant l'activation de l'Account que la suppression du dit Account requièrent la confirmation de l'utilisateur, (ce qui modifie le statut de l'Account).

Pour les utilisateurs d'organisations, l'utilisateur peut ouvrir l'Account, mais il doit être possible, en cas de besoin, d'amorcer un processus d'autorisation afin qu'un responsable de l'organisation puisse autoriser la publication.

Les données d'Account sont enregistrées dans l'Account Management, plus précisément dans l'User Identifier Repository (UIR).

7.3.1.2 Importer des utilisateurs

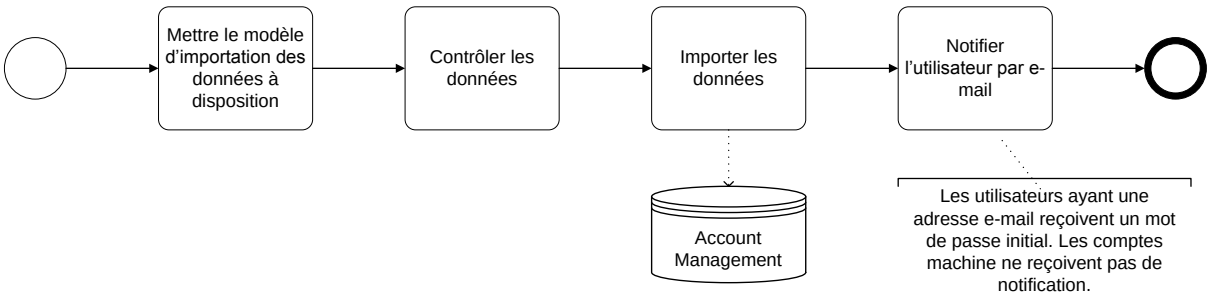


Figure 15: processus d'importation d'utilisateurs

Outre l'enregistrement manuel d'utilisateurs, des Accounts peuvent également être créés par un OrgSysAdmin d'une organisation membre au moyen d'une importation de masse. Un Template (modèle) correspondant est mis à disposition à cette fin. Les utilisateurs créés reçoivent une notification comprenant un mot de passe initial pour l'accès au Hub STIAM.

Dans ce cas également, les données d'utilisateurs dans l'Account Management sont enregistrées avec plus de précision dans l'UIR. Leurs contenus sont décrits dans la suite du document.

7.3.1.3 User Identifier Repository (UIR)

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

L'User Identifier Repository (UIR) contient les informations sur l'Account d'un sujet. Ces informations peuvent, tel que décrit ci-dessus, être enregistrées manuellement ou téléchargées dans le cadre d'une importation de masse.

Comme le montre le tableau ci-dessous, l'UIR contient, outre quelques champs obligatoires, un ‚champ de statut', qui contient le statut visible dans la Figure 14.

Nom du champ	Signification	Type
GUID	Désignation sans ambigüité du sujet. Le GUID est affecté à un Account par le système.	Clé primaire
Login Name	Identifiant de connexion de l'utilisateur	Champ obligatoire
Password	Mot de passe Bootstrap pour l'User Account (compte utilisateur)	Champ obligatoire
E-Mail Address	Adresse E-mail pour la confirmation de l'Account	Champ obligatoire
Status	Statut de l'User Account. Valeurs possibles: Initial, Active, Recover, Disabled, Inactive (les valeurs sont affectées par le système)	Champ obligatoire

Nom du champ	Signification	Type
Role	A titre facultatif, un sujet peut jouer un rôle au sein l'organisation. Exemple d'une plage de valeurs: - Responsible (RO) - User-Management (OrgSysAdmin) - IdP/AA-Management (OrgSysAdmin) - RP-Management (OrgSysAdmin)	Champ facultatif

Tableau 6: User Identifier Repository

7.3.2 Administration des IdP/AA-Links

A titre facultatif, un sujet peut associer un(e) ou plusieurs Identity Providers (IdP) respectivement Attribute Authorities (AA) à son Account.

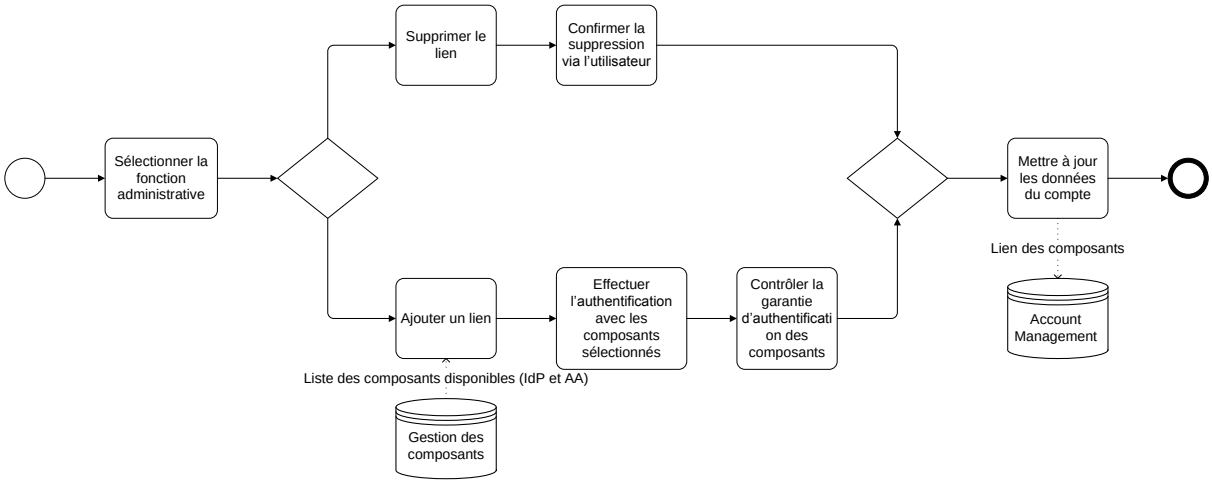


Figure 16: processus d'administration des IdP/AA-Links

cette fin, l'utilisateur se voit proposer de choisir entre les IdP respectivement AA enregistrés dans le Component Management (voir chapitre 7.5.1). Afin de pouvoir établir un lien vers un composant correspondant, il est nécessaire de disposer d'une authentification de l'utilisateur par rapport au composant (voir chapitre 6.1). En cas de succès, celui-ci émet un *Security Token*, qui est contrôlé par le Hub STIAM. Si le contrôle est concluant, l'IdP/AA-Link dans l'Account Management est enregistré dans le Link Table correspondant.

IdP Link	AA Link
GUID **IdP-ID**	**GUID** **AA-ID**
IdP-Identifier	**AA-Identifier**

Chaque lien de composant est confirmé par l'instance concernée au moyen de l'identificateur, ce qui entraîne un classement unique de l'utilisateur pour le système destinataire.

Outre l'ajout de liens de composant, l'utilisateur peut également se charger de leur suppression. Cette suppression doit faite l'objet d'une confirmation par l'utilisateur. Le Component-Link correspondant est supprimé dans l'Account Management.

7.4 Administrer l'Organisation Management

La saisie d'une organisation comme membre de SuisseTrustIAM implique deux processus, qui doivent être exécutés par différents rôles.

7.4.1 Administrer l'organisation

Une organisation est tout d'abord ajoutée sur le Hub STIAM par le STIAM-SysAdmin. L'organisation se voit affecter un Org-ID unique ainsi qu'un responsable d'organisation (RO). L'Org-ID est délivrée automatiquement par le système. Le STIAM-SysAdmin affecte le RO. Pour ce faire, il faut qu'un Account correspondant soit déjà présent dans l'Account Management. Tant l'Org-ID que le GUID du RO sont enregistrés dans l'Organisation Management (voir Tableau 7).

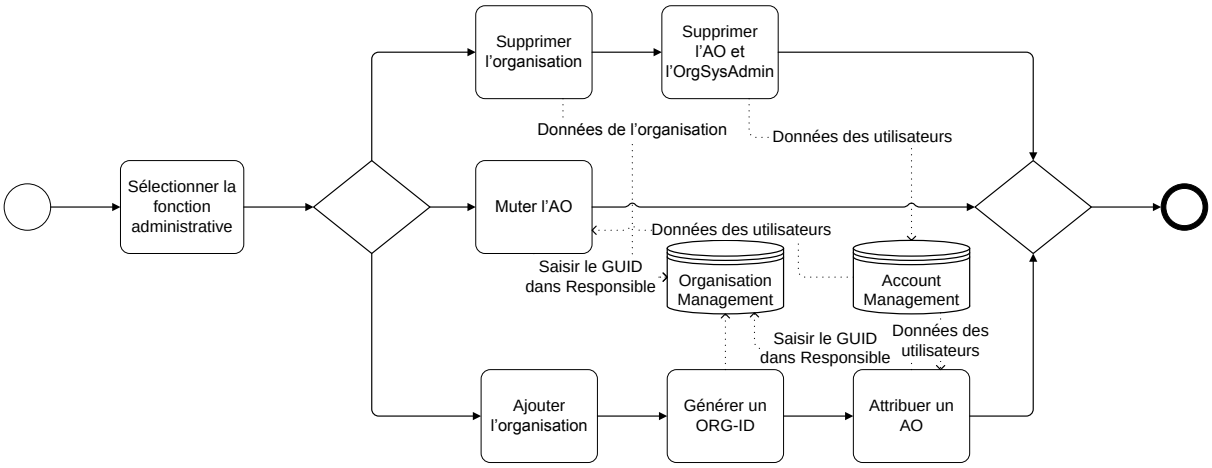


Figure 17: processus d'administration des organisations

Outre l'ajout d'une organisation, le STIAM-SysAdmin se réserve également le droit de changer le responsable d'organisation d'une organisation ou de supprimer une organisation. Si l'on supprime une organisation, le système respectivement le STIAM-SysAdmin doit vérifier qu'aucun composant (voir chapitre 7.5.1) n'y est plus affecté. Il faut de plus supprimer les éventuelles affectations de responsable d'organisation et d'OrgSysAdmin dans l'Account Management.

7.4.2 Administrer les informations d'organisation et des rôles

Après qu'une organisation a été ajoutée par le STIAM-SysAdmin, il incombe au responsable d'organisation de gérer les informations de l'organisation et de nommer un ou plusieurs administrateurs système (OrgSysAdmin).

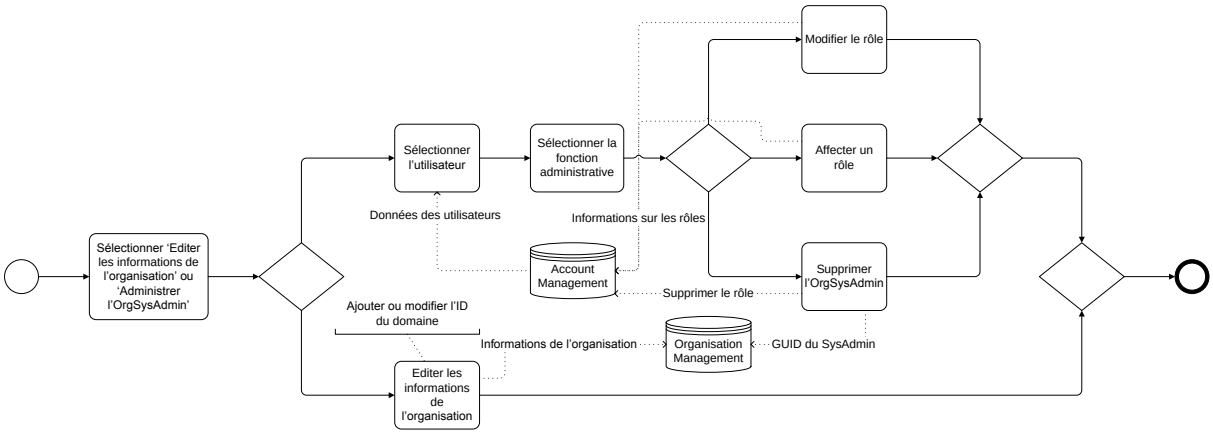


Figure 18: processus d'administration des informations d'organisation et des rôles

Le RO enregistre un interlocuteur ainsi que les informations supplémentaires (Name, Display Name, URL) concernant l'organisation. Une organisation peut par ailleurs être affectée à un ou plusieurs domaines (voir chapitre 2.3).

Seul un User-Account déjà existant peut se voir affecter un rôle spécifique par le RO en tant qu'OrgSysAdmin. Il est également possible d'adapter ce rôle ainsi que de le supprimer. Le GUID de l'Account correspondant est conservé dans l'Organisation Management, les données relatives au rôle correspondant étant enregistrées dans l'Account Management.

7.4.3 Organisation dans le modèle de données

La définition d'une organisation en tant que membre de SuisseTrustIAM comprend quelques champs obligatoires. Une organisation a un ou plusieurs administrateurs système (SysAdmin). A titre facultatif, une organisation peut appartenir à un ou plusieurs domaines (ID domaine). De plus, les métadonnées, ex. ‚Contact Person' ou ‚Organization', doivent être enregistrées.

Une organisation peut avoir des caractéristiques descriptives, comme un nom ou une URL.

Nom du champ	Signification	Type
Org-ID	Désignation sans ambigüité de l'organisation	Clé primaire
SysAdmin (OrgSysAdmin)	GUID de l'administrateur système d'une organisation. Le SysAdmin se voit attribuer le rôle correspondant dans l'UIR.	Clé étrangère
ID domaine	Champ facultatif, qui désigne l'appartenance à un domaine (groupe délimité d'organisations). Une organisation peut se trouver dans plusieurs domaines.	Champ facultatif
MetaData	Métadonnées de l'organisation	Champ obligatoire
Name	Nom de l'organisation	Champ facultatif

URL	URL de l'organisation	Champ facultatif

Tableau 7: Organisation Management

Un domaine constitue un groupe délimité d'organisations. Les entités d'IdP/AA au sein de ce groupe peuvent mettre à disposition des attributs spéciaux. L'appartenance à un domaine habilite alors un Relying Party à demander ces attributs
Un domaine a un plusieurs administrateurs système, comme le nom et la description

Nom du champ	Signification	Type
ID domaine	Désignation sans ambigüité du domaine	Clé primaire
SysAdmin (OrgSysAdmin)	GUID de l'administrateur système d'une organisation. Le SysAdmin se voit attribuer le rôle correspondant dans l'UIR.	Clé étrangère
Nom	Nom du domaine	Clé facultative
Description	Description du domaine	Clé facultative

Tableau 8: définition du domaine

Afin de pouvoir affecter un SysAdmin à une organisation ou à un domaine, ces derniers doivent disposer d'un Account sur le Hub STIAM.

7.5 Component Management

Dans le Component Management, les différents composants d'une organisation, c'est-à-dire l'IdP, l'AA et le Relying Party (RP), sont gérés par l'OrgSysAdmin. Dans le cas d'un Relying Party, les ressources sont en outre tenues à jour comme les attributs par une autorité d'attributs.

7.5.1 Administrer les composants

Un composant est ajouté respectivement supprimé par l'OrgSysAdmin ou ses données sont modifiées.

Si l'on ajoute un composant, un certificat doit être émis par STIAM-CSP. Pour ajouter un IdP, il est impératif d'indiquer un QAA-Level.

Si un composant existant est supprimé, il faut vérifier que plus aucune ressource ne soit en relation avec le composant. La suppression définitive doit être confirmée et le certificat émis par le SuisseTrustIAM-CSP être révoqué. Toutes les modifications sont mises à jour dans la Component Management, ce qui a pour effet que les métadonnées de Community sont à nouveau signées et publiées par SuisseTrustIAM-MDR.

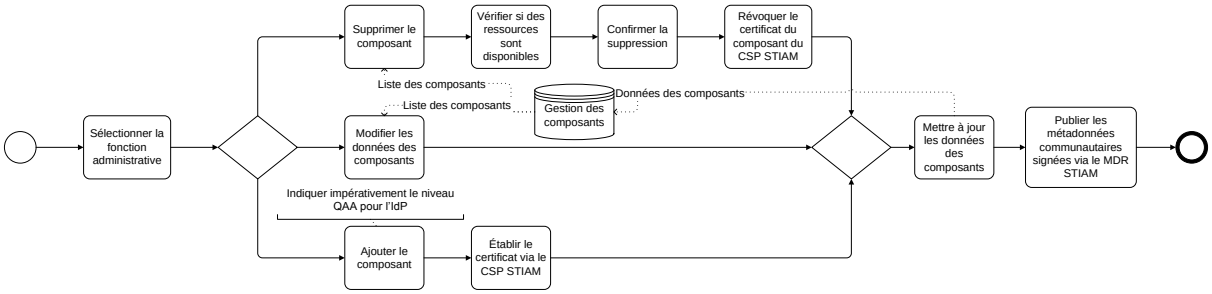


Figure 19: processus d'administration des composants

7.5.2 Administration des ressources

L'OrgSysAdmin affecte les ressources correspondantes à un Relying Party enregistré dans le Component Management.

Une RES-ID est affectée par le système à une ressource créée. A titre facultatif, différentes règles peuvent être configurées pour une ressource:

- Prescrire le(s) attribut(s) (attributs du domaine correspondant comme seule possibilité)
- Prescrire l'Identity Provider (seuls certains IdP sont acceptés)
- Prescrire le QAA-Level (QAA-Level minimal accepté)
- Valider l'Assertion elle-même

En outre, les options d'attributs suivantes peuvent être configurées:

- L'attribut est facultatif
- Prescrire la qualité d'attribut

Les informations saisies par l'OrgSysAdmin, ainsi que les options configurées concernant une ressource doivent être validées par le RO compétent et la ressource être activée. Ce n'est qu'alors que le statut de la ressource passe de «ToBeValidated» à «actif».

De la même manière, il est également possible de modifier les données d'une ressource existante. Si une ressource existante est affectée à un autre Relying Party, l'affectation est modifiée en conséquence dans le Component Management, les données des ressources en revanche sont reprises inchangées. Il est en outre possible de supprimer une ressource existante. Dans tous les cas, une suppression définitive doit faire l'objet d'une confirmation. Toutes les modifications entraînent une publication des métadonnées de Community signées par le SuisseTrustIAM-MDR.

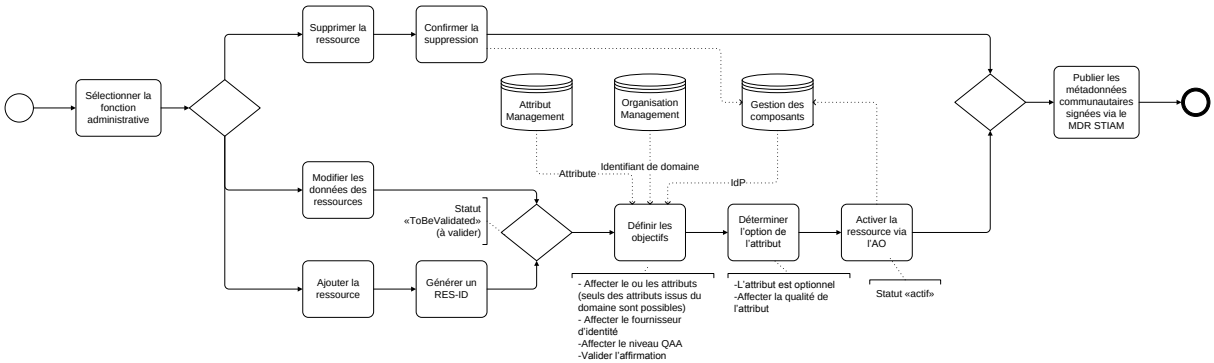


Figure 20: processus d'administration des ressources

7.5.3 Administrer les attributs

Les attributs correspondants sont ajoutés ou supprimés pour une autorité d'attributs. En outre, leur configuration peut faire l'objet de modifications. Les attributs sont affectés à un AA spécifique par l'OrgSysAdmin.

Toute nouvelle affectation d'attribut reçoit du système une Attribute-ID. L'attribut concret est sélectionné à partir d'une liste d'attributs disponibles. Les renseignements concernant les attributs proviennent à ce titre de l'Attribute Management. La liste générée est filtrée selon les données de configuration dans l'Organisation Management (selon l'ID domaine par exemple). Pour chaque attribut ajouté, il faut indiquer une valeur de qualité ainsi qu'un QAA-Level (voir chapitre 7.5.4.4).
En outre les options suivantes peuvent être configurées:

- Demande de «validation de l'affirmation»
- Prescription du cryptage des attributs
- Désactivation du «Consentement utilisateur nécessaire»
- Prescription de l'Identity Provider

Dans le cas de l'administration des attributs également, les informations saisies par l'OrgSysAdmin, ainsi que les options configurées doivent être validées par le RO compétent et ainsi activées. Ce n'est qu'alors que le statut de la ressource passe de «ToBeValidated» à «actif».

Toute suppression définitive d'un ou de plusieurs attributs affectés requiert une confirmation préalable. Toutes les modifications entraînent également la publication des métadonnées Community signées par le SuisseTrustIAM-MDR.

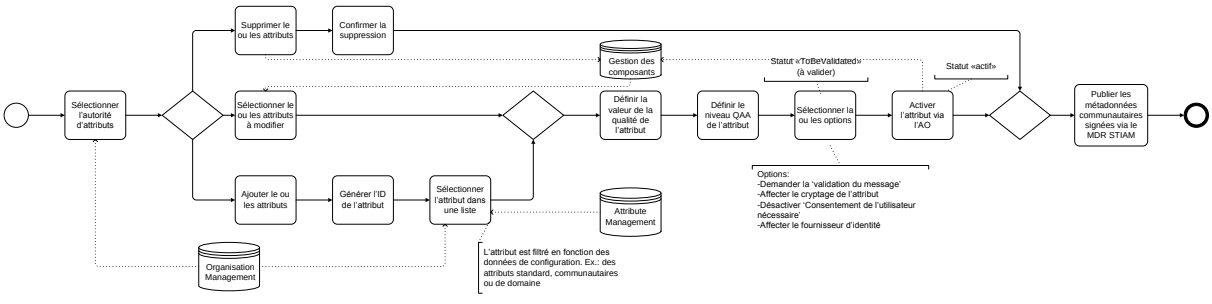


Figure 21: processus d'administration des attributs

7.5.4 Composants, ressources et attributs dans le modèle de données

Lors de l'intégration d'une organisation en tant que membre de SuisseTrustIAM, un objet Organisation est créé tel que décrit au chapitre 7.4 Sous cet objet, l'OrgSysAdmin peut créer les différents composants (IdP, AA, RP). Les attributs nécessaires sont enregistrés dans les tableaux suivants:

- Définition de l'Identity Provider
- Définition de l'Attribute Authority
- Définition du Relying Party
- Définition de la ressource

Avec les métadonnées de l'organisation (Organization, Contact Person) du chapitre 7.4 , toutes les métadonnées pour la Community SuisseTrustIAM peuvent être constituées à partir de ces données.

7.5.4.1 Définition du QAA-Level et de la qualité d'attribut

La définition des différents composants présuppose la définition de la qualité d'authentification et d'attribut.

La qualité d'authentification doit être définie conformément à «eCH-0170 Modèle de qualité des identités électroniques» [4]. Pour ce faire, un identificateur unique et la valeur (Value) doivent être définis pour chaque niveau possible. A titre facultatif, il est possible d'indiquer une description.

Nom du champ	Signification	Type
QAA-Level	Désignation sans ambigüité du QAA-Level	Clé primaire
Value	Niveau de qualité	Champ obligatoire
Description	Description du QAA-Level	Clé facultative

Tableau 9: définition de la qualité d'authentification (QAA-Level)

La qualité d'attribut doit être définie conformément à «eCH-0171 Modèle de qualité de la confirmation de valeur d'attribut pour l'eID» [5]. Pour ce faire, un identificateur unique et la valeur (Value) doivent être définis pour chaque niveau de qualité possible. A titre facultatif, il est possible d'indiquer une description.

Nom du champ	Signification	Type
Attr-Quality	Désignation sans ambigüité de la qualité d'attribut	Clé primaire

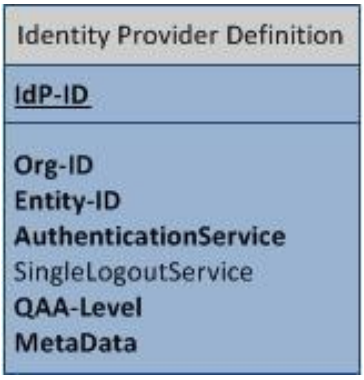
Nom du champ	Signification	Type
Value	Niveau de qualité	Champ obligatoire
Description	Description de la qualité d'attribut	Clé facultative

Tableau 10: définition qualité d'attribut

7.5.4.2 Identity Provider Definition

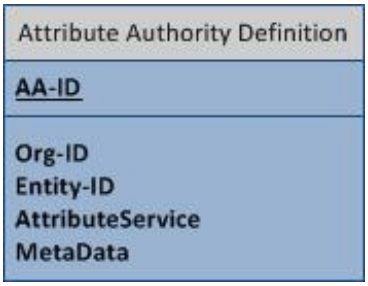
Nom du champ	Signification	Type
IdP-ID	Désignation sans ambigüité de l'IdP	Clé primaire
Org-ID	Organisation à laquelle appartient l'IdP	Clé étrangère
Entity-ID	Nom unique de l'Entity	Champ obligatoire
AuthenticationService	URI pour le service d'authentification	Champ obligatoire
SingleLogoutService	URI pour le SingleLogoutService de l'IdP	Clé facultative
QAA-Level	Indique le niveau d'authentification de l'IdP	Clé étrangère
MetaData	Métadonnées de l'IdP	Champ obligatoire

Tableau 11: définition de l'Identity Provider



Les IdP STIAM, les Identity Provider commerciaux (ex. SuisseID) et l'Identity Provider d'une organisation peuvent être définis en tant qu'Identity Provider (IdP).

7.5.4.3 Définition de l'Attribute Authority

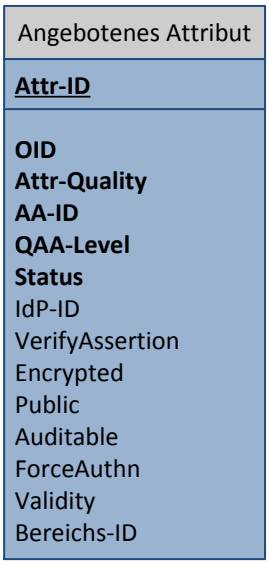


Une autorité d'attributs est un service d'une organisation, qui, en réponse à un Attribute Request Message, renvoie au Hub STIAM les attributs demandés sous forme signée (Attribute Assertion). Pour en savoir plus sur les messages échangés entre le Hub STIAM et l'AA pour la durée d'exécution, se reporter au chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.**.

Nom du champ	Signification	Type
AA-ID	Désignation sans ambigüité de l'AA	Clé primaire
Org-ID	Organisation à laquelle appartient l'AA	Clé étrangère
Entity-ID	Nom sans ambigüité de l'entité	Champ obligatoire
AttributeService	URI pour l'Attribute Assertion Service	Champ obligatoire
MetaData	Métadonnées de l'AA, y compris les informations clé permettant de vérifier la signature	Champ obligatoire

Tableau 12: définition de l'Attribute Authority

7.5.4.4 Attribut proposé



Les Attribute Authorities peuvent proposer des attributs au sein de la Community SuisseTrustIAM. Ces attributs ont besoin d'une Attribute-ID (Attr-ID) et d'un Object Identifier (OID), qui définit l'attribut.

Une organisation, qui propose un attribut, doit indiquer un Niveau d'authentification minimal (QAA-Level) et pourvoir l'attribut d'une valeur de qualité (Attr-Quality).

Un attribut proposé doit avoir un statut.

Il est stipulé (Consent) si un User Consent est nécessaire et quel composant se le procure.

A titre facultatif, un fournisseur peut exiger de pouvoir contrôler lui-même l'authentification d'un Identity Provider.

A titre facultatif, l'utilisation d'un attribut peut être limitée à un domaine précis par un fournisseur.

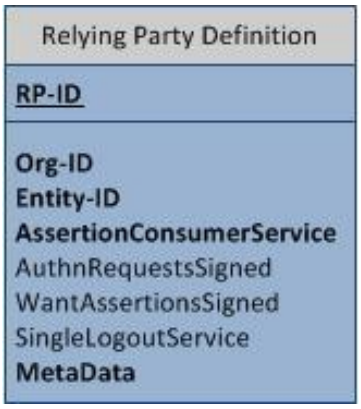
Nom du champ	Signification	Type
Attr-ID	Désignation sans ambigüité d'un attribut	Clé primaire
OID	Object Identifier (OID) pour la définition d'attribut	Clé étrangère
Attr-Quality	Qualité de l'attribut proposé valeurs possibles conformément à eCH-0171 [5]	Clé étrangère
QAA-Level	Quality Authentication Assurance Level de l'eID du sujet Valeurs possibles [1..4]	Clé étrangère
AA-ID	Renvoi de l'ID du fournisseur	Clé étrangère
Status	Statut de l'attribut proposé	Champ obligatoire
IdP-ID	Identity Provider prescrit	Clé étrangère
VerifyAssertion	AA exige une authentification supplémentaire du sujet. Le Hub STIAM doit ainsi répondre dans ‚Identity Relay Modus'[22].	Clé facultative
Encrypted	Le contenu de l'attribut doit être crypté	Clé facultative
Consent	Indique si le consentement de l'utilisateur est nécessaire et quel composant se le procure: • Hub: valeur par défaut, le hub se procure l'User Consent • AA: l'expéditeur STIAM se procure l'User Consent. • Public: pas d'User Consent	Champ obligatoire
Auditable	Indique si le Hub STIAM est autorisé à consigner le contenu de l'attribut.	Clé facultative
ForceAuthn	Avec la publication de cet attribut, une authentification rapide du sujet par un IdP est signalée comme impérative.	Clé facultative
Validity	Indique la période durant laquelle un attribut peut être conservé de manière temporaire dans un cookie.	Clé facultative
Domain-ID	Affecte un attribut à un domaine.	Clé étrangère

Tableau 13: attribut proposé

7.5.4.5 Définition du Relying Party

[22] Comparer avec le chapitre 3.4.2

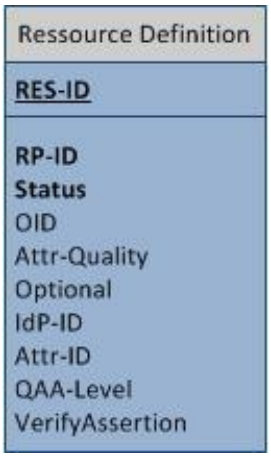
Une organisation peut définir un Service Provider Service, qui reçoit les Security Tokens et les Attribute Assertions. Sous ce Service Provider, qui doit être compris comme un portail, il est possible de définir une ou plusieurs ressources comme applications.



Nom du champ	Signification	Type
RP-ID	Désignation sans ambigüité d'un RP	Clé primaire
Org-ID	Organisation à laquelle appartient le RP	Clé étrangère
Entity-ID	Nom sans ambigüité de l'entité	Champ obligatoire
AssertionConsumerService	URI du Service Provider Service	Champ obligatoire
AuthnRequestsSigned	Indique si le Relying Party envoie ses Authentication Requests signées	Champ facultatif
WantAssertionsSigned	Indique si les Assertions doivent être signées par le Hub STIAM	Champ facultatif
SingleLogoutService	URI pour le SingleLogoutService du Service Provider	Champ facultatif
MetaData	Métadonnées du RP, y compris les informations clé pour chiffrer et vérifier la signature	Champ obligatoire

Tableau 14: définition du Relying Party

7.5.4.6 Définition de la ressource



En tant que Service Provider, un Relying Party peut définir une ou plusieurs ressources. La ressource est transmise par le Relying Party au Hub STIAM, dans l'Authentication Request, pour la durée d'exécution et sous la forme d'un numéro d'index. Le Hub STIAM peut ainsi lire les exigences prescrites dans les définitions de ressources. Il reste ainsi informé des attributs et des exigences facultatives qui sont imposées pour accéder à la ressource.

Nom du champ	Signification	Type
RES-ID	Désignation sans ambigüité d'une ressource	Clé primaire
RP-ID	Relying Party à l'origine de la référence	Clé étrangère
Status	Statut de la ressource	Champ obligatoire
OID	Lien direct vers un ou plusieurs attributs, qui sont requis pour la décision portant sur une autorisation d'accès à la ressource	Clé étrangère
Attr-Quality	Un SysAdmin peut prescrire une valeur de qualité pour chaque OID définie	Clé étrangère
Optional	Indique pour chaque attribut, si il peut être ‚facultatif'. Pa défaut, un attribut est toujours requis dans SuisseTrustIAM.	Clé facultative
IdP-ID	Pour chaque ressource, un Identity Provider peut être prescrit.	Clé facultative
Attr-ID	Indique un ou plusieurs ‚attributs proposés', qui sont nécessaires à la décision d'autoriser l'accès à la ressource.	Clé facultative
QAA-Level	Un niveau d'authentification (QAA-Level) peut être prescrit pour chaque ressource.	Clé étrangère
VerifyAssertion	La ressource demande ainsi l',Identity Relay Modus' auprès du Hub STIAM.	Clé facultative

Tableau 15: définition de la ressource

7.6 Attribut Management

Attribut Definition
OID
Name **Description** **XSD-URI** Public Bereichs-ID

Chaque attribut dispose d'un Object Identifier (OID) unique et de certaines informations, qui viennent compléter la définition de l'attribut.

Outre le nom et la description, d'autres informations techniques telles la syntaxe, l'espace de nom et les valeurs possibles en font partie. Celles-ci sont marquées en tant que lien vers un fichier XSD de schéma d'attribut.

Nom du champ	Signification	Type
OID	Désignation unique d'un attribut	Clé primaire
Name	Friendly-Name de l'attribut	Champ obligatoire

Nom du champ	Signification	Type
Description	Description de l'attribut	Champ obligatoire
XSD-URI	Lien vers le schéma d'attribut	Champ obligatoire
Public	Permet de passer outre le consentement de l'utilisateur pour la publication d'un attribut	Clé facultative
Bereichs-ID	Classe un attribut sous un ou plusieurs domaines	Clé facultative

Tableau 16: définition de l'attribut

8 Considérations de sécurité

La présente architecture SuisseTrustIAM tente de prendre en compte autant d'exigences de respect de la vie privée et de sécurité que possible. Il n'est toutefois pas possible de répondre à toutes les questions concernant notamment la protection de la sphère privée et de la sécurité. Les possibilités d'attaques et les scénarios d'utilisations abusives intentionnelles, par exemple, doivent faire l'objet de vérifications et de discussions en continu.

Scénario	Description	Probabilité	Potentiel de dommage
Mauvais LinkedID	Un utilisateur mal intentionné crée des liens de fausses identités sur l'expéditeur STIAM ou un IdP vers son Account.	Faible. L'utilisateur doit avoir accès aux mauvaises identités.	Moyen. L'utilisateur bénéfice d'un accès éventuellement illégitime au RP.
Identité AA faible	Quand un assaillant connaît les Credentials d'un AA-Account ‚faible' d'un autre utilisateur, il peut alors associer de mauvais attributs à son identité pour la période de définition.	Faible. L'assaillent doit se procurer les informations de l'Account.	Moyen. L'assaillant bénéfice d'un accès éventuellement illégitime au RP.
Vol de Security Token	Un Security Token est intercepté lors du transfert vers le navigateur de l'utilisateur.	Faible.	Faible. L'auteur du méfait peut prendre l'identité de l'utilisateur et poursuivre les activités entamés par l'utilisateur sous la Security-Session.
Logging central	Le logging central sur le Hub STIAM (cf. chap. 5.6) soulève des questions relatives à la protection des données, car les opérations correspondantes sont enregistrées de manière centrale à titre de conservation.	Moyen.	Faible. Les activités des utilisateurs dans l'Identity Federation peuvent être suivies.

Tableau 17: considérations de sécurité

9 Thèmes apparentés

Le tableau suivant répertorie quelques-uns des thèmes qui ne sont pas abordés ou seulement en marge du présent document. Cette liste doit être considérée comme une suggestion en vue de versions ultérieures de SuisseTrustIAM et n'est nullement exhaustive.

Thème	Description
Inter-Federation	A quoi ressemble l'intégration d'une Identity Federation déjà existante? Par exemple quand intégrer SWITCH-aai dans SuisseTrust-IAM?
Identity Federation interne à l'organisation	A quoi ressemblent l'exigence et le modèle de confiance de l'Identity Federation à l'intérieur d'une organisation? De quelles fonctionnalités peut-on se passer? Quelles nouvelles exigences ex. Provisioning, surveillances des autorisations s'y ajoutent?
Intégration de registres publiques	Comment les registres publics peuvent-ils être intégrés comme Attribute Authority sans possibilité d'authentification? Comme établit-on un Identity Mapping fiable?
Request on behalf of...	Dans l'architecture actuelle, on part du principe selon lequel le Hub STIAM est toujours autorisé à déposer auprès d'une AA, une requête portant sur un attribut concernant un sujet particulier. Quand l'AA ne veut pas contrôler elle-même l'authentification du sujet effectuée, elle accepte alors chaque requête signée par le Hub STIAM pour une AA-ID comme identificateur. Que se passe-t-il quand le RP et l'AA exigent une confiance accrue? Que se passe-t-il quand le RP et l'AA doivent se convaincre que le Hub a le droit, à cet endroit, de solliciter effectivement cet attribut pour ce sujet? L'AA doit aussi pouvoir contrôler si le Hub agit vraiment pour le compte du RP à l'origine de la requête?

Tableau 18: autres thèmes

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 et bibliographie

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

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

[3] Haute école spécialisée bernoise, «eCH-0167 Concept cadre SuisseTrustIAM» [Online]. Available: http://www.ech.ch.

[4] eCH, «eCH-0170 Modèle de qualité des identités électroniques,» [Online]. http://www.ech.ch.

[5] eCH, «eCH-0171 Modèle de qualité de la confirmation de valeur d'attribut pour l'eID,» [Online]. http://www.ech.ch.

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

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

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

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

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

[11] Haute école spécialisée bernoise, «eCH-0169 Architecture administrative SuisseTrustIAM,» [Online]. Available: www.ech.ch.

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

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

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

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

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

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

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

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

[19] Haute école spécialisée bernoise, «eCH-0168 Processus standards SuisseTrustIAM» 2013.

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

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

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

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

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

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

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

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

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

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

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

Annexe B – Collaboration & vérification

Agosti Stefan	Haute école spécialisée bernoise
Bernold Ronny	Haute école spécialisée bernoise
Bürge Urs	Urs Bürge Beratung GmbH
Häni Hans	Haute école spécialisée bernoise
Häring Ulrich	ATOS
Hassenstein Gerhard	Haute école spécialisée bernoise
Laube-Rosenpflanzer Annett	Haute école spécialisée bernoise eCH Groupe spécialisé IAM
Leiser Daniel	ATOS
Topfel Martin	Haute école spécialisée bernoise eCH Groupe spécialisé IAM
Vinzens Marcel	Adnovum

Annexe C – Abréviations

IdP	Identity Provider
AA	Attribute Authority
RP	Relying Party
SSO	Single-Sign-On
SAML	Security Assertion Markup Language
IAM	Identity & Access Management
OID	Object Identifier
XSD	XML Schema Definition
URL	Uniform Resource Locator
URI	Uniform Resource Indicator
UIR	User Identifier Repository
STIAM	SuisseTrustIAM
SysAdmin	Administrateur système
OrgSysAdmin	Administrateur système d'une organisation
RO	Responsable d'organisation
CSP	Certification Service Provider
CA	Certification Authority
RLM	Reporting, Logging, Monitoring
MDR	Metadata Registry

Annexe D – Glossaire

Les termes spécifiques employés dans ces pages sont décrits en début de document au chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.**. Aucun glossaire n'est proposé à ce stade, car tous les autres termes ont déjà été décrits en détail dans les documents eCH-0107 [2] et eCH-0167 [3].

Annexe E – Contrôle des modifications

Version	Date	Description, remarque	Nom
0.5	13.12.2012	Version initiale	Gerhard Hassenstein
0.6	15.12.2012	Version harmonisée avec le ‚Processus standard SuisseTrustIAM'	Gerhard Hassenstein
0.7	03.01.2013	Adaptations après révision interne	Stefan Agosti
0.8	07.01.2013	Fusion architecture techn. et processus standards	Stefan Agosti
0.9	22.02.2013	Adaptations après révision interne HESB	Gerhard Hassenstein
0.95	27.02.2013	Adaptations après révision ATOS	Gerhard Hassenstein
0.98	25.11.2013	Version entièrement retravaillée	Gerhard Hassenstein Stefan Agosti
1.0	27.11.2013	Version après révision interne	Gerhard Hassenstein Stefan Agosti
1.1	12.03.2014	Révision après réunion chez Atos	Gerhard Hassenstein Hans Häni Marcel Vinzens Urs Pfenninger Daniel Leiser
1.2	23.05.2014	Feedback Urs Bürge, révision après réunion chez Atos, neutre du point de vue technologique	Annett Laube-Rosenpflanzer
1.3	04.06.2014	Feedback de FG IAM, version soumise à consultation	Annett Laube-Rosenpflanzer
1.4	03.09.2014	Feedback de la consultation	Annett Laube-Rosenpflanzer

Annexe F – Liste des figures

Annexe G – Liste des tableaux